NUMBER THEORY

OLIVIER BRINON

Abstract. These are the lecture notes from a M2 number theory course taught at the University of Bordeaux. They have almost no originality. The main references used were [8], [20] and [18]. Some proofs are near-copies of *loc. cit.*. I thank the students who attended the course and the tutorials for their questions and remarks that helped to improve it, and Pascal Autissier, Annabelle Ducret, Raoul Hallopeau and Théo Untrau for their reading of these notes and their observations, which reduced the number of imprecisions and errors.

Contents

Version: October 4, 2023

1. Notions on commutative algebra

In what follows, A denotes a commutative ring with unit. Ring homomorphisms map units to units.

1.1. Rings.

1.1.1. *Ideals.*

Definition 1.1.2. An *ideal* of A is a subset $I \subset A$ such that:

(1) $(\forall x, y \in I)\, x + y \in I$ (so that I is a subgroup of $(A, +)$);

(2) $(\forall a \in A)\, (\forall x \in I)\, ax \in I$.

Given an ideal $I \subset A$, the quotient group A/I is endowed with a unique ring structure such that the canonical map $A \to A/I$ is a ring homomorphism.

Example 1.1.3. (0) $\{0\}$ is an ideal.
(1) A is an ideal (called the *unit ideal*). We say that an ideal $I \subset A$ is strict if $I \neq A$.
(2) Ideals of $\mathbf{Z}$ are of the form $n\,\mathbf{Z}$ for a unique $n \in \mathbf{Z}_{\geqslant 0}$.
(3) Similarly, if K is a field, nonzero ideals of $K[X]$ are of the form $P(X)K[X]$ for a unique monic polynomial $P(X) \in K[X]$.

Definition 1.1.4. Let $I \subset A$ be a *strict* ideal.
(1) I is *maximal* if it is maximal (for the inclusion) among strict ideals in A.
(2) $I \subset A$ is *prime* if $(\forall x, y \in A)\, (xy \in I \Rightarrow (x \in I \text{ or } y \in I))$.

Example 1.1.5. • The ring A is an *integral domain* if and only if $\{0\}$ is prime.
• $n\,\mathbf{Z}$ is prime in $\mathbf{Z}$ if and only if $n\,\mathbf{Z}$ is maximal if and only if n is a prime integer. Similarly, $P(X)K[X]$ is prime in $K[X]$ if and only if $P(X)K[X]$ is maximal if and only if $P(X)$ is irreducible.

Remark 1.1.6. (1) A maximal ideal is prime.
(2) An ideal $I \subset A$ is maximal (reps. prime) if and only if A/I is a field (resp. an integral domain).
(3) Let Λ be a set and $(I_\lambda)_{\lambda\in\Lambda}$ be ideals in A. Then $\bigcap\limits_{\lambda\in\Lambda} I_\lambda$ is an ideal of A.

Theorem 1.1.7. (Krull). Let $I \subset A$ be a strict ideal. There exists[1] a maximal ideal $\mathfrak{m} \subset A$ such that $I \subset \mathfrak{m}$.

Proof. Let $\mathscr{E}$ be the set of strict ideals $J \subset A$ containing I: it is non empty since $I \in \mathscr{E}$. We (partially) order $\mathscr{E}$ with the relation given by $J_1 \leqslant J_2 \Leftrightarrow J_1 \subset J_2$. The ordered set $(\mathscr{E}, \leqslant)$ is inductive: if $(J_\lambda)_{\lambda\in\Lambda}$ is a chain (*i.e.* a totally ordered subset) of $\mathscr{E}$, then $J := \bigcup\limits_{\lambda\in\Lambda} J_\lambda$ is an element in $\mathscr{E}$, and an upper bound of $(J_\lambda)_{\lambda\in\Lambda}$. By Zorn's lemma, $(\mathscr{E}, \leqslant)$ admits a maximal element $\mathfrak{m}$. If $J \subset A$ is a strict ideal containing $\mathfrak{m}$, then $J \in \mathscr{E}$, hence $J = \mathfrak{m}$ by maximality. This shows that $\mathfrak{m}$ is a maximal ideal, that contains I by definition. □

Remark 1.1.8. One can show that Krull's theorem is equivalent to the axiom of choice.

Definition 1.1.9. • If $X \subset A$, the ideal *generated* by X is the smallest ideal of A that contains X, this is nothing but the intersection of all ideals[2] of A that contain X.
• If $I \subset A$ is an ideal and $X \subset I$, we say that X *generates* I if the ideal generated by X is I. We sometimes denote it by $\langle X\rangle$.
• A *principal* ideal of A is an ideal generated by one element. The ring A is called *principal* (PID) if it is an integral domain and its ideals are all principal.

Example 1.1.10. (1) $\mathbf{Z}$ and $K[X]$ are principal, more generally euclidean rings are principal.
(2) If K is a field, $\langle X, Y\rangle$ is not principal in $K[X, Y]$. Similarly, $\langle 2, X\rangle$ is not principal in $\mathbf{Z}[X]$.
(3) $\mathbf{Z}[i\sqrt{5}]$ is not principal.

Definition 1.1.11. • Let Λ be a set and $(I_\lambda)_{\lambda\in\Lambda}$ be ideals in A. Their *sum* is the ideal generated by $\bigcup\limits_{\lambda\in\Lambda} I_\lambda$. This is nothing but the set of finite A-linear combinations $\sum\limits_{i=1}^{n} a_i x_i$ with $r \in \mathbf{Z}_{\geqslant 0}$, $a_1, \ldots, a_r \in A$ and $x_i \in I_{\lambda_i}$ for all $i \in \{1, \ldots, r\}$.
• Let $I, J \subset A$ be ideals. Their *product* IJ is the ideal generated by $\{xy\}_{\substack{x\in I\\ y\in J}}$.

Definition 1.1.12. Two ideals $I, J \subset A$ are *coprime* (or I is prime to J) when $I + J = A$.

[1] This statement is equivalent to the axiom of choice.

[2] This makes sense by Remark 1.1.6 (3).

Proposition 1.1.13. (1) Two distinct maximal ideals are coprime.
(2) If $I_1, \ldots, I_n$ are prime to J, then $I_1 \cdots I_n$ is prime to J.
(3) If $I, J \subset A$ are coprime and $n, m \in \mathbf{Z}_{>0}$, then I^n and J^m are coprime.

Proof. (1) As $I \subsetneq I + J \subset A$, we have $I + J = A$.
(2) As $I_k + J = A$ for all $k \in \{1, \ldots, n\}$, we have $A = (I_1 + J)(I_2 + J) \cdots (I_n + J) =\subset I_1 \cdots I_n + J$, whence $I_1 \cdots I_n + J = A$.
(3) Applied to $I_k = I$ for all $k \in \{1, \ldots, n\}$, (2) implies that I^n and J are coprime. After replacing I by J and J by I^n, we deduce that I^n and J^m are coprime. □

Theorem 1.1.14. (Chinese remainder theorem). Assume $I_1, \ldots, I_n \subset A$ are pairwise coprime ideals (*i.e.* $i \neq j \Rightarrow I_i + I_j = A$). Then:
(1) $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$;
(2) the canonical ring homomorphism $A/I_1 I_2 \cdots I_n \to \prod\limits_{k=1}^{n} A/I_k$ is an isomorphism.

Proof. By proposition 1.1.13, the case $n = 2$ implies the general case: let $I, J \subset A$ be coprime ideals. There exist $e_I \in I$ and $e_J \in J$ such that $e_I + e_J = 1$.
(1) We have always $IJ \subset I \cap J$. Let $a \in I \cap J$: we have $a = a(e_I + e_J) = ae_I + ae_J$. As $a \in J$ and $e_I \in I$, we have $ae_I \in IJ$. Similarly $ae_J \in IJ$, hence $a \in IJ$, proving the equality.
(2) Let $\varphi\colon A \to (A/I) \times (A/J)$ be the natural map. If $x, y \in A$, we have $\varphi(xe_J + ye_I) = (x + I, y + J)$, so φ is surjective. As $\mathsf{Ker}(\varphi) = I \cap J = IJ$, it induces an isomorphism $A/IJ \xrightarrow{\sim} (A/I) \times (A/J)$. □

1.1.15. *UFDs.*

Definition 1.1.16. Assume that A is an integral domain.
- An element $\alpha \in A \backslash (A^\times \cup \{0\})$ is *prime* (resp. *irreducible*) if the ideal αA is prime (resp. $(\forall a, b \in A)\,(ab = \alpha \Rightarrow (a \in A^\times$ or $b \in A^\times)))$. A prime element is always irreducible[(3)], but the converse is not true in general.
- The ring A is a unique factorization domain (UFD) if it is an integral domain in which every non-zero element can be written as a product of or irreducible elements, uniquely up to order and multiplication by units. More precisely, for any $\alpha \in A \backslash \{0\}$, there exist $n \in \mathbf{Z}_{\geqslant 0}$ and irreducible elements $p_1, \ldots, p_n$ such that

$$\alpha A = p_1 \cdots p_n A$$

and if $\alpha A = q_1 \cdots q_m A$ with $m \in \mathbf{Z}_{\geqslant 0}$ and $q_1, \ldots, q_m$ irreducible, then $m = n$ and there exists $\sigma \in \mathfrak{S}_n$ such that $q_k A = p_{\sigma(k)} A$ for all $k \in \{1, \ldots, n\}$.
There exists $u \in A^\times$ such that $\alpha = u p_1 \cdots p_n$: such an quality is called a *prime decomposition* of α.

Example 1.1.17. (0) A field is a UFD.
(1) $\mathbf{Z}$ and $K[X]$ (where K is a field) are UFD.
(2) The subring $\mathbf{Z}[i\sqrt{5}] = \{x + iy\sqrt{5} \in \mathbf{C}\,;\, x, y \in \mathbf{Z}\}$ of $\mathbf{C}$ is not a UFD, because 2, 3, $1 + i\sqrt{5}$ and $1 - i\sqrt{5}$ are irreducible, the unit are 1 and -1, but $2.3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ (*i.e.* there is no unicity for a prime decomposition of 6).

Lemma 1.1.18. In a PID, irreducible element are prime.

Proof. Let $p \in A$ be an irreducible element. Let $\mathfrak{m} \subset A$ be a maximal ideal such that $p \in \mathfrak{m}$ (*cf* Krull theorem, or use the noetherianity of A). As A is a PID, there exists $\alpha \in A$ such that $\mathfrak{m} = aA$, so $p = \alpha a$ for some $a \in A$. As p is irreducible, we must have $a \in A^\times$ (because $\alpha \notin A^\times$ since $\mathfrak{m} = aA \neq A$). Thus $pA = \mathfrak{m}$ is maximal. □

Definition 1.1.19. Assume A is a UFD, and let $p \in A$ be an irreducible element. If $\alpha \in A \backslash \{0\}$, the *p-adic valuation* of α is

$$v_p(\alpha) = \max\{k \in \mathbf{Z}_{\geqslant 0}\,;\, p^k \mid \alpha\}$$

This is well defined and only depends on the ideals pA and αA.

Proposition 1.1.20. (Properties of valuations). Assume A is a UFD and let $a, b \in A$.
(1) $v_p(ab) = v_p(a) + v_p(b)$;
(2) $a \mid b$ if and only if $v_p(a) \leqslant v_p(b)$ for all irreducible element $p \in A$;
(3) $a \in A^\times$ if and only if $v_p(a) = 0$ for all irreducible element $p \in A$.
(4) $v_p(a + b) \geqslant \min\{v_p(a), v_p(b)\}$ with equality when $v_p(a) \neq v_p(b)$.

[(3)] Because A is a domain. Note that 2 is prime in $\mathbf{Z}/6\mathbf{Z}$, but not irreducible since $2 = 2 \times 4$.

Proof. (1)-(3) follow from the definition and the unicity of decomposition into a product of prime elements. For (4), if $v = \inf\{v_p(a), v_p(b)\}$, then $p^v \mid a$ and $p^v \mid b$, so $p^v \mid a+b$, thus $v_p(a+b) \geqslant v$. Assume $v_p(a) \neq v_p(b)$: we may assume that $v = v_p(a) < v_p(b)$. Write $a = p^v a'$ with $p \nmid a'$ and $b = p^v b'$ with $p \mid b'$, so that $a+b = p^v(a'+b')$ and $p \nmid a'+b'$: we have $v_p(a+b) = v$. □

Proposition 1.1.21. Assume A is a UFD and let $p \in A \backslash \{0\}$. Then p is irreducible if and only if p is prime.

Proof. If p is irreducible and $p \mid ab$, then $v_p(a) + v_p(b) = v_p(ab) \geqslant 1$ so $v_p(a) \geqslant 1$ or $v_p(b) \geqslant 1$ *i.e.* $p \mid a$ or $p \mid b$. Conversely, a prime element is always irreducible. □

Remark 1.1.22. It is easy to show that a noetherian ring (*cf* definition 1.3.3) in which irreducible elements are prime is a UFD. This said, there exist non-noetherian UFD (*eg* $\mathbf{Z}[X_n]_{n \in \mathbf{Z}_{\geqslant 0}}$).

Definition 1.1.23. Assume A is a UFD and let $a, b \in A \backslash \{0\}$. The *gcd* (greatest common divisor) and the *lcm* (least common multiple) of a and b are the greatest lower bound (resp. smallest upper bound) of the set $\{a, b\}$ for the divisibility relation. They are denoted $\mathsf{gcd}(a,b)$ and $\mathsf{lcm}(a,b)$ respectively. We say that a and b are *coprime* when $\mathsf{gcd}(a,b) = 1$.

Remark 1.1.24. (1) Strictly speaking, $\mathsf{gcd}(a,b)$ and $\mathsf{lcm}(a,b)$ are only defined up to multiplication by a unit: only the ideal they generate are well defined.
(2) Let $a, b \in A \backslash \{0\}$ and an irreducible element $p \in A$. Then $v_p(\mathsf{gcd}(a,b)) = \min\{v_p(a), v_p(b)\}$ and $v_p(\mathsf{lcm}(a,b)) = \max\{v_p(a), v_p(b)\}$. Note that $\mathsf{gcd}(a,b)\,\mathsf{lcm}(a,b)A = abA$.
(3) By induction, one can easily extend the definition and consider gcd and lcm of a*finite* family in $A \backslash \{0\}$.

Lemma 1.1.25. (Gauss lemma). Assume that A is a UFD and let $a, b, c \in A \backslash \{0\}$ be such that $\mathsf{gcd}(a,b) = 1$. If $a \mid bc$, then $a \mid c$.

Proof. If $p \in A$ is irreducible and divides a, then $v_p(b) = 0$ since $p \nmid b$ (because a and b are coprime). This implies that $v_p(a) \leqslant v_p(bc) = v_p(c)$. As this holds for any irreducible element p dividing a, we have $a \mid c$ (*cf* proposition 1.1.20 (2)). □

Proposition 1.1.26. A PID is a UFD.

Lemma 1.1.27. Assume that A is an integral domain in which irreducible elements are prime (*cf* proposition 1.1.21). If an element admits a prime decomposition, the latter is unique (in the sense of definition 1.1.16).

Proof. Assume $\alpha = up_1p_2\cdots p_n = vq_1q_2\cdots q_m$, with $n, m \in \mathbf{Z}_{\geqslant 0}$, $u, v \in A^\times$ and $p_1, \ldots, p_n, q_1, \ldots, q_m$ irreducible elements. Possibly after exchanging the decompositions, we may assume $n \leqslant m$. We proceed by induction on n. If $n = 0$, then $\alpha = u \in A^\times$: the product $vq_1q_2\cdots q_m$ is invertible so all its factors are: we must have $m = 0$. Assume $n \geqslant 1$. As p_1 is irreducible and divides the product $vq_1q_2\cdots q_s$, it divides one of the factors (since it is prime). As $v \in A^\times$, it is not divisible by p_1: after renumbering the q_i, we may assume that $p_1 \mid q_1$ *i.e.* $p_1A = q_1A$. Dividing α by p_1, we reduce to the case $n-1$, and use induction hypothesis. □

Proof of proposition 1.1.26. Assume A is a PID. By lemmas 1.1.18 and 1.1.27, it is enough to shows that any nonzero element in A admits at least one prime decomposition. Let $\mathscr{E}$ be the set of elements in $A \backslash \{0\}$ that do not admit a prime decomposition. Assume $\mathscr{E}$ is not empty. As A is noetherian, the set $\mathscr{E}$ admits a minimal element α (for the divisibility relation). The element α can be nor a unit, nor irreducible: it can be written $\alpha = \alpha_1\alpha_2$ with $\alpha_1, \alpha_2 \in A \backslash (A^\times \cup \{0\})$. Then α_1 and α_2 are strict divisors of α, so $\alpha_1, \alpha_2 \notin \mathscr{E}$ by minimality of α: they admit prime decomposition. This implies that their product α admits a prime decomposition: contradiction. □

Remark 1.1.28. • When A is a PID, there is an other characterization of gcd and lcm of two element $a, b \in A$: we have $\mathsf{gcd}(a,b)A = aA + bA$ and $\mathsf{lcm}(a,b)A = aA \cap bA$. Let's prove it for the gcd (the proof for the lcm is similar). As A is principal, there exists $d \in A$ such that $aA + bA = dA$. As $x \in A$ divides a and b if and only if $aA \subset xA$ and $bA \subset xA$ *i.e.* $dA \subset xA$, so $\mathsf{gcd}(a,b) = d$.
• This characterization does not hold in any UFD. For instance, $\mathbf{Q}[X,Y]$ is a UFD (*cf* theorem 1.1.41). As X and Y are irreducible and coprime, we have $\mathsf{gcd}(X,Y) = 1$, though $X\,\mathbf{Q}[X,Y] + Y\,\mathbf{Q}[X,Y] \neq \mathbf{Q}[X,Y]$ (the LHS is the ideal of polynomials vanishing at $(0,0)$). Of course, this follows from the fact that $\mathbf{Q}[X,Y]$ is not a PID.

Example 1.1.29. If K is a field and $n \in \mathbf{Z}_{>0}$, the ring $K[X_1, \ldots, X_n]$ is a UFD (*cf* theorem 1.1.41) but not a PID (*cf* remark above). Similarly the ring $\mathbf{Z}[X]$ is a UFD (*cf loc. cit.*) but not a PID (the ideal generated by 2 and X is not principal).

Proposition 1.1.30. In a PID, nonzero prime ideals are maximal.

Proof. Assume A is a PID, and let $\mathfrak{p} \subset A$ be a nonzero prime ideal. Write $\mathfrak{p} = \langle a \rangle$ with $a \in A \backslash \{0\}$: if $I \subset A$ is an ideal containing $\mathfrak{p}$, we have $I = \langle b \rangle$ with $b \in A \backslash \{0\}$ dividing a: write $a = bc$ with $c \in A$. As a is prime, we have $a \mid b$ or $a \mid c$. If $a \mid b$ (resp. $a \mid c$) there exists $d \in A$ such that $b = ad$ (resp. $c = ad$). Then we have $a = bc = acd$ (resp. $a = bc = abd$), hence $1 = cd$ (resp. $1 = bd$) because $a \neq 0$ and A is integral, so that $I = \mathfrak{p}$ (resp. $I = A$), showing that $\mathfrak{p}$ is maximal. □

Definition 1.1.31. Assume that A is a integral domain.
- An *euclidean function* is a map $\phi\colon A \backslash \{0\} \to \mathbf{Z}_{\geqslant 0}$ such that if $b \mid a$ in $A \backslash \{0\}$, then $\phi(b) \leqslant \phi(a)$.
- An euclidean function ϕ defines an *euclidean division* if for all $(a, b) \in A \times A \backslash \{0\}$, there exist $q, r \in A$ such that $a = bq + r$ and ($r = 0$ or $\phi(r) < \phi(b)$). "The" element q is called the *quotient* and r the *remainder* of the division.
- The ring A is *euclidean* if it admits an euclidean function that defines an euclidean division.

Remark 1.1.32. If A is an euclidean domain, there is not unicity for an euclidean function. Moreover, unicity of quotient and remainder is not required.

Exemples 1.1.33. A field is an euclidean domain. The ring $\mathbf{Z}$ is euclidean domain, an euclidean function being given by $\phi(a) = |a|$ (absolute value). In that case, euclidean division is the usual one. When K is a field, the ring of polynomials $K[X]$ is euclidean, an euclidean function being given by $\phi(P) = \deg(P)$. Here again, euclidean division is the usual one.
The ring $\mathbf{Z}[i] = \{a + ib \in \mathbf{C}\,;\, a, b \in \mathbf{Z}\}$ of *Gauss integers* is euclidean, endowed with the euclidean function given by $\phi(a + ib) = a^2 + b^2$.

Proposition 1.1.34. An euclidean domain is a PID.

Proof. Assume A is an euclidean domain, let $\phi\colon A \backslash \{0\} \to \mathbf{Z}_{\geqslant 0}$ be an euclidean function and $I \subset A$ an ideal. To prove that I is principal, we may assume that $I \neq 0$. In that case, $\phi(I \backslash \{0\})$ is an nonempty subset of $\mathbf{Z}_{\geqslant 0}$, so it admits a smallest element: let $b \in I \backslash \{0\}$ be such that $\phi(b)$ is minimal. One has $bA \subset I$. Conversely, let $a \in I$. There exist $q, r \in A$ such that $a = qb + r$ with $r = 0$ or $\phi(r) < \phi(b)$. Assume $r \neq 0$, so that $\phi(r) < \phi(b)$. As $r = a - qb \in I$ and $r \neq 0$, we have $\phi(b) \leqslant \phi(r)$ by minimality of $\phi(b)$, which s absurd: we must have $r = 0$, *i.e.* $a = qb \in bA$. Thus $I = bA$ is principal. □

Remark 1.1.35. There are PID that are not euclidean domains, for instance $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$.

Corollary 1.1.36. Let K be a field, the rings $\mathbf{Z}$ and $K[X]$ are PID, hence UFD (*cf* proposition 1.1.26).

A ring homomorphism $f\colon A \to B$ induces a ring homomorphism $A[X] \to B[X]$. If A is a subring of B, then $A[X]$ is a subring of $B[X]$.

Definition 1.1.37. Assume that A is a UFD and let $P = a_0 + a_1X + \cdots + a_nX^n \in A[X] \backslash \{0\}$. The *content* of P is

$$c(P) = \mathsf{gcd}\{a_i\,;\, a_i \neq 0\}.$$

Lemma 1.1.38. (Gauss Lemma). If A is a UFD and $P, Q \in A[X] \backslash \{0\}$, then $c(PQ) = c(P)c(Q)$.

Remark 1.1.39. As gcd is defined up to multiplication by a unit, one should write $c(PQ)A = c(P)c(Q)A$. In what follows, we will keep this abusive notation to avoid heaviness.

Proof. Write $P = c(P)\widetilde{P}$ and $Q = c(Q)\widetilde{Q}$ with $c(\widetilde{P}) = 1$ and $c(\widetilde{Q}) = 1$: we have $PQ = c(P)c(Q)\widetilde{P}\widetilde{Q}$. Replacing P and Q by $\widetilde{P}$ and $\widetilde{Q}$ respectively, we may assume that $c(P) = 1$ and $c(Q) = 1$: we have to show that $c(PQ) = 1$.
Assume instead that there exist a prime element $p \in A$ such that $p \mid c(PQ)$. Denote by $\overline{P}$ and $\overline{Q}$ the images of P and Q in $(A/pA)[X]$ respectively, this implies that $\overline{P}\,\overline{Q} = 0$ in $(A/pA)[X]$. As p is prime, the ring A/pA is an integral domain: so is the ring $(A/pA)[X]$. This implies that $\overline{P} = 0$ or $\overline{Q} = 0$, *i.e.* $p \mid c(P)$ or $p \mid c(Q)$, contradicting $c(P) = 1$ and $c(Q) = 1$. □

Proposition 1.1.40. Assume that A is a UFD. Let $K = \mathsf{Frac}(A)$ and $P \in A[X]$ such that $c(P) = 1$. Then P is irreducible in $A[X]$ if and only if P is irreducible in $K[X]$.

Proof.
- Assume that P is irreducible in $K[X]$ and write $P = Q_1Q_2$ with $Q_1, Q_2 \in A[X]$. As P is irreducible in $K[X]$, possibly after exchanging Q_1 and Q_2, the polynomial Q_1 is constant so $Q_1 = c(Q_1)$. By lemma 1.1.38, we have $1 = c(P) = c(Q_1)c(Q_2)$, so $Q_1 \in A^\times$. Thus P is irreducible in $A[X]$.
- Conversely, assume that P is irreducible in $A[X]$ write $P = Q_1Q_2$ with $Q_1, Q_2 \in K[X]$. There exist $a_1, a_2 \in A \backslash \{0\}$ such that $a_1Q_1 \in A[X]$ and $a_2Q_2 \in A[X]$. We have $a_1a_2 = c(a_1a_2P) = c(a_1Q_1)c(a_2Q_2)$ by lemma 1.1.38, because $c(P) = 1$. Write $a_1Q_1 = c(a_1Q_1)\widetilde{Q}_1$ and $a_2Q_2 = c(a_2Q_2)\widetilde{Q}_2$ with $\widetilde{Q}_1, \widetilde{Q}_2 \in A[X]$:

we have $a_1a_2P = c(a_1Q_1)\widetilde{Q}_1c(a_2Q_2)\widetilde{Q}_2 = a_1a_2\widetilde{Q}_1\widetilde{Q}_2$ whence $P = \widetilde{Q}_1\widetilde{Q}_2$ (the ring A is an integral domain). As P is irreducible in $A[X]$, we may assume, possibly after exchanging $\widetilde{Q}_1$ and $\widetilde{Q}_2$, that $\widetilde{Q}_1 \in A^\times$. Then $Q_1 \in K^\times$ and P is irreducible in $K[X]$. □

Theorem 1.1.41. If A is a UFD, then[4] $A[X]$ is a UFD.

Proof. • If $p \in A$ is an irreducible element, the constant polynomial p is irreducible in $A[X]$. Indeed, A/pA is an integral domain: so is $A[X]/pA[X] \simeq (A/pA)[X]$ and p is prime hence irreducible in $A[X]$.
• If $P \in A[X]$ is of degree $\geqslant 1$ and irreducible, then $c(P) = 1$. Indeed one can write $P = c(P)\widetilde{P}$ with $\widetilde{P} \in A[X]$, providing a non trivial factorization if $c(P)$ is not invertible.
• *Existence of a prime decomposition.* Let $P \in A[X]\backslash\{0\}$. Write $P = c(P)\widetilde{P}$ with $\widetilde{P} \in A[X]$ such that $c(\widetilde{P}) = 1$. As A is a UFD, $c(P)$ has a prime decomposition, so it is enough to show that $\widetilde{P}$ has a prime decomposition: we may assume that $c(P) = 1$. If $P \in A$, then $P = 1$: we may assume that $\deg(P) \geqslant 1$. Put $K = \mathsf{Frac}(A)$. As $K[X]$ is a UFD (*cf* corollary 1.1.36), we may write $P = P_1P_2\cdots P_r$ with $P_i \in K[X]$ irreducible for all $i \in \{1,\ldots,r\}$. For $i \in \{1,\ldots,r\}$, let $a_i \in A\backslash\{0\}$ be such that $a_iP_i \in A[X]$, and $\widetilde{P}_i = c(a_iP_i)^{-1}(a_iP_i) \in A[X]$. As $\widetilde{P}_i$ has content 1 and is irreducible in $K[X]$ (because P_i is), it is irreducible in $A[X]$ (*cf* proposition 1.1.40). We have $a_1a_2\cdots a_r = c(a_1P_1)\cdots c(a_rP_r)$ by lemma 1.1.38, because $c(P) = 1$, hence the prime decomposition $P = \widetilde{P}_1\widetilde{P}_2\cdots\widetilde{P}_r$.
• *Unicity of prime decomposition.* Let $P \in A[X]\backslash\{0\}$ and $P = P_1P_2\cdots P_r$ and $P = Q_1Q_2\cdots Q_s$ two prime decompositions in $A[X]$. Possibly after renumbering the P_i (resp. the Q_j), there exist $r_0 \leqslant r$ (resp. $s_0 \leqslant s$) such that $P_i \in A\backslash\{0\}$ for $i \leqslant r_0$ and $\deg(P_i) > 0$ for $r_0 < i \leqslant r$ (resp. $Q_j \in A\backslash\{0\}$ for $j \leqslant s_0$ and $\deg(Q_j) > 0$ for $s_0 < j \leqslant s$). By the second point above, we have $c(P_i) = c(Q_j) = 1$ for $r_0 < i \leqslant r$ and $s_0 < j \leqslant s$. Taking contents in the equality $P_1P_2\cdots P_r = Q_1Q_2\cdots Q_s$, we get $P_1P_2\cdots P_{r_0} = Q_1Q_2\cdots Q_{s_0}$, which is an equality of two prime decompositions in the UFD A: we have $r_0 = s_0$, and after renumbering, we may assume that $P_iA = Q_iA$ for all $i \in \{1,\ldots,r_0\}$. Dividing P by $P_1P_2\cdots P_{r_0}$, we get $P_{r_0+1}\cdots P_rA[X] = Q_{r_0+1}\cdots Q_sA[X]$. This is a prime decomposition in $K[X]$, which is a UFD: we have $r = s$ and after renumbering, we may assume that $P_iK[X] = Q_iK[X]$ for all $i \in \{r_0+1,\ldots,r\}$. As $c(P_i) = c(Q_i) = 1$, we have in fact $P_iA[X] = Q_iA[X]$ for all $i \in \{r_0+1,\ldots,r\}$. □

Remark 1.1.42. (1) During the proof, we showed that a complete family of representative of irreducible elements in $A[X]$ is given by the union of a complete family of representative of irreducible elements in A and that of a family of polynomials in $A[X]$ with content 1 that forms a complete family of representatives of irreducible elements in $K[X]$.
(2) In general, A may be a UFD without $A[\![X]\!]$ being one.

To summarize the relationships between the classes of rings recalled above, we have the following implications (whose reverses are false):

$$\text{fields} \Rightarrow \text{Euclidean domains} \Rightarrow \text{PID} \Rightarrow \text{UFD} \Rightarrow \text{integrally closed domains} \Rightarrow \text{integral domains}$$

1.2. Modules and algebras.

1.2.1. *Modules.*

Definition 1.2.2. An *A-module* is a triple $(M,+,\cdot)$ where $(M,+)$ is an abelian group and $\cdot\colon A \times M \to M$ an external composition law such that :

(1) $(\forall a,b \in A)\ (\forall m \in M)\ (a+b)\cdot m = a\cdot m + b\cdot m$;
(2) $(\forall a,b \in A)\ (\forall m \in M)\ (ab)\cdot m = a\cdot(b\cdot m)$;
(3) $(\forall a \in A)\ (\forall m_1,m_2 \in M)\ a\cdot(m_1+m_2) = a\cdot m_1 + a\cdot m_2$;
(4) $(\forall m \in M)\ 1\cdot m = m$

This amounts to give a ring homomorphism $A \to \mathsf{End}(M)$.

Remark 1.2.3. Elements in A are called *scalars*. As usual, we usually denote a module by the underlying set and write am instead of $a\cdot m$.

Example 1.2.4. (1) A $\mathbf{Z}$-module in nothing but an abelian group.
(2) If K is a field, an K-module is just a K-vector space.
(3) If K is a field, a $K[X]$-module is a K-vector space endowed with a K-linear endomorphism (corresponding to the multiplication by X).
(4) If $I \subset A$ is an ideal, then I and A/I are A-modules.

[4] The converse is true and easy.

Definition 1.2.5. Let M be an A-module. A *sub-A-module* of M is an additive subgroup $N \subset M$ which is stable under multiplication by scalars, *i.e.* such that

$$(\forall a \in A)\ (\forall n_1, n_2 \in N)\ n_1 + an_2 \in N.$$

Exemples 1.2.6. Submodules of A are nothing but its ideals. When A is a field, submodules are sub-vector spaces.

Operations on submodules of an A-module. Let M be an A-module and $(M_\lambda)_{\lambda\in\Lambda}$ a family of sub-A-modules of M. The intersection $\bigcap\limits_{\lambda\in\Lambda} M_\lambda$ is a submodule of M. Put

$$\sum_{\lambda\in\Lambda} M_\lambda = \Big\{ \sum_{\lambda\in\Lambda} m_\lambda\,;\ (m_\lambda)_{\lambda\in\Lambda} \in \bigoplus_{\lambda\in\Lambda} M_\lambda \Big\}$$

(the set of *finite* sums of elements in $\bigcup\limits_{\lambda\in\Lambda} M_\lambda$). This is a sub-$A$-module of M, called the *sum* of $(M_\lambda)_{\lambda\in\Lambda}$.

Definition 1.2.7. Let M be an A-module.
(1) Let $X \subset M$. There exists a smallest sub-A-module N of M such that $X \subset N$: it is called the sub-A-module of M *generated* by X (it is the intersection of all sub-A-modules of M that contain X). It is also the sum $\sum\limits_{x\in X} Ax$ (where $Ax = \{ax,\ a \in A\}$).
(2) A subset $X \subset M$ *generates* M when the sub-A-module of M generated by X is M itself.
(3) The A-module M is *of finite type* if it is generated by a finite part.
(4) The A-module M is called *noetherian* if all its sub-A-modules are of finite type.

Definition 1.2.8. Let Λ be a set and $(M_\lambda)_{\lambda\in\Lambda}$ a family of A-modules.
(1) The *product* $\prod\limits_{\lambda\in\Lambda} M_\lambda$ is the A-module of maps $f\colon \Lambda \to \bigcup\limits_{\lambda\in\Lambda} M_\lambda$ such that $f(\lambda) \in M_\lambda$ for all $\lambda \in \Lambda$.
(2) The (direct) *sum* $\bigoplus\limits_{\lambda\in\Lambda} M_\lambda$ is the sub-A-module of $\prod\limits_{\lambda\in\Lambda} M_\lambda$ made of maps $f\colon \Lambda \to \bigcup\limits_{\lambda\in\Lambda} M_\lambda$ such that the set $\{\lambda \in \Lambda,\ f(\lambda) \neq 0\}$ is *finite*.
(3) If $M_\lambda = M$ for all $\lambda \in \Lambda$, one writes M^Λ and $M^{(\Lambda)}$ instead of $\prod\limits_{\lambda\in\Lambda} M$ and $\bigoplus\limits_{\lambda\in\Lambda} M$. When $n \in \mathbf{Z}_{\geqslant 0}$ and $\Lambda = \{1, \ldots, n\}$, one denotes it M^n.

Remark 1.2.9. When Λ is finite, the A-modules $\prod\limits_{\lambda\in\Lambda} M_\lambda$ and $\bigoplus\limits_{\lambda\in\Lambda} M_\lambda$ are the same.

Definition 1.2.10. (1) Let M and N be A-modules. An *A-linear* map from M to N is a group homomorphism $f\colon M \to N$ such that $f(am) = af(m)$ for all $a \in A$ and $m \in M$. The set of A-linear maps from M to N is an abelian group denoted $\mathsf{Hom}_A(M, N)$.
(2) The *kernel* of $f \in \mathsf{Hom}_A(M, N)$ is the submodule $\mathsf{Ker}(f) = f^{-1}(0)$ of M, and the *image* of f is the submodule $\mathsf{Im}(f) = f(M)$ of N. The *cokernel* of f is $\mathsf{Coker}(f) := N/\mathsf{Im}(f)$.
(3) We say that f is an *isomorphism* when f is bijective (the inverse map f^{-1} is then A-linear). This is equivalent to $\mathsf{Ker}(f) = \{0\}$ (*i.e.* f is injective) and $\mathsf{Im}(f) = N$ (that is $\mathsf{Coker}(f) = \{0\}$, *i.e.* f is surjective).

Definition 1.2.11. Let M be an A-module and N a sub-A-module. The quotient group M/N is naturally endowed with a A-module structure (because $a(m+N) = am + aN \subset am + N$ for all $m \in M$ and $a \in A$). The A-module M/N is called the *quotient* of M by N. The canonical map $\pi\colon M \to M/N; m \mapsto m + N$ is A-linear, and has the following universal property: for all A-linear map $f\colon M \to M'$ such that $N \subset \mathsf{Ker}(f)$, there exists a unique A-linear map $\widetilde{f}\colon M/N \to M'$ such that $f = \widetilde{f} \circ \pi$.

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, "\pi"'] & M' \\
M/N \arrow[ur, "\widetilde{f}"'] &
\end{tikzcd}$$

In particular, if $f\colon M \to M'$ is A-linear, there is a *canonical decomposition* $f = \iota \circ \widetilde{f} \circ \pi$ where $\iota\colon\ \mathsf{Im}(f) \to M'$ is the inclusion, $\widetilde{f}$ an isomorphism and $\pi\colon M \to M/\mathsf{Ker}(f)$ the canonical projection.

Definition 1.2.12. (1) A *free* A-module is an A-module isomorphic to $A^{(\Lambda)}$ for some set Λ.
(2) Let Λ be a set. For $\lambda \in \Lambda$, let $e_\lambda \in A^{(\Lambda)}$ be the element defined by $e_\lambda(\eta) = \delta_{\lambda,\eta}$ (Kronecker symbol). The family $(e_\lambda)_{\lambda\in\Lambda}$ is called the *canonical basis* of $A^{(\Lambda)}$.

Proposition 1.2.13. (1) If $a \in A^{(\Lambda)}$, then $a = \sum\limits_{\lambda\in\Lambda} a(\lambda)e_\lambda$ (the sum is finite).

(2) If M is an A-module, the A-linear map

$$\begin{aligned}\mathsf{Hom}_A(A^{(\Lambda)}, M) &\to M^\Lambda\\ f &\mapsto (f(e_\lambda))_{\lambda\in\Lambda}\end{aligned}$$

is an isomorphism. In other words, the data of an A-linear map $f\colon A^{(\Lambda)} \to M$ is equivalent to that of the family $(f(e_\lambda))_{\lambda\in\Lambda}$.

Proof. (1) For $\eta \in \Lambda$, one has $\Big(\sum\limits_{\lambda\in\Lambda} a(\lambda)e_\lambda\Big)(\eta) = a(\eta)$.

(2) Follows from $f(a) = \sum\limits_{\lambda\in\Lambda} a(\lambda)f(e_\lambda)$ for all $f \in \mathsf{Hom}_A(A^{(\Lambda)}, M)$ and $a \in A^{(\Lambda)}$. □

Definition 1.2.14. Let M be an A-module and $\{m_\lambda\}_{\lambda\in\Lambda} \subset M$. Form proposition 1.2.13 (2), there exists a unique A-linear map $f\colon A^{(\Lambda)} \to M$ such that $f(e_\lambda) = m_\lambda$ for all $\lambda \in \Lambda$. The A-module $\mathsf{Im}(f)$ is the submodule of M generated by $\{m_\lambda\}_{\lambda\in\Lambda}$. In particular, the family $\{m_\lambda\}_{\lambda\in\Lambda}$ generates M if and only if f is surjective. When f is injective, we say that $\{m_\lambda\}_{\lambda\in\Lambda}$ is *free* (or linearly independent). When f is an isomorphism (so that M is free), we say that $(m_\lambda)_{\lambda\in\Lambda}$ is a *basis* of M. In that case, any $m \in M$ can be uniquely written $m = \sum\limits_{\lambda\in\Lambda} a_\lambda m_\lambda$ with $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$. Such a family $(m_\lambda)_{\lambda\in\Lambda}$ is called a *basis* of M (this generalizes the usual notion of basis of a vector space over a field).

Remark 1.2.15. When A is a field, any A-module is free (any vector space has a basis). This is not true if A is not a field: there exists a non zero ideal $I \subset A$ such that $I \neq A$, and the A-module A/I is not free (if $e \in A/I$ and $a \in I\backslash\{0\}$, then $ae = 0$). For instance, $\mathbf{Z}/2\mathbf{Z}$ is a $\mathbf{Z}/4\mathbf{Z}$-module, and it is not free. It can be shown (this in *not* obvious) that $\mathbf{Z}^{\mathbf{Z}_{\geqslant 0}}$ is not free over $\mathbf{Z}$ (though it has no torsion).

Proposition 1.2.16. Bases of a free modules have all the same cardinality.

Proof. We have to show that if Λ and Λ' are sets such that the A-modules $A^{(\Lambda)}$ and $A^{(\Lambda')}$ are isomorphic, then Λ and Λ' have the same cardinality. Let $f\colon A^{(\Lambda)} \to A^{(\Lambda')}$ be an isomorphism, and $I \subset A$ a maximal ideal A (*cf* Krull's theorem). As f is A-linear, it induces an isomorphism $\overline{f}\colon (A/I)^{(\Lambda)} \to (A/I)^{(\Lambda')}$. As I is maximal, A/I is a field: the A/I-vector spaces $(A/I)^{(\Lambda)}$ and $(A/I)^{(\Lambda')}$ are isomorphic, so $\mathsf{Card}(\Lambda) = \mathsf{Card}(\Lambda')$. □

Definition 1.2.17. From the preceding proposition, if M is isomorphic to A^n with $n \in \mathbf{Z}_{\geqslant 0}$, the integer n is an invariant of M, called the *rank* of M and denoted by $\mathsf{rk}(M)$.

Remark 1.2.18. When M and N are free A-module of ranks m and n, proposition 1.2.13 (2), implies that the choice of bases of M and N provide an isomorphism

$$\mathsf{Hom}_A(M, N) \simeq \mathsf{Hom}_A(A^m, A^n) = \mathsf{M}_{n\times m}(A).$$

As for vector spaces over a field, after the choice of bases, the data of a A-linear map between free A-modules of finite rank is equivalent to that of its matrix in the chosen bases.

Definition 1.2.19. Let M be an A-module and $m \in M$. Put $\mathsf{ann}_A(m) = \{a \in A\,;\, am = 0\}$. This is an ideal of A, called *annihilator* of m. We say that m is *torsion* if $\mathsf{ann}_A(m) \neq \{0\}$, *i.e.* if it exists $a \in A\backslash\{0\}$ such that $am = 0$. We denote M_{tors} the set of torsion elements in M, and we say that M is *torsion-free* (resp. *has torsion*) if $M_{\mathsf{tors}} = \{0\}$ (resp. $M_{\mathsf{tors}} = M$).
Put $\mathsf{ann}_A(M) = \{a \in A\,;\, (\forall m \in M)\ am = 0\} = \bigcap\limits_{m\in M} \mathsf{ann}_A(m)$ (the annihilator of A): this is an ideal. The A-module structure on M induces an $A/\mathsf{ann}_A(M)$-module structure on M. Note that M may have torsion even if $\mathsf{ann}_A(M) = \{0\}$: for instance $\mathsf{ann}_{\mathbf{Z}}(\mathbf{Q}/\mathbf{Z}) = \{0\}$.

Example 1.2.20. If $I \subset A$ is a non zero ideal, the A-module A/I has torsion. For instance, $\mathbf{Z}/2\mathbf{Z}$ is a $\mathbf{Z}/6\mathbf{Z}$-module with torsion. *Idem* for the $\mathbf{Z}$-module $\mathbf{Q}/\mathbf{Z}$.

Proposition 1.2.21. If A is an integral domain and M is an A-module, then M_{tors} is a submodule of M and the quotient A-module M/M_{tors} is torsion-free.

Proof. If $m_1, m_2 \in M_{\mathsf{tors}}$ and $\alpha \in A$, there exist $a_1, a_2 \in A\backslash\{0\}$ such that $a_1m_1 = 0$ and $a_2m_2 = 0$. As A is an integral domain, we have $a_1a_2 \neq 0$ and $a_1a_2(m_1 + \alpha m_2) = 0$ so that $m_1 + \alpha m_2 \in M_{\mathsf{tors}}$.
Let $m \in M$ whose image $m + M_{\mathsf{tors}}$ is torsion in M/M_{tors}: there exists $a \in A\backslash\{0\}$ such that $am + M_{\mathsf{tors}} = M_{\mathsf{tors}}$ *i.e.* $am \in M_{\mathsf{tors}}$, so that there exists $b \in A\backslash\{0\}$ such that $b(am) = 0$. As A is an integral domain, we have $ab \neq 0$, and $m \in M_{\mathsf{tors}}$. □

Remark 1.2.22. (1) The previous statement does not hold if A is not an integral domain. For instance, if $A = M = \mathbf{Z} \times \mathbf{Z}$, then $M_{\mathsf{tors}} = (\mathbf{Z} \times \{0\}) \cup (\{0\} \times \mathbf{Z})$ is not a submodule of M.
(2) A free A-module is torsion-free, but the converse is false in general (it holds for modules of finite type over principal rings).

1.2.23. *Algebras.*

Definition 1.2.24. An A-algebra is a ring homomorphism $f\colon A \to B$ (which may not be injective), whose image lies in the center of B. We will often denote it by the underlying ring B. A *morphism* between two A-algebras $f_1\colon A \to B_1$ and $f_2\colon A \to B_2$ is a ring homomorphism $g\colon B_1 \to B_2$ such that $g \circ f_1 = f_2$.

$$\begin{tikzcd} B_1 \arrow[rr, "g"] & & B_2 \\ & A \arrow[ul, "f_1"] \arrow[ur, "f_2"'] & \end{tikzcd}$$

Remark 1.2.25. (0) Any ring is a $\mathbf{Z}$-algebra, in a unique way.
(1) If $f\colon A \to B$ is an algebra, then B is naturally endowed with an A-module structure, and the multiplication law $B \times B \to B$ is A-bilinear. Conversely, if B is a ring endowed with an A-module structure such that the multiplication $B \times B \to B$ is A-bilinear, then the map $f\colon A \to B$; $a \mapsto a1_B$ is an A-algebra.

Example 1.2.26. (1) A field extension L/K is a K-algebra.
(2) If K is a field and V a K-vector space, the (non commutative) ring $\mathsf{End}_K(V)$ is a K-algebra.
(3) If A is a ring, the polynomial ring $A[X_\lambda]_{\lambda\in\Lambda}$ is an A-algebra.
(4) If B and C are A-algebras, so is their product $B \times C$.
(5) If B is an A-algebra and $I \subset B$ an ideal, then B/I is an A-algebra.

Definition 1.2.27. Let $f\colon A \to B$ an A-algebra.
(1) A *sub-A-algebra* is a subring $B' \subset B$ such that f factors through a ring homomorphism $A \to B'$ (in other words such that the inclusion map $B' \to B$ is a morphism of A-algebras).
(2) Let $X := \{x_\lambda\}_{\lambda\in\Lambda} \subset B$. There exists a smallest sub-A-algebra of B that contains X (this is nothing but the intersection of all the sub-A-algebras of B containing X). This subalgebra is denoted $A[x_\lambda]_{\lambda\in\Lambda}$ and is called the sub-A-algebra *generated* by X. If it is B itself, we say that $\{x_\lambda\}_{\lambda\in\Lambda}$ *generates* the A-algebra B.
(3) An A-algebra is of *finite type* if it is generated by a finite set. This is equivalent to the existence of a surjective morphism of A-algebras $A[X_1, \ldots, X_n] \to B$.
(4) An A-algebra is *finite* if it is finite as an A-module.

Remark 1.2.28. (1) A finite A-algebra is of finite type, but the converse does not hold (for instance the polynomial A-algebra $A[X]$ is not finite).
(2) Let B a finite A-algebra and M a B-module of finite type. The M is an A-module of finite type. Indeed, one can write $B = \sum\limits_{i=1}^{r} b_i A$ and $M = \sum\limits_{j=1}^{s} Bm_j$, so that $M = \sum\limits_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant s}} Ab_i m_j$.

1.3. Noetherianity.

Proposition 1.3.1. (1) Let M be an A-module. The following properties are equivalent:

(i) M is noetherian (*cf* definition 1.2.7 (4));
(ii) every ascending sequence of sub-A-modules of M is stationary;
(iii) every non empty subset of submodules of M contains elements that are maximal under the inclusion.

(2) Let M be an A-module and $N \subset M$ a submodule. Then M is noetherian if and only if the A-modules N and M/N are.

Proof. (1) **(i)⇒(ii)**. Let $(M_n)_{\in\mathbf{Z}_{\geqslant 0}}$ be an ascending sequence of submodules. As the submodule $\sum\limits_{n\in\mathbf{Z}_{\geqslant 0}} M_n$ is of finite type, it is generated by a finite set $\{m_1, \ldots, m_r\}$: let $N \in \mathbf{Z}_{\geqslant 0}$ be such that $\{m_1, \ldots, m_r\} \subset M_N$, so that $M_N \subset \sum\limits_{n\in\mathbf{Z}_{\geqslant 0}} M_n \subset M_N$, hence $\sum\limits_{n\in\mathbf{Z}_{\geqslant 0}} M_n = M_N$, and $M_n = M_N$ for all $n \geqslant N$.
(ii)⇒(iii). Let $\mathscr{E}$ be such a subset. If it has no maximal element, one can inductively construct a strictly ascending (for the inclusion) sequence of elements in $\mathscr{E}$, contradicting (ii).
(iii)⇒(i). Let $N \subset M$ be a submodule and $\mathscr{E}$ the set of submodules of finite type in N. As $\{0\} \in \mathscr{E}$, we have $\mathscr{E} \neq \varnothing$: by (iii), the set $\mathscr{E}$ contains a maximal element N_0. Assume $N_0 \neq N$: there exists $x \in N\backslash N_0$ and $N' = N_0 + Ax \subset N \in \mathscr{E}$. As $N_0 \subsetneq N'$, this contradicts the maximality of N_0: we have $N_0 = N$ and N is of finite type.

(2) • If M is noetherian, then N is noetherian. If N' is a submodule of M/N, we can write $N' = \widetilde{N}/N$ with $\widetilde{N} = \pi^{-1}(N')$ (where $\pi\colon M \to M/N$ is the canonical map). As M is noetherian, $\widetilde{N}$ is of finite type, which implies that $N' = \widetilde{N}/N$ is of finite type as well, and M/N is noetherian.

• Assume N and M/N are noetherian. Let $(M_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ be an ascending sequence of submodules of M. The sequences $(M_n \cap N)_{n\in\mathbf{Z}_{\geqslant 0}}$ and $((N + M_n)/N)_{n\in\mathbf{Z}_{\geqslant 0}}$ are ascending in N and M/N respectively. As they are noetherian, those sequences are stationary: there exists $n_0 \in \mathbf{Z}_{\geqslant 0}$ such that $M_n \cap N = M_{n_0} \cap N$ and $(N + M_n)/N = (N + M_{n_0})/N$ *i.e.* $N + M_n = N + M_{n_0}$ for all $n \geqslant n_0$. If $m \in M_n$, there exists $x \in N$ and $y \in M_{n_0} \subset M_n$ such that $m = x + y$. As $x = y - m \in N \cap M_n = N \cap M_{n_0}$, we have $m \in M_{n_0}$, hence $M_n \subset M_{n_0}$ *i.e.* $M_n = M_{n_0}$. The A-module M is thus noetherian. □

Corollary 1.3.2. If M_1 and M_2 are noetherian, so is their product $M_1 \times M_2$.

Proof. As $M_1 \simeq M_1 \times \{0\}$ and $M_2 \simeq (M_1 \times M_2)/(M_1 \times \{0\})$ are noetherian, this follows from proposition 1.3.1 (2). □

Definition 1.3.3. The ring A is *noetherian* if it is as an A-module. By definition, this means that every ideal of A is of finite type. By proposition 1.3.1, this is equivalent to the fact that any ascending sequence of ideals in A is stationary.

Proposition 1.3.4. If A is noetherian, every A-module of finite type is noetherian.

Proof. Let M be an A-module of finite type: there exists $n \in \mathbf{Z}_{\geqslant 0}$ and a surjective A-linear map $f\colon A^n \to M$. As A is noetherian, so is A^n (corollary 1.3.2), and $M = A^n/\mathsf{Ker}(f)$ (proposition 1.3.1 (2)). □

Example 1.3.5. (1) Let R be a ring and I an infinite set. The ring of polynomials $A = R[X_i]_{i\in I}$ is not noetherian: the ideal generated by $\{X_i\}_{i\in I}$ is not of finite type.

(2) Let $A = \mathbf{Z}[2X, 2X^2, 2X^3, \ldots] = \mathbf{Z} + 2X\,\mathbf{Z}[X] \subset \mathbf{Z}[X]$. Then A is not noetherian: the ideal I generated by $\{2X^i\}_{i\in\mathbf{Z}_{>0}}$ is not finitely generated. Indeed, the ring homomorphism $f\colon \mathbf{Z}[X_i]_{i\in\mathbf{Z}_{>0}} \to \mathbf{Z}[X]$ defined by $f(X_i) = 2X^i$ factors through an injective morphism $\mathbf{Z}[X_i]_{i\in\mathbf{Z}_{>0}}/\langle 2^{i-1}X_i - X_1^i\rangle_{i\in\mathbf{Z}_{>1}} \to \mathbf{Z}[X]$, inducing an isomorphism $\mathbf{Z}[X_i]_{i\in\mathbf{Z}_{>0}}/\langle 2^{i-1}X_i - X_1^i\rangle_{i\in\mathbf{Z}_{>1}} \xrightarrow{\sim} A$, hence an isomorphism $\mathbf{F}_2[X_i]_{i\in\mathbf{Z}_{>0}}/\langle X_1^2\rangle \xrightarrow{\sim} A/2A$: the image of I in $A/2A$ corresponds to the ideal generated by $\{X_i\}_{i\in\mathbf{Z}_{>0}}$: it is not finitely generated. Moreover, the ideal $\langle 2X\rangle \cap \langle 2X^2\rangle = \langle 4X^2, 4X^3, \ldots\rangle$ is not finitely generated: this gives an example of an intersection of two principal ideal which is not finitely generated (same reasoning as above).

Theorem 1.3.6. (Hilbert) If the ring A is noetherian, so is $A[X]$.

Proof. Let $I \subset A[X]$ be an ideal. For $n \in \mathbf{Z}_{\geqslant 0}$, let J_n denote the set of leading coefficients of elements in I which are of degree n. As I is an ideal in $A[X]$, the set J_n is an ideal in A. If $n \leqslant m$ and $a \in J_n$ (so that there exists $P \in I$ of degree n whose leading coefficient is a), then $a \in J_m$ (since a is the leading coefficient of $X^{m-n}P$): the sequence of ideals $(J_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ is ascending. As A is noetherian, this sequence is stationary: let $d \in \mathbf{Z}_{\geqslant 0}$ be such that $n \geqslant d \Rightarrow J_n = J_d$. As A is noetherian, the ideal J_d is of finite type: choose $\alpha_1, \ldots, \alpha_r$ generators of J_d, these are the leading coefficients of $P_1, \ldots, P_r \in J_d$ respectively. On the other hand, denote by $A[X]_{<d}$ the sub-A-module of $A[X]$ made of elements of degree $< d$, and put $M = I \cap A[X]_{<d}$. As $A[X]_{<d}$ is an A-module of finite type, it is noetherian (*cf* proposition 1.3.4), hence M is of finite type: let $Q_1, \ldots, Q_s$ be generators of M. We have of course

$$\alpha_1 A[X] + \cdots + \alpha_r A[X] + Q_1 A[X] + \cdots + Q_s A[X] \subset I$$

If $P \in I$ has degree $n \geqslant d$, its leading coefficient a belongs to J_d: there exists $a_1, \ldots, a_r \in A$ such that $a = a_a\alpha_1 + \cdots + a_r\alpha_r$. The polynomial $P - \sum\limits_{i=1}^{r} a_i X^{n-d} P_i \in I$ has degree $< n$: after subtracting an element of $\alpha_1 A[X] + \cdots + \alpha_r A[X]$ to P, we may assume $\deg(P) < d$. Then $P \in M = I \cap A[X]_{<d}$, hence $P \in Q_1 A[X] + \cdots + Q_s A[X]$, which shows that $P \in \alpha_1 A[X] + \cdots + \alpha_r A[X] + Q_1 A[X] + \cdots + Q_s A[X]$. The I is of finite type, and $A[X]$ is noetherian. □

Corollary 1.3.7. Let A be a noetherian ring and B an A-algebra of finite type. Then B is a noetherian ring.

Proof. As B is of finite type, there exist $b_1, \ldots, b_r \in B$ such that $B = A[b_1, \ldots, b_r]$: there is a surjective morphism of A-algebras $f\colon A[X_1, \ldots, X_r] \to B$ defined by $f(X_i) = b_i$ for $i \in \{1, \ldots, r\}$. Put $I = \mathsf{Ker}(f)$: we have $B \simeq A[X_1, \ldots, X_r]/I$. As A is noetherian, so is $A[X_1, \ldots, X_r]$ (apply theorem 1.3.6 r times), so that B is a noetherian $A[X_1, \ldots, X_r]$-algebra: it is a noetherian ring. □

1.4. **Modules of finite type over PIDs.** In this paragraph, we assume that A is a PID. The ring A is an integral domain: denote by K its fraction field. Recall that A is a UFD (*cf* proposition 1.1.26): there are gcd and lcm. Moreover, as ideals in A are generated by one element, A is noetherian.
In what follows, empty entries in a matrix correspond to zeros. If $n \in \mathbf{Z}_{>0}$ and $a_1, \ldots, a_n \in A$, we put

$$\mathsf{diag}(a_1, \ldots, a_n) = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \in \mathsf{M}_n(A).$$

Definition 1.4.1. If $n \in \mathbf{Z}_{>0}$, we put $\mathsf{GL}_n(A) = \{M \in \mathsf{M}_n(A)\,;\, \det(M) \in A^\times\}$. Cramer formulas imply that this is the group of units in the (non commutative) ring $\mathsf{M}_n(A)$ (note that the $\det(A) \neq 0$ is not enough). Put $\mathsf{SL}_n(A) = \{M \in \mathsf{M}_n(A)\,;\, \det(M) = 1\}$: this is a subgroup of $\mathsf{GL}_n(A)$.

Proposition 1.4.2. Let $n \in \mathbf{Z}_{\geqslant 2}$ and $a_1, \ldots, a_n$ be elements in A generating the unit ideal. Then there exists a matrix in $\mathsf{SL}_n(A)$ whose first row is $(a_1, \ldots, a_n)$.

Proof. Put $X = (a_1, \ldots, a_n)$: we have to build $M \in \mathsf{SL}_n(A)$ such that $XM^{-1} = (1, 0, \ldots, 0)$. We work by induction on $n \geqslant 2$.
Case $n = 2$. As $A = Aa_1 + Aa_2$, there exist $u, v \in A$ such that $va_1 - ua_2 = 1$. The matrix $M = \left(\begin{smallmatrix} a_1 & a_2 \\ u & v \end{smallmatrix}\right)$ does the job.
Case $n > 2$. Let $dA = \mathsf{gcd}(a_2, \ldots, a_n)$ and $b_2, \ldots, b_n \in A$ such that $db_i = a_i$ for $i \in \{2, \ldots, n\}$. We have $\mathsf{gcd}(b_2, \ldots, b_n) = A$: by induction, there exists $M_1' \in \mathsf{SL}_{n-1}(A)$ such that $YM_1'^{-1} = (1, 0, \ldots, 0)$ where $Y = (b_2, \ldots, b_n)$. Let

$$M_1 = \begin{pmatrix} 1 & \\ & M_1' \end{pmatrix}$$

We have $\det(M_1) = \det(M_1') = 1$ and $XM_1^{-1} = (a_1, d, 0, \ldots, 0)$. Use case $n = 2$: as $\mathsf{gcd}(a_1, d) = A$, there exists $M_2' \in \mathsf{SL}_2(A)$ with $(a_1, d)M_2^{-1} = (1, 0)$. Let

$$M_2 = \begin{pmatrix} M_2' & \\ & \mathrm{I}_{n-2} \end{pmatrix}$$

($\mathrm{I}_{n-2} \in \mathsf{SL}_{n-2}(A)$ is the unit matrix). We have $\det(M_2) = \det(M_2') = 1$ and $XM_1^{-1}M_2^{-1} = (1, 0, \ldots, 0)$, *i.e.* $XM^{-1} = (1, 0, \ldots, 0)$ with $M = M_2M_1 \in \mathsf{SL}_n(A)$. □

Remark 1.4.3. This proof provides an effective procedure to construct the matrix provided one can deal with the case $n = 2$ (which is the case, for instance, when A is euclidean).

Definition 1.4.4. If $n, m \in \mathbf{N}_{>0}$, we make the group $\mathsf{SL}_n(A) \times \mathsf{SL}_m(A)$ act on the A-module $\mathsf{M}_{n\times m}(A)$ by

$$(P, Q) \cdot M = P^{-1}MQ.$$

Two matrices $M_1, M_2 \in \mathsf{M}_{n\times m}(A)$ are *equivalent* if they are in the same orbit for this action. We write then $M_1 \sim M_2$ (this defines an equivalence relation). Note that we may also make $\mathsf{GL}_n(A) \times \mathsf{GL}_m(A)$ act in a similar way.

Remark 1.4.5. When $n = m$, one should not confuse this notion with the finer notion of similarity: two matrices $M_1, M_2 \in \mathsf{M}_n(A)$ are similar if there exists $P \in \mathsf{GL}_n(A)$ such that $M_2 = P^{-1}M_1P$.

Definition 1.4.6. A *reduced* matrix is a matrix of the form

$$\begin{pmatrix} \alpha_1 & & & \\ & \ddots & & \\ & & \alpha_r & \\ & & & \end{pmatrix} \in \mathsf{M}_{n\times m}(A)$$

with $r \in \{0, \ldots, \min\{m, n\}\}$ and $\alpha_1, \ldots, \alpha_r \in A\backslash\{0\}$ such that $\alpha_i \mid \alpha_{i+1}$ for all $i \in \{0, \ldots r-1\}$.

Notation. (1) Fix a family $(p_\lambda)_{\lambda\in\Lambda}$ of representatives of irreducible elements in A. Any element $a \in A\backslash\{0\}$ admits a unique decomposition as a product of irreducible factors:

$$a = u \prod_{\lambda\in\Lambda} p_\lambda^{n_\lambda}$$

where $u \in A^\times$ and $(n_\lambda)_{\lambda\in\Lambda}$ is a family of integers, all but finitely many being equal to zero. We put

$$\ell(a) = \sum_{\lambda\in\Lambda} n_\lambda \in \mathbf{Z}_{\geqslant 0}$$

that we call the *length* of a. This is nothing but the number of irreducible factors in a (for instance, we have $\ell(a) = 0 \Leftrightarrow a \in A^\times$ and $\ell(a) = 1$ if and only if A is irreducible). If $M = [m_{i,j}]_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}} \in \mathsf{M}_{n\times m}(A)\backslash\{0\}$, we put

$$\ell(M) = \min\big\{\ell(m_{i,j})\,;\, 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m,\ m_{i,j} \neq 0\big\}.$$

(2) If $\sigma \in \mathfrak{S}_n$ is a permutation, we put $P_\sigma = \big(\delta_{\sigma(i),j}\big)_{1\leqslant i,j\leqslant n} \in \mathsf{M}_n(A)$ (where $\delta_{i,j}$ is the Kronecker symbol). We have $\det(P_\sigma) = \varepsilon(\sigma)$ (where $\varepsilon(\sigma)$ is the signature of σ), so that $P_\sigma \in \mathsf{GL}_n(A)$. Put $\widetilde{P}_\sigma = \mathsf{diag}\big(1,\ldots,1,\varepsilon(\sigma)\big)P_\sigma \in \mathsf{SL}_n(A)$.
If $M \in \mathsf{M}_{n\times m}(A)$, the matrix $P_\sigma M$ is the element in $\mathsf{M}_{n\times m}(A)$ whose i-th row is the $\sigma(i)$-th row of M. Similarly, if $\gamma \in \mathfrak{S}_m$ is a permutation, the matrix MP_γ is deduced from M by permuting the columns according to γ. Multiplying M by $\widetilde{P}_\sigma$ on the left (resp. by $\widetilde{P}_\gamma$ on the right), permutes rows according to σ (resp. columns according to γ) and multiplies the last row (resp. column) by $\varepsilon(\sigma)$ (resp. $\varepsilon(\gamma)$).

Theorem 1.4.7. Every matrix $M \in \mathsf{M}_{n\times m}(A)$ is equivalent to a reduced matrix.

Proof. We may assume $M \neq 0$. We proceed by induction on $d = \min\{m,n\}$.
Assume $d = 1$. Transposing if necessary, we may assume $n = 1$, so that M is a row. If $m = 1$, there is nothing to do: assume $m \geqslant 2$. Let α_1 be the gcd of the coefficients of M: we have $M = \alpha_1 X$ where X is a row vector whose entries generate the unit ideal. By proposition 1.4.2, there exists $Q \in \mathsf{SL}_n(A)$ such that the first row of Q^{-1} is X. Then $XQ = (1,0,\ldots,0)$ thus $MQ = (\alpha_1,0,\ldots,0)$ is reduced.
Assume $d > 1$. Recall that $M \neq 0$. Let $\delta = \min\big\{\ell(M')\,;\, M' \sim M\big\} \in \mathbf{Z}_{\geqslant 0}$. Replacing M by an appropriate equivalent matrix, we may assume that $\ell(M) = \delta$. There exist $i_0 \in \{1,\ldots,n\}$ and $j_0 \in \{1,\ldots,m\}$ such that $\ell(m_{i_0,j_0}) = \delta$. Let $\tau_{1,i_0} \in \mathfrak{S}_n$ (resp. $\tau_{1,j_0} \in \mathfrak{S}_m$) be the transposition of $\{1,\ldots,n\}$ (resp. $\{1,\ldots,m\}$) that exchanges 1 and i_0 (resp. j_0), and put $M' = \widetilde{P}_{\tau_{1,i_0}}^{-1} M \widetilde{P}_{\tau_{1,j_0}} \in \mathsf{M}_{n\times m}(A)$ (where $\widetilde{P}_{\tau_{1,i_0}} \in \mathsf{SL}_n(A)$ and $\widetilde{P}_{\tau_{1,j_0}} \in \mathsf{SL}_m(A)$ are the modified permutation matrices, *cf* definition 1.4.1 (2)). We have $M' \sim M$ and $m'_{1,1} = m_{i_0,j_0}$: replacing M by M', we may assume that $\ell(m_{1,1}) = \delta$. Put $\alpha_1 := m_{1,1}$.
• We first show that α_1 divides the coefficients of the first row and of the first column of M. Transposing if necessary, it is enough to deal with the first column. Assume there exists $i \in \{2,\ldots,n\}$ such that $\alpha_1 \nmid m_{i,1}$. Exchanging the second and the i-th rows, we may assume $i = 2$. Let $\widetilde{\alpha}_1 = \mathsf{gcd}(\alpha_1, m_{2,1})$. As $\widetilde{\alpha}_1$ strictly divides α_1, we have $\ell(\widetilde{\alpha}_1) < \delta$. On the other hand, there exist $a,b \in A$ such that $\widetilde{\alpha}_1 = am_{1,1} + bm_{2,1}$. Put

$$P = \begin{pmatrix} a & b & & & \\ -m_{2,1}/\widetilde{\alpha}_1 & m_{1,1}/\widetilde{\alpha}_1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

We have $\det(P) = 1$ and the entry of index $(1,1)$ in $M' = PM$ is $\widetilde{\alpha}_1$: this implies that $M' \sim M$ and $\ell(M') \leqslant \ell(\widetilde{\alpha}_1) < \delta$, contradicting the definition of δ.
• Multiplying M on the left by the matrix

$$\begin{pmatrix} 1 & & & \\ -m_{2,1}/\alpha_1 & 1 & & \\ \vdots & & \ddots & \\ -m_{n,1}/\alpha_1 & & & 1 \end{pmatrix} \in \mathsf{SL}_n(A)$$

on the left, and by

$$\begin{pmatrix} 1 & -m_{1,2}/\alpha_1 & \cdots & -m_{1,m}/\alpha_1 \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \in \mathsf{SL}_m(A)$$

on the right, we may assume that $m_{i,1} = 0$ for $\in \{2,\ldots,n\}$ and $m_{1,j} = 0$ for $j \in \{2,\ldots,m\}$. Indeed this provides an equivalent matrix, with same length (the entry of index $(1,1)$ was not modified).
• The matrix M is now of the form

$$\begin{pmatrix} \alpha_1 & \\ & M_1 \end{pmatrix}$$

with $M_1 \in \mathsf{M}_{(n-1)\times(m-1)}(A)$. By induction hypothesis, there exist $P_1 \in \mathsf{SL}_{n-1}(A)$, $Q_1 \in \mathsf{SL}_{m-1}(A)$, $r \in \mathbf{N}$, and elements $\alpha_2,\ldots,\alpha_r \in A\backslash\{0\}$ such that $\alpha_i \mid \alpha_{i+1}$ for all $i \in \{2,\ldots,r-1\}$ and

$$P_1^{-1}M_1Q_1 = \begin{pmatrix} \alpha_2 & & \\ & \ddots & \\ & & \alpha_r \end{pmatrix}$$

Multiplying M by $\begin{pmatrix} 1 & \\ & P_1^{-1} \end{pmatrix} \in \mathsf{SL}_n(A)$ on the left and by $\begin{pmatrix} 1 & \\ & Q_1 \end{pmatrix} \in \mathsf{SL}_m(A)$ on the right, we may assume that

$$M = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_r \end{pmatrix}$$

It remains to check that $\alpha_1 \mid \alpha_2$. Assume the contrary. Let $\alpha'_1 = \mathsf{gcd}(\alpha_1,\alpha_2)$. As $\alpha_1 \nmid \alpha_2$, we have $\ell(\alpha'_1) < \ell(\alpha_1) = \delta$. There exist $a,b \in A$ such that $a\alpha_1 + b\alpha_2 = \alpha'_1$. The equality

$$\begin{pmatrix} 1 & \\ a & 1 \end{pmatrix}\begin{pmatrix} \alpha_1 & \\ & \alpha_2 \end{pmatrix}\begin{pmatrix} 1 & \\ b & 1 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \\ \alpha'_1 & \alpha_2 \end{pmatrix}$$

imply that there exists $M' = (m_{i,j})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} \in \mathsf{M}_{n\times m}(A)$ equivalent to M and such that $m'_{2,1} = \alpha'_1$: we have $\ell(M') \leqslant \ell(\alpha'_1) < \delta$, contradicting the definition of δ. □

Remark 1.4.8. (1) When A is *euclidean*, it is possible to make this statement constructive, using elementary operations.
(2) When A is a field, one recovers the well known fact that the orbits for the equivalence relation are characterized by the rank: every matrix M is equivalent to $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$ (where the number of 1 is $\mathsf{rk}(M)$).

Notation. Let $M \in \mathsf{M}_{n,m}(A)$. If $k \in \{0, \ldots, \min\{n, m\}\}$, let $I_k(M)$ be the ideal generated by the minors of order k of M (so this is the gcd of those minors). The sequence of ideals $(I_k(M))_{0 \leqslant k \leqslant \min\{n,m\}}$ is decreasing[(5)], and $I_k(M) = \{0\}$ if $k > \mathsf{rk}(M)$. These are called the *invariant factors* of M.

Lemma 1.4.9. Two matrices that are equivalent have the same invariant factors.

Proof. Let $M \in \mathsf{M}_{n,m}(A)$ and $P \in \mathsf{GL}_n(A)$. Put $M' = P^{-1}M$. Lines of M' are A-linear combinations of those of M: by multilinearity of the determinant, a minor of order k of M' is an A-linear combination of minors of M of order k. This implies that $I_k(M') \subset I_k(M)$. As $M = PM'$, we have also $I_k(M) \subset I_k(M')$, *i.e.* $I_k(M') = I_k(M)$. Similarly, we have $I_k(MQ) = I_k(M)$ for all $Q \in \mathsf{GL}_m(A)$ (using the fact that columns of MQ are A-linear combinations of those of M). □

Theorem 1.4.10. With the notations of theorem 1.4.7, we have $I_k(M) = \alpha_1 \cdots \alpha_k A$ for $k \in \{1, \ldots, r\}$ (where $r = \mathsf{rk}(M)$). In particular, the sequence of ideals $\alpha_1 A \supset \alpha_2 A \supset \cdots \supset \alpha_r A$ is unique.

Proof. By lemma 1.4.9, we have $I_k(M) = I_k(\mathsf{diag}(\alpha_1, \ldots, \alpha_r, 0, \ldots, 0)) = \alpha_1 \cdots \alpha_k A$ for $k \in \{1, \ldots, r\}$. □

Theorem 1.4.11. (Adapted basis theorem). Let M be a sub-A-module of an A-module L free of finite rank n. Then M is free, and there exists a basis $(e_1, \ldots, e_n)$ of L, an integer $r \leqslant n$ and $\alpha_1, \ldots, \alpha_r \in A \backslash \{0\}$ such that

$$\begin{cases} \alpha_i \mid \alpha_{i+1} & \text{for all } i \in \{0, \ldots r-1\} \\ (\alpha_1 e_1, \ldots, \alpha_r e_r) & \text{is a basis of } M. \end{cases}$$

Proof. As A is a PID, it is noetherian. As L is of finite type, it is noetherian (proposition 1.3.4): its sub-A-module M is of finite type as well. Choose a generating family $x_1, \ldots, x_m \in M$: we have an A-linear map

$$\begin{aligned} f\colon A^m &\to L \\ (a_1, \ldots, a_m) &\mapsto \sum_{j=1}^{m} a_j x_j \end{aligned}$$

whose image is nothing but M. After the choice of a basis $\mathfrak{B}$ of L, this map is given by an $n \times m$ matrix (whose j-th column consists in the coordinates of x_j in $\mathfrak{B}$). By theorem 1.4.7, this matrix is equivalent to a reduced matrix: after a change of bases in A^m and L, it has the form

$$\begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_r \end{pmatrix}$$

with $r \in \{0, \ldots, \min\{m, n\}\}$ and $\alpha_1, \ldots, \alpha_r \in A \backslash \{0\}$ such that $\alpha_i \mid \alpha_{i+1}$ for $i \in \{0, \ldots r-1\}$. Denote by $(e_1, \ldots, e_n)$ the new basis of L: the image M of f is then the free sub-A-module with basis $(\alpha_1 e_1, \ldots, \alpha_r e_r)$. □

Remark 1.4.12. The previous result is obviously false when A is not a PID. For instance $\mathbf{Z}/2\mathbf{Z}$ is a sub-$\mathbf{Z}/4\mathbf{Z}$-module of $\mathbf{Z}/4\mathbf{Z}$. Similarly, the sub-$\mathbf{Z} \times \mathbf{Z}$-module $\mathbf{Z} \times \{0\}$ of $\mathbf{Z} \times \mathbf{Z}$ is not free.

Theorem 1.4.13. (Invariant factor decomposition). Let M be an A-module of finite type. There exist integers $d, r \in \mathbf{Z}_{\geqslant 0}$ and $a_1, \ldots, a_d \in A \backslash (\{0\} \cup A^\times)$ such that

$$\begin{cases} a_i \mid a_{i+1} & \text{for all } i \in \{0, \ldots d-1\} \\ M \simeq (A/a_1 A) \times \cdots \times (A/a_d A) \times A^r \end{cases}$$

Moreover, the integers d, r and the ideals $a_1 A, \ldots, a_d A$ are unique. The integer r is called the *rank* of M and when $r = 0$, the elements $(a_1, \ldots, a_d)$ "the" *invariant factors* of M.

[(5)] This follows from the fact that minors of order k a linear combinations of minors of order $k-1$, as can be seen by developing determinant along the first row.

Proof. • We start with the existence. As M is of finite type, we can choose a generating family $m_1,\dots,m_n$: we have a surjective A-linear map

$$\begin{aligned} f\colon A^n &\to M \\ (\lambda_1,\dots,\lambda_n) &\mapsto \sum_{i=1}^n \lambda_i m_i. \end{aligned}$$

As A^n is free of finite rank, there is a basis $(e_1,\dots,e_n)$ such that

$$\mathsf{Ker}(f) = \bigoplus_{i=1}^s A\alpha_i e_i$$

with $s \in \{1,\dots,n\}$ and $\alpha_1,\dots,\alpha_s \in A\backslash\{0\}$ such that $\alpha_i \mid \alpha_{i+1}$ for all $i \in \{0,\dots s-1\}$ (*cf* theorem 1.4.11). Taking the quotient, f induces an A-linear isomorphism

$$M \simeq A^n/\mathsf{Ker}(f) = \Big(\bigoplus_{i=1}^s (A/\alpha_i A)e_i\Big) \oplus \Big(\bigoplus_{i=s+1}^n Ae_i\Big)$$

Let $t = \max\big\{i \in \{1,\dots,s\}\,;\, \alpha_i \in A^\times\big\}$ (we have $t=0$ if $\alpha_1 \notin A^\times$). Put $d = s-t$, $r = n-s$ and $a_i = \alpha_{t+i}$ for $i \in \{1,\dots,d\}$. We have $a_1,\dots,a_d \in A\backslash\big(\{0\}\cup A^\times\big)$ and $a_i \mid a_{i+1}$ for all $i \in \{0,\dots d-1\}$. Moreover, as

$$A/\alpha_i A = \begin{cases} 0 & \text{if } i \leqslant t \\ A/a_{i-t}A & \text{if } t < i \leqslant s \end{cases}$$

we have

$$M \simeq (A/a_1A) \times \cdots \times (A/a_dA) \times A^r.$$

• We now prove the unicity. We have $M_{\mathsf{tors}} = (A/a_1A) \times \cdots \times (A/a_dA)$ thus $M/M_{\mathsf{tors}} \simeq A^r$. The integer r thus depends only on M (*cf* proposition 1.2.16). We are thus reduced to the case where M is a torsion module. We have $M \simeq \prod\limits_{i=1}^d (A/a_iA)$ with $a_1 \mid a_2 \mid \cdots \mid a_d$ in $A\backslash\{0\}$. Let $\mathscr{P}$ be the set of irreducible elements in A. If $p \in \mathscr{P}$, the ideal pA is prime an non-zero, hence maximal[(6)]: the A-module M/pM is an A/pA-vector space of finite dimension $d_p(M)$ (we have $d_p(M) = \#\{i \in \{1,\dots,d\}\,;\, p \mid a_i\}$). This shows in particular that $d = d(M) := \max\limits_{p\in\mathscr{P}} d_p(M)$ only depends on M.

For all $n \in \mathbf{Z}_{\geqslant 0}$, we have $d_p(p^nM/p^{n+1}M) = \#\{i \in \{1,\dots,d\}\,;\, v_p(a_i) \geqslant n+1\}$. This implies that for all $n \in \mathbf{Z}_{>0}$, the integer

$$\#\{i \in \{1,\dots,d\}\,;\, v_p(a_i) = n\} = d_p(p^{n-1}M/p^nM) - d_p(p^nM/p^{n+1}M)$$

only depends on M and p. As $v_p(a_1) \leqslant v_p(a_2) \leqslant \cdots \leqslant v_p(a_d)$, this implies that for all $p \in \mathscr{P}$ and all $i \in \{1,\dots,d\}$, the integer $v_p(a_i)$ only depends on M and p. This means that the ideals a_iA only depend on M.

Remark: an other way to conclude.

Lemma 1.4.14. If $a,b \in A\backslash\{0\}$, we have $a(A/bA) \simeq A/\frac{b}{\mathsf{gcd}(a,b)}A$.

Proof. Write $a = \alpha\,\mathsf{gcd}(a,b)$ and $b = \beta\,\mathsf{gcd}(a,b)$: we have $\mathsf{gcd}(\alpha,\beta) = 1$. Let $\pi\colon A \to A/bA$ be the canonical projection. Then $a(A/bA)$ is the image of the composite $\pi\circ m_a$, where $m_a : A \to A$ is the multiplication by a. We have $x \in \mathsf{Ker}(\pi\circ m_a) \Leftrightarrow ax \in bA \Leftrightarrow \alpha x \in \beta A \Leftrightarrow x \in \beta A$ (because $\mathsf{gcd}(\alpha,\beta) = 1$). The surjective morphism $\pi\circ m_a : A \to a(A/ba)$ thus induces an isomorphism $A/\beta A \xrightarrow{\sim} a(A/bA)$. □

We prove the unicity of the ideals $\{a_iA\}_{1\leqslant i\leqslant d}$ by induction on d, the case $d=0$ being empty. Assume that $M \simeq \prod\limits_{i=1}^d (A/a_iA) \simeq \prod\limits_{i=1}^d (A/b_iA)$ with $a_1 \mid a_2 \mid \cdots \mid a_d$ and $b_1 \mid b_2 \mid \cdots \mid b_d$. Let $s = \max\{i \in \{1,\dots,d\}\,;\, a_iA = a_1A\}$. We have $a_1M \simeq \prod\limits_{i=s+1}^d a_1(A/a_iA) \simeq \prod\limits_{i=1}^d a_1(A/b_iA)$. By lemma 1.4.14, this means that $a_1M \simeq \prod\limits_{i=s+1}^d A/\frac{a_i}{a_1}A \simeq \prod\limits_{i=1}^d A/\frac{b_i}{\mathsf{gcd}(a_1,b_i)}A$. By unicity of $d(a_1M)$, this implies that $A/\frac{b_i}{\mathsf{gcd}(a_1,b_i)}A = \{0\}$, *i.e.* $b_iA = \mathsf{gcd}(a_1,b_i)A$ whence $a_1A \subset b_iA$ for all $i \in \{1,\dots,s\}$. Symmetrically, we also have $b_iA \subset a_1A$, so $a_iA = b_iA$ for $i \in \{1,\dots,s\}$. Moreover, we have $a_1M \simeq \prod_{i=s+1}^d A/\frac{a_i}{a_1}A \simeq \prod_{i=s+1}^d A/\frac{b_i}{a_1}A$: the induction hypothesis implies that $\frac{a_i}{a_1}A = \frac{b_i}{a_1}A$ and thus $a_iA = b_iA$ for all $i \in \{s+1,\dots,d\}$, finishing the proof. □

Corollary 1.4.15. A torsionfree A-module of finite type is free.

Corollary 1.4.16. The ideals $\alpha_1A,\dots,\alpha_rA$ in theorems 1.4.7 and 1.4.11 are unique.

[(6)] If A is a PID and $\mathfrak{p} \subset A$ is prime and non-zero, then $\mathfrak{p}$ is maximal. Indeed, let $\mathfrak{m} \supset \mathfrak{p}$ be a maximal ideal (*cf* Krull's theorem, *cf* theorem 1.1.7). As A is a PID, there exist $a,b \in A\backslash\{0\}$ such that $\mathfrak{p} = aA$ and $\mathfrak{m} = bA$. As $\mathfrak{p} \subset \mathfrak{m}$, we have $b \mid a$: there exists $c \in A$ such that $a = bc$. As $\mathfrak{p}$ is prime, we have $b \in \mathfrak{p}$ or $c \in \mathfrak{p}$. In the last case, there would exist $d \in A$ such that $c = ad$, whence $a = abd$ *i.e.* $bd = 1$ since A is a domain and $a \neq 0$. This would imply that $b \in A^\times$ *i.e.* $\mathfrak{m} = A$ which is not. We thus have $b \in \mathfrak{p}$, hence $\mathfrak{m} \subset \mathfrak{p}$ *i.e.* $\mathfrak{p} = \mathfrak{m}$ is maximal.

Proof. If $M = \bigoplus\limits_{i=1}^{r} A\alpha_i e_i \subset \bigoplus\limits_{i=1}^{n} Ae_i = L$, we have $L/M \simeq \bigoplus\limits_{i=1}^{r}(A/\alpha_i A)e_i \times A^{n-r}$. Let s be the number of indices $i \in \{1,\ldots,r\}$ such that $\alpha_i A = A$ (*i.e.* $\alpha_i \in A^\times$). We have $L/M \simeq (A/\alpha_{s+1}A)\times\cdots\times(A/\alpha_r A)\times A^{n-r}$. By theorem 1.4.13, the integers $r-s$ and $n-r$ and thus s only depend on L and M, and the ideals $\alpha_{s+1}A,\ldots,\alpha_r A$ as well, which implies unicity in theorem 1.4.11. This implies unicity in theorem 1.4.7. □

1.5. **Tensor product.** Let M and N be A-modules.

Definition 1.5.1. Let L be an A-module. A map $f\colon M\times N\to L$ is *bilinear* if it satisfies the following conditions:

(1) f is left-linear, *i.e.* $(\forall a\in A)\,(\forall m_1,m_2\in M)\,(\forall n\in N)\, f(am_1+m_2,n) = af(m_1,n)+f(m_2,n)$;
(2) f is right-linear, *i.e.* $(\forall a\in A)\,(\forall m\in M)\,(\forall n_1,n_2\in N)\, f(m,an_1+n_2) = af(m,n_1)+f(m,n_2)$.

The set $\mathsf{Bil}_A(M,N;L)$ of bilinear maps $M\times N\to L$ is an A-module.

Proposition 1.5.2. There exists a pair $(M\otimes_A N,\varphi)$ where $M\otimes_A N$ is an A-module and $\varphi\colon M\times N\to M\otimes_A N$ a bilinear map, having the following universal property: if $f\colon M\times N\to L$ is a bilinear map, there exists a unique A-linear map $\tilde f\colon M\otimes_A N\to L$ such that $f=\tilde f\circ\varphi$.

$$\begin{tikzcd}
M\times N \arrow[rr, "f"] \arrow[dr, "\varphi"'] & & L \\
& M\otimes_A N \arrow[ur, "\tilde f"'] &
\end{tikzcd}$$

Remark 1.5.3. (1) The universal property of the pair $(M\otimes_A N,\varphi)$ implies its unicity up to a unique isomorphism.
(2) One can slightly generalize the previous construction to cover the case where A may not be commutative (this is useful for representation theory for instance).

Proof. Consider the A-module $A^{(M\times N)}$ of maps $M\times N\to A$ having a finite support, and its canonical basis $\big(e_{(m,n)}\big)_{(m,n)\in M\times N}$. Let K be the submodule of $A^{(M\times N)}$ generated by the following elements:

- $e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)}$ for $m_1,m_2\in M$ and $n\in N$;
- $e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)}$ for $m\in M$ and $n_1,n_2\in N$;
- $e_{(am,n)} - ae_{(m,n)}$ and $e_{(m,an)} - ae_{(m,n)}$ for $a\in A$, $m\in M$ and $n\in N$.

Put $M\otimes_A N = A^{(M\times N)}/K$. Let $i\colon M\times N\to A^{(M\times N)}; (m,n)\mapsto e_{(m,n)}$ and $\pi\colon A^{(M\times N)}\to M\otimes_A N$ the canonical projection. Put $\varphi=\pi\circ i$: by definition of K, the map φ is bilinear. If $f\colon M\times N\to L$ is bilinear, we define an A-linear map $\hat f\colon A^{(M\times N)}\to L$ by $\hat f(e_{(m,n)}) = f(m,n)$ for all $m\in M$ and $n\in N$. As f is bilinear, we have $K\subset\mathsf{Ker}(\hat f)$: the map $\hat f$ factors through a map $\tilde f\colon M\otimes_A N\to L$, so that $f=\tilde f\circ\varphi$ (we have $\tilde f(\pi(e_{(m,n)})) = f(m,n)$ for all $m\in M$ and $n\in N$).

$$\begin{tikzcd}
M\times N \arrow[drr, bend left, "f"] \arrow[dr, "\varphi"] \arrow[dd, "i"'] & & \\
& M\otimes_A N \arrow[r, dashed, "\tilde f"] & L \\
A^{(M\times N)} \arrow[ur, "\pi"'] \arrow[urr, bend right, "\hat f"'] & &
\end{tikzcd}$$

□

Definition 1.5.4. $M\otimes_A N$ is called the *tensor product* of M and N over A.

Remark 1.5.5. (1) The universal property of tensor product means that there is a functorial isomorphism

$$\mathsf{Bil}(M,N;L)\simeq\mathsf{Hom}_A(M,\mathsf{Hom}_A(N,.))\simeq\mathsf{Hom}_A(M\otimes_A N,.)$$

(2) If M is an A-module and B an A-algebra, then $B\otimes_A M$ is endowed with a B-module structure (base change).

Notation. With notations of proposition 1.5.2, put $m\otimes n = \pi(e_{(m,n)})\in M\otimes_A N$ for all $m\in M$ and $n\in N$. Elements in $M\otimes_A N$ of this form are called *simple tensors.* They generate $M\otimes_A N$ as an A-module, but in general, all elements in $M\otimes_A N$ are not simple tensors.

Proposition 1.5.6. Let M be an A-module.
(1) If N is an A-module, there is an isomorphism $M\otimes_A N\xrightarrow{\sim}N\otimes_A M$ sending $x\otimes y$ to $y\otimes x$.
(2) If $(N_\lambda)_{\lambda\in\Lambda}$ is a family of A-modules, then $M\otimes_A\Big(\bigoplus\limits_{\lambda\in\Lambda}N_\lambda\Big)\simeq\bigoplus\limits_{\lambda\in\Lambda}(M\otimes_A N_\lambda)$ (distributivity of the tensor product).

Proof. Follow from the universal property of the tensor product. □

Proposition 1.5.7. If M and N are free, with bases $(e_\lambda)_{\lambda\in\Lambda}$ and $(f_\delta)_{\delta\in\Delta}$ respectively, then $M\otimes_A N$ is free, with base $(e_\lambda\otimes f_\delta)_{(\lambda,\delta)\in\Lambda\times\Delta}$.

Proof. Write $N=\bigoplus\limits_{\delta\in\Delta}Af_\delta$. By proposition 1.5.6 (2), we have $M\otimes_A N=\bigoplus\limits_{\delta\in\Delta}M\otimes_A Af_\delta$. Similarly, we have $M\otimes_A Af_\delta=\bigoplus\limits_{\lambda\in\Lambda}Ae_\lambda\otimes_A Af_\delta$. As $Ae_\lambda\otimes_A Af_\delta=Ae_\lambda\otimes f_\delta$, we get $M\otimes_A N=\bigoplus\limits_{\substack{\lambda\in\Lambda\\ \delta\in\Delta}}Ae_\lambda\otimes f_\delta$, whence the result. □

Functoriality of tensor product. Let $f\colon M\to M'$ and $g\colon N\to N'$ be two A-linear maps. They induce a map $M\times N\to M'\otimes_A N'; (m,n)\mapsto f(m)\otimes g(n)$. It is bilinear, so factors uniquely through an A-linear map

$$f\otimes g\colon M\otimes_A N\to M'\otimes_A N'.$$

In particular, if N an A-module, there is a natural A-linear map $M\otimes_A N\xrightarrow{f\otimes\mathsf{Id}_N}M'\otimes_A N$. An important special case is *base change*: if B is an A-algebra, f induces a B-linear map $B\otimes_A M\to B\otimes_A M'$.

Remark 1.5.8. If $f\colon M\to M'$ is an isomorphism, then $M\otimes_A N\xrightarrow{f\otimes\mathsf{Id}_N}M'\otimes_A N$ is an isomorphism. If f is only injective, then $M\otimes_A N\xrightarrow{f\otimes\mathsf{Id}_N}M'\otimes_A N$ may not be injective. If f is surjective, then $f\otimes\mathsf{Id}_N$ is surjective (even better, $\mathsf{Coker}(f\otimes\mathsf{Id}_N)\simeq\mathsf{Coker}(f)\otimes_A N$, see below).

Example 1.5.9. (1) $(\mathbf{Z}/a\mathbf{Z})\otimes_{\mathbf{Z}}(\mathbf{Z}/b\mathbf{Z})\simeq\mathbf{Z}/\mathsf{gcd}(a,b)\,\mathbf{Z}$ for all $a,b\in\mathbf{Z}_{>0}$.
(2) $(\mathbf{Q}/\mathbf{Z})\otimes_{\mathbf{Z}}(\mathbf{Q}/\mathbf{Z})=0$.
(3) $\mathbf{Q}\otimes_{\mathbf{Z}}\mathbf{Q}=\mathbf{Q}$.
(4) The maps $\mathbf{C}\otimes_{\mathbf{C}}\mathbf{C}\to\mathbf{C}$; $z_1\otimes z_2\mapsto z_1z_2$ and $\mathbf{C}\otimes_{\mathbf{R}}\mathbf{C}\to\mathbf{C}^2$; $z_1\otimes z_2\mapsto(z_1z_2,z_1\overline{z}_2)$ are isomorphisms.
(5) Let K be a field, V and W be K-vector spaces, and let $V^\vee=\mathsf{Hom}_K(V,K)$ be the dual of V. The map $W\otimes_K V^\vee\to\mathsf{Hom}_K(V,W)$ sending $w\otimes\alpha$ (with $w\in W$ and $\alpha\in V^\vee$) to the rank 1 linear map given by $x\mapsto\alpha(x)v$ is an isomorphism (because it is surjective since any element in $\mathsf{Hom}_K(V,W)$ can be written as a sum of rank 1 maps, and $\dim_K(W\otimes_K V^\vee)=\dim_K(V)\dim_K(W)=\dim_K(\mathsf{Hom}_K(V,W))$). In particular, one has $V\otimes_K V^\vee\xrightarrow{\sim}\mathsf{End}_K(V)$. Note that the map $V\otimes_K V^\vee\to K$; $v\otimes\alpha\mapsto\alpha(v)$ corresponds, *via* this isomorphism, to the trace map $\mathsf{Tr}\colon\mathsf{End}_K(V)\to K$.

1.5.10. *Tensor product of algebras.* Let B and C be A-algebras. The multiplication on B (resp. C) provides maps $m_B\colon B\otimes_A B\to B$; $x\otimes y\mapsto xy$ and $m_C\colon C\otimes_A C\to C$; $x\otimes y\mapsto xy$. Moreover, there is an isomorphism $\varepsilon\colon C\otimes_A B\xrightarrow{\sim}B\otimes_A C$; $x\otimes y\mapsto y\otimes x$. Consider the composite

$$\begin{tikzcd}
(B\otimes_A C)\otimes_A(B\otimes_A C) \arrow[r, "\mathsf{Id}_B\otimes\varepsilon\otimes\mathsf{Id}_C", "\sim"'] \arrow[rr, bend right=15, "\mu"'] & (B\otimes_A B)\otimes_A(C\otimes_A C) \arrow[r, "m_B\otimes m_C"] & B\otimes_A C
\end{tikzcd}$$

(here we tacitly used the natural isomorphisms $(B\otimes_A C)\otimes_A(B\otimes_A C)\xrightarrow{\sim}B\otimes_A(C\otimes_A B)\otimes_A C$ and $B\otimes_A(B\otimes_A C)\otimes_A C\xrightarrow{\sim}(B\otimes_A B)\otimes_A(C\otimes_A C)$ *i.e.* the associativity of tensor product).

Definition 1.5.11. The preceding map $\mu\colon(B\otimes_A C)\otimes_A(B\otimes_A C)\to B\otimes_A C$ endows the A-module $B\otimes_A C$ with an A-algebra structure: the product law is simply given by

$$(b_1\otimes c_1)\cdot(b_2\otimes c_2)=(b_1b_2)\otimes(c_1c_2)$$

on simple tensors. This A-algebra is called the *tensor product* of the A-algebras B and C.

Remark 1.5.12. Note that this construction is functorial.

There are natural morphisms of A-algebras $i_B\colon B\to B\otimes_A C$; $b\mapsto b\otimes 1_C$ and $i_C\colon C\to B\otimes_A C$; $c\mapsto 1_B\otimes c$.

Proposition 1.5.13. (Universal property of the tensor product of algebras). If X is an A-algebra, then

$$\mathsf{Hom}_{A\text{-alg}}(B\otimes_A C,X)=\big\{(f,g)\in\mathsf{Hom}_{A\text{-alg}}(B,X)\times\mathsf{Hom}_{A\text{-alg}}(C,X)\,;\,(\forall b\in B)\,(\forall c\in C)\,f(b)g(c)=g(c)f(b)\big\}$$

In particular, if B and C are commutative, the tensor product $(B\otimes_A C,i_B,i_C)$ is the *coproduct* of B and C in the category of *commutative* A-algebras.

$$\begin{tikzcd}
 & B \arrow[dr, "i_B"] \arrow[drr, bend left, "f"] & & \\
A \arrow[ur] \arrow[dr] & & B\otimes_A C \arrow[r, dotted] & X \\
 & C \arrow[ur, "i_C"'] \arrow[urr, bend right, "g"'] & &
\end{tikzcd}$$

Example 1.5.14. (1) $A[X_1,\ldots,X_n]\otimes_A B\simeq B[X_1,\ldots,X_n]$.
(2) If $I\subset B$ is an ideal and $\bar{I}\subset B\otimes_A C$ the ideal generated by $i_B(I)$, then $(B/I)\otimes_A C\simeq(B\otimes_A C)/\bar{I}$. For instance, assume that $P_1,P_2\in A:=\mathbf{C}[X,Y]$, and let $B=\mathbf{C}[X,Y]/\langle P_1\rangle$ and $C=\mathbf{C}[X,Y]/\langle P_2\rangle$. Then $B\otimes_A C\simeq\mathbf{C}[X,Y]/\langle P_1,P_2\rangle$. Geometrically, this corresponds to the functions on the intersection of the two curves defined by P_1 and P_2 in the affine plane $\mathbf{A}^2_{\mathbf{C}}$.
(3) (Example 1.5.9 (4) continued) Let L/K is a finite Galois extension with group G, the natural map $L\otimes_K L\to\bigoplus\limits_{\sigma\in G}L$; $x\otimes y\mapsto(x\sigma(y))_{\sigma\in G}$ is an isomorphism of L-algebras (for the left structure on the LHS, and the diagonal structure on the RHS). Indeed, choose a primitive element $\alpha\in L$ (*i.e.* such that $(1,\alpha,\alpha^2,\ldots,\alpha^{d-1})$ is a K-basis of L, where $d=[L:K]$), and let $P(X)=\prod\limits_{\sigma\in G}(X-\sigma(\alpha))\in K[X]$ be its minimal polynomial over K. Then $L\otimes_K L\simeq L\otimes_K K[X]/\langle P\rangle\simeq L[X]/\langle P\rangle\simeq\bigoplus\limits_{\sigma\in G}L$, the last map sending the class of X to $(\sigma(\alpha))_{\sigma\in G}$ (this is nothing but the Chinese remainder theorem). By L-linearity, it is obvious that the composite maps $x\otimes y$ to $(x\sigma(y))_{\sigma\in G}$ (remark: in down to earth terms, $(1\otimes\alpha^i)_{0\leqslant i<d}$ is an L-basis of $L\otimes_K L$, which is mapped to $((\sigma(\alpha)^i)_{0\leqslant i<d})_{\sigma\in G}$, which is an L-basis of $\bigoplus\limits_{\sigma\in G}L$ because the Vandermonde matrix $(\sigma(\alpha)^i)_{\substack{0\leqslant i<d\\ \sigma\in G}}\in\mathsf{M}_d(L)$ is invertible).

1.6. Tensor, symmetric and exterior algebras.

1.6.1. *Graded algebras.*

Definition 1.6.2. Let $A\to B$ be an A-algebra. A *grading* on B is a collection of sub-A-modules $\{B_n\}_{n\in\mathbf{Z}_{\geqslant0}}$ such that

- $B=\bigoplus\limits_{n=0}^{\infty}B_n$;
- $(\forall m,n\in\mathbf{Z}_{\geqslant0})\,B_nB_m\subset B_{n+m}$.

A *graded A-algebra* is an A-algebra endowed with a grading.

Remark 1.6.3. If $B=\bigoplus\limits_{n=0}^{\infty}B_n$ is a graded A-algebra, then B_0 is an A-algebra.

Example 1.6.4. • $B=A[X_1,\ldots,X_d]$ has a natural grading, for which B_n is the sub-A-module made of 0 and homogeneous polynomials of degree n.
• Idem for $A[\![X_1,\ldots,X_n]\!]$.

Remark 1.6.5. By analogy with the previous example, elements in B_n are sometimes called *homogeneous of degree n.*

Definition 1.6.6. Let $B=\bigoplus\limits_{n=0}^{\infty}B_n$ be a graded A-algebra. An ideal $I\subset B$ is called *graded* if $I=\bigoplus\limits_{n=0}^{\infty}(I\cap B_n)$.

Example 1.6.7. If $B=A[X]$ and $I=\langle 1+X\rangle\subset B$, then I is not graded (because $I\cap B_n=\{0\}$ for all $n\in\mathbf{Z}_{\geqslant0}$).

Proposition 1.6.8. If $B=\bigoplus\limits_{n=0}^{\infty}B_n$ is a graded A-algebra and $I\subset B$ an ideal generated by homogeneous elements, then I is graded.

Proof. Write $I=\sum\limits_{\lambda\in\Lambda}\beta_\lambda B$ with β_λ homogeneous of degree $n_\lambda\in\mathbf{Z}_{\geqslant0}$ for all $\lambda\in\Lambda$. Let $x\in I$: there exists $\lambda_1,\ldots,\lambda_r\in\Lambda$ and $b_1,\ldots,b_r\in B$ such that $x=\sum\limits_{k=1}^{r}\beta_{\lambda_k}b_k$. For $k\in\{1,\ldots,r\}$, write $b_k=\sum\limits_{n=0}^{\infty}b_{k,n}$ with $b_{k,n}\in B_n$, and $b_{k,n}=0$ for $n\gg0$: we have $x=\sum\limits_{n=0}^{\infty}x_n$ with $x_n=\sum\limits_{\substack{k\in\mathbf{Z}_{\geqslant0}\\ n_{\lambda_k}\leqslant n}}\beta_{\lambda_k}b_{k,n-n_{\lambda_k}}\in I\cap B_n$, so that $I\subset\bigoplus\limits_{n=0}^{\infty}(I\cap B_n)$. The reverse inclusion is trivial. □

Proposition 1.6.9. Let $B=\bigoplus\limits_{n=0}^{\infty}B_n$ be a graded A-algebra and $I\subset B$ a graded ideal. For $n\in\mathbf{Z}_{\geqslant0}$, let $(B/I)_n=(B_n+I)/I\simeq B_n/(I\cap B_n)$ be the image of B_n in B/I. Then $B/I=\bigoplus\limits_{n=0}^{\infty}(B/I)_n$, so that B/I is a graded A-algebra.

Proof. The map $B = \bigoplus_{n=0}^{\infty} B_n \to \bigoplus_{n=0}^{\infty} (B/I)_n$ is surjective (because $B_n \to (B/I)_n \simeq B_n/(I \cap B_n)$ is for each $n \in \mathbf{Z}_{\geqslant 0}$) and its kernel is $\bigoplus_{n=0}^{\infty} (I \cap B_n) = I$. □

Definition 1.6.10. Let $B = \bigoplus_{n=0}^{\infty} B_n$ and $C = \bigoplus_{n=0}^{\infty} C_n$ be graded A-algebras.

- A morphism of A-algebras $\varphi\colon B \to C$ is *graded* if $\varphi(B_n) \subset C_n$ for all $n \in \mathbf{Z}_{\geqslant 0}$.
- The tensor product algebra $B \otimes_A C$ is naturally graded by $(B \otimes_A C)_n = \bigoplus_{k=0}^{n} B_k \otimes_A C_{n-k}$.

Remark 1.6.11. As $B = \bigoplus_{n=0}^{\infty} B_n$ and $C = \bigoplus_{n=0}^{\infty} C_n$, we have $B \otimes_A C = \bigoplus_{n,m \in \mathbf{Z}_{\geqslant 0}} B_n \otimes_A C_m$ (*cf* proposition 1.5.6 (2)), so $B \otimes_A C = \bigoplus_{n=0}^{\infty} (B \otimes_A C)_n$. Moreover, if $0 \leqslant k \leqslant n$ and $0 \leqslant \ell \leqslant m$ are integers, and $x \in B_k$, $x' \in B_\ell$, $y \in C_{n-k}$ and $y' \in C_{m-\ell}$, we have $(x \otimes y)(x' \otimes y') = xx' \otimes yy' \in B_{k+\ell} \otimes_A C_{n+m-(k+\ell)} \subset (B \otimes_A C)_{n+m}$, so the previous definition makes sense.

1.6.12. *Tensor, symmetric and exterior algebras.* In this section M denotes an A-module. If $n \in \mathbf{Z}_{\geqslant 0}$, we put

$$M^{\otimes n} = \underbrace{M \otimes_A M \otimes_A \cdots \otimes_A M}_{n \text{ times}}.$$

(in particular $M^{\otimes 0} = A$ and $M^{\otimes 1} = M$).

Definition 1.6.13. The *tensor algebra* of M is

$$\mathsf{T}_A(M) := \bigoplus_{n=0}^{\infty} M^{\otimes n}$$

where the A-algebra structure is characterized by

$$(x_1 \otimes \cdots \otimes x_n) \otimes (y_1 \otimes \cdots \otimes y_m) \mapsto x_1 \otimes \cdots \otimes x_n \otimes y_1 \otimes \cdots \otimes y_m.$$

It is a graded A-algebra, the n-th graded piece being $M^{\otimes n}$.

Remark 1.6.14. In general, $\mathsf{T}_A(M)$ is *not* commutative.

Example 1.6.15. • If $M = Ax$ in free of rank 1, then $M^{\otimes n} = Ax^{\otimes n}$ is of rank 1 for all $n \in \mathbf{Z}_{\geqslant 0}$, and $\mathsf{T}_A(M) = \bigoplus_{n=0}^{\infty} Ax^{\otimes n} \simeq A[X]$ is isomorphic to the ring of polynomials in one variable X corresponding to $(0, x, 0, \ldots) \in \mathsf{T}_A(M)$.
• If $M = Ax \oplus Ay$ is free of rank 2, then $\mathsf{T}_A(M)$ is isomorphic to the free A-algebra on two indeterminates X and Y (that correspond to $(0, x, 0, \ldots)$ and $(0, y, 0, \ldots)$ respectively).

Definition 1.6.16. Let $I_s(M) \subset \mathsf{T}_A(M)$ (resp. $I_a(M) \subset \mathsf{T}_A(M)$) be the two-sided ideal generated by elements of the form $x_1 \otimes \cdots x_n - x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)}$ with $n \in \mathbf{Z}_{>0}$, $x_1, \ldots, x_n \in M$ and $\sigma \in \mathfrak{S}_n$ (resp. of the form $x_1 \otimes \cdots \otimes x_n$ where $n \in \mathbf{Z}_{\geqslant 2}$ and $x_1, \ldots, x_n \in M$ are such that there exist $1 \leqslant i < j \leqslant n$ such that $x_i = x_j$).

Remark 1.6.17. As $\mathfrak{S}_n$ is generated by transpositions, a set of generators for $I_s(M)$ (resp. $I_a(M)$) is given by $\{x \otimes y - y \otimes x\}_{x,y \in M}$ (resp. $\{x \otimes x\}_{x \in M}$).

Being generated by homogeneous elements, the ideals $I_s(M)$ and $I_a(M)$ of $\mathsf{T}_A(M)$ are graded.

Definition 1.6.18. The *symmetric algebra* (resp. *exterior algebra*) of M is

$$\mathsf{Sym}_A(M) := \mathsf{T}_A(M)/I_s(M) \quad (\text{resp. } \mathsf{Alt}_A(M) = \mathsf{T}_A(M)/I_a(M))$$

By proposition 1.6.9, these are graded A-algebras: $\mathsf{Sym}_A(M) = \bigoplus_{n=0}^{\infty} \mathsf{Sym}_A^n(M)$ and $\mathsf{Alt}_A(M) = \bigoplus_{n=0}^{\infty} \mathsf{Alt}_A^n(M)$ where $\mathsf{Sym}_A^n(M) = M^{\otimes n}/(I_s(M) \cap M^{\otimes n})$ and $\mathsf{Alt}_A^n(M) = M^{\otimes n}/(I_a(M) \cap M^{\otimes n})$.

Remark 1.6.19. (1) As A-algebras, $\mathsf{Sym}_A(M)$ and $\mathsf{Alt}_A(M)$ are generated by $\mathsf{Sym}_A^1(M) = \mathsf{Alt}_A^1(M) = M$. As A is commutative, this implies in particular that the ring $\mathsf{Sym}_A(M)$ is commutative, and that the graded A-algebra $\mathsf{Alt}_A(M)$ is *anticommutative*, which means that $yx = (-1)^{nm}xy$ if $x \in \mathsf{Alt}_A^n(M)$ and $y \in \mathsf{Alt}_A^m(M)$.
(2) These constructions are functorial: an A-linear map $f\colon M \to M'$ induces morphisms of A-algebras $\mathsf{T}_A(f)\colon \mathsf{T}_A(M) \to \mathsf{T}_A(M')$, $\mathsf{Sym}_A(f)\colon \mathsf{Sym}_A(M) \to \mathsf{Sym}_A(M')$ and $\mathsf{Alt}_A(f)\colon \mathsf{Alt}_A(M) \to \mathsf{Alt}_A(M')$.
(3) Base change: if B is a commutative A-algebra and M an A-module, then $\mathsf{T}_B(B \otimes_A M) \simeq B \otimes_A \mathsf{T}_A(M)$, $\mathsf{Sym}_B(B \otimes_A M) \simeq B \otimes_A \mathsf{Sym}_A(M)$ and $\mathsf{Alt}_B(B \otimes_A M) \simeq B \otimes_A \mathsf{Alt}_A(M)$.

Definition 1.6.20. The A-module $\mathsf{Sym}^n_A(M)$ (resp. $\mathsf{Alt}^n_A(M)$) is called the n-th *symmetric power* (resp. *exterior power*) of M.

Notation. • Quite often, $\mathsf{Alt}^n_A(M)$ is denoted by $\bigwedge^n_A M$.
• Let $t\colon M^n \to M^{\otimes n}$; $(x_1, \ldots, x_n) \mapsto x_1 \otimes \cdots \otimes x_n$ and $s\colon M^n \to \mathsf{Sym}^n_A(M)$ (resp. $a\colon M^n \to \mathsf{Alt}^n_A(M)$) be the composite of t with the natural projection. Then one writes $x_1 \cdot x_2 \cdots x_{k-1} \cdot x_n$ instead of $s(x_1, \ldots, x_n)$ and $x_1 \wedge \cdots \wedge x_n$ instead of $a(x_1, \ldots, x_n)$.

Example 1.6.21. • If $M = Ax$ in free of rank 1, then $\mathsf{Sym}_A(M) = \mathsf{T}_A(M) \simeq A[X]$, and $\mathsf{Alt}_A(M) = A \oplus Ax$.
• If $M = Ax \oplus Ay$ is free of rank 2, then $\mathsf{Sym}_A(M) \simeq A[X, Y]$, and $\mathsf{Alt}_A(M) = A \oplus Ax \oplus Ay \oplus Ax \wedge y$ is free of rank 4.

Definition 1.6.22. Let L be an A-module and $n \in \mathbf{Z}_{>0}$. A map $f\colon M^n \to L$ is *n-linear* if it is A-linear with respect to each of its variables. A n-linear map $f\colon M^n \to L$ is *symmetric* (resp. *alternating*) if $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$ for all $x_1, \ldots, x_n \in M$ and $\sigma \in \mathfrak{S}_n$ (resp. $f(x_1, \ldots, x_n) = 0$ as soon as there are $1 \leqslant i < j \leqslant n$ such that $m_i = m_j$).

Remark 1.6.23. If $f\colon M^n \to L$ is an alternating n-linear map, then f it is antisymmetric, *i.e.*

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \varepsilon(\sigma) f(x_1, \ldots, x_n)$$

for all $x_1, \ldots, x_n \in M$ and $\sigma \in \mathfrak{S}_n$. When $2 \in A^\times$, the converse holds, *i.e.* an antisymmetric map is alternating.

Proposition 1.6.24. The n-linear map $t\colon M^n \to M^{\otimes n}$ (resp $s\colon M^n \to \mathsf{Sym}^n_A(M)$, resp. $a\colon M^n \to \mathsf{Alt}^n_A(M)$) has the following universal property: if $f\colon M^n \to L$ is a n-linear map (resp. a symmetric, resp. an alternating n-linear map), then there exists a unique A-linear map $\tilde{f}\colon M^{\otimes n} \to L$ (resp. $\tilde{f}\colon \mathsf{Sym}^n_A(M) \to L$, resp. $\tilde{f}\colon \mathsf{Alt}^n_A(M) \to L$) such that $f = \tilde{f} \circ t$ (resp. $f = \tilde{f} \circ s$, resp. $f = \tilde{f} \circ a$), *i.e.* such that the diagram

$$\begin{tikzcd}
M^n \arrow[rr, "f"] \arrow[dr, "t"'] & & L & \text{(resp. } M^n \arrow[rr, "f"] \arrow[dr, "s"'] & & L\ , & \text{resp. } M^n \arrow[rr, "f"] \arrow[dr, "a"'] & & L\ ) \\
& M^{\otimes n} \arrow[ur, "\tilde{f}"'] & & & \mathsf{Sym}^n_A(M) \arrow[ur, "\tilde{f}"'] & & & \mathsf{Alt}^n_A(M) \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$

commutes.

Proof. By the universal property of tensor product, there exists a unique A-linear map $\breve{f}\colon M^{\otimes n} \to L$ such that $f = \breve{f} \circ t$. By definition, f is symmetric (resp. alternating) if and only if $I_s(M) \cap M^{\otimes n} \subset \mathsf{Ker}(\breve{f})$ (resp. $I_a(M) \cap M^{\otimes n} \subset \mathsf{Ker}(\breve{f})$), *i.e.* if and only if the map $\breve{f}$ factorizes through an A-linear map $\tilde{f}\colon \mathsf{Sym}^n_A(M) \to L$ (resp. $\tilde{f}\colon \mathsf{Alt}^n_A(M) \to L$). □

Proposition 1.6.25. (Universal property of the symmetric algebra). Let $f\colon A \to B$ be a commutative A-algebra. The map

$$\mathsf{Hom}_{A\text{-alg}}(\mathsf{Sym}_A(M), B) \to \mathsf{Hom}_{A\text{-mod}}(M, B)$$

is bijective. In other words, any A-linear map $\psi\colon M \to B$ extends uniquely into a morphism of A-algebras $\widehat{\psi}\colon \mathsf{Sym}_A(M) \to B$.

$$\begin{tikzcd}
M \arrow[rr, "\psi"] \arrow[dr] & & B \\
& \mathsf{Sym}_A(M) \arrow[ur, dotted, "\widehat{\psi}"'] &
\end{tikzcd}$$

Proof. If $h\colon \mathsf{Sym}_A(M) \to B$ is a morphism of A-algebras, and $\psi = h_{|M}$, then ψ is A-linear, and for $n \in \mathbf{Z}$, we have

$$h(x_1 \cdot x_2 \cdots x_n) = \psi(x_1)\psi(x_2)\cdots\psi(x_n)$$

for all $x_1, \ldots, x_n \in M$, which implies that h is entirely determined by ψ (we are just using the fact that M generates $\mathsf{Sym}_A(M)$ as an A-algebra). This shows that the map $\mathsf{Hom}_{A\text{-alg}}(\mathsf{Sym}_A(M), B) \to \mathsf{Hom}_{A\text{-mod}}(M, B)$ is well defined and injective.
Let $\psi \in \mathsf{Hom}_{A\text{-mod}}(M, B)$. If $n \in \mathbf{Z}_{\geqslant 0}$, the map $M^n \to B$; $(x_1, \ldots, x_n) \mapsto \psi(x_1)\psi(x_2)\cdots\psi(x_n)$ is n-linear, so factors through a map $\widehat{h}_n\colon M^{\otimes n} \to B$. The map $\widehat{h} = \bigoplus\limits_{n=0}^{\infty} \widehat{h}_n\colon \mathsf{T}(M) \to B$ is a morphism of A-algebras. As B is commutative, we have $I_s(M) \subset \mathsf{Ker}(\widehat{h})$, so $\widehat{h}$ factors through a morphism of A-algebras $h\colon \mathsf{Sym}_A(M) \to B$ such that $h_{|M} = \psi$, which shows the surjectivity of $\mathsf{Hom}_{A\text{-alg}}(\mathsf{Sym}_A(M), B) \to \mathsf{Hom}_{A\text{-mod}}(M, B)$. □

Similarly:

Proposition 1.6.26. (Universal property of the exterior algebra). Let $f\colon A\to B$ be an anticommutative A-algebra. The map

$$\mathsf{Hom}_{A\text{-alg}}(\mathsf{Alt}_A(M),B)\to\mathsf{Hom}_{A\text{-mod}}(M,B)$$

is bijective. In other words, any A-linear map $\psi\colon M\to B$ extends uniquely into a morphism of A-algebras $\widehat{\psi}\colon\ \mathsf{Alt}_A(M)\to B$.

$$\begin{tikzcd} M \arrow[rr, "\psi"] \arrow[dr] & & B \\ & \mathsf{Alt}_A(M) \arrow[ur, dotted, "\widehat{\psi}"'] & \end{tikzcd}$$

Corollary 1.6.27. Let M_1 and M_2 be A-modules. There are natural isomorphisms

$$\mathsf{Sym}_A(M_1)\otimes_A\mathsf{Sym}_A(M_2)\simeq\mathsf{Sym}_A(M_1\oplus M_2)$$
$$\mathsf{Alt}_A(M_1)\otimes_A\mathsf{Alt}_A(M_2)\simeq\mathsf{Alt}_A(M_1\oplus M_2)$$

Proof. Let $f\colon A\to B$ be an A-algebra. Assume B is commutative: we have natural bijections

$$\begin{aligned}\mathsf{Hom}_{A\text{-alg}}(\mathsf{Sym}_A(M_1\oplus M_2),B)&\simeq\mathsf{Hom}_{A\text{-mod}}(M_1\oplus M_2,B)\\&\simeq\mathsf{Hom}_{A\text{-mod}}(M_1,B)\times\mathsf{Hom}_{A\text{-mod}}(M_2,B)\\&\simeq\mathsf{Hom}_{A\text{-alg}}(\mathsf{Sym}_A(M_1),B)\times\mathsf{Hom}_{A\text{-alg}}(\mathsf{Sym}_A(M_2),B)\\&\simeq\mathsf{Hom}_{A\text{-alg}}(\mathsf{Sym}_A(M_1)\otimes_A\mathsf{Sym}_A(M_2),B)\end{aligned}$$

by the universal property of symmetric algebras and tensor product of A-algebras. Since this holds for any commutative A-algebra B, we get an isomorphism $\mathsf{Sym}_A(M_1\oplus M_2)\simeq\mathsf{Sym}_A(M_1)\otimes_A\mathsf{Sym}_A(M_2)$. The case of the exterior algebra is similar. □

Remark 1.6.28. If $n,k\in\mathbf{Z}_{\geqslant 0}$ and $x_1,\dots,x_k\in M_1$, $y_1,\dots,y_{n-k}\in M_2$, then

$$x_1\otimes\cdots x_k\otimes y_1\otimes\cdots\otimes y_{n-k}\in(M_1\oplus M_2)^{\otimes n}$$

so we get a map

$$\bigoplus_{k=0}^{k}M_1^{\otimes k}\otimes_A M_2^{\otimes n-k}\to(M_1\oplus M_2)^{\otimes n}$$

This map is *not* an isomorphism in general. For instance, using proposition 1.5.6 (2) we have

$$(M_1\oplus M_2)^{\otimes 2}=M_1^{\otimes 2}\oplus M_1\otimes_A M_2\oplus M_2\otimes_A M_1\oplus M_2^{\otimes 2}$$

and the factor $M_2\otimes_A M_1$ is not included in the image.
If we add all those maps, we get a graded morphism of A-algebras

$$\mathsf{T}_A(M_1)\otimes_A\mathsf{T}_A(M_2)\to\mathsf{T}_A(M_1\oplus M_2)$$

(which is *not* an isomorphism in general). It induces graded morphisms of A-algebras

$$\mathsf{Sym}_A(M_1)\otimes_A\mathsf{Sym}_A(M_2)\xrightarrow{\sim}\mathsf{Sym}_A(M_1\oplus M_2)\qquad\mathsf{Alt}_A(M_1)\otimes_A\mathsf{Alt}_A(M_2)\xrightarrow{\sim}\mathsf{Alt}_A(M_1\oplus M_2)$$

which are nothing but those provided by corollary 1.6.27.

Considering the graded pieces of the graded isomorphisms of corollary 1.6.27, we get A-linear isomorphisms:

$$\bigoplus_{k=0}^{n}\mathsf{Sym}_A^k(M_1)\otimes_A\mathsf{Sym}_A^{n-k}(M_2)\xrightarrow{\sim}\mathsf{Sym}_A^n(M_1\oplus M_2)$$
$$\bigoplus_{k=0}^{n}\mathsf{Alt}_A^k(M_1)\otimes_A\mathsf{Alt}_A^{n-k}(M_2)\xrightarrow{\sim}\mathsf{Alt}_A^n(M_1\oplus M_2).$$

Corollary 1.6.29. Assume $M=\bigoplus\limits_{k=1}^{d}Ax_k$ is free of rank d.
(1) We have $\mathsf{Sym}_A(M)\simeq A[X_1,\dots,X_d]$ (where X_k corresponds to the image of $(0,x_k,0,\dots)\in\mathsf{T}(M)$), so in particular $\mathsf{Sym}_A^n(M)$ is a free module of rank $\binom{n+d-1}{n}$ (a basis being given by homogeneous monomials of degree n).
(2) The A-module $\mathsf{Alt}_A^n(M)$ is free of rank $\binom{d}{n}$ with basis $(x_{i_1}\wedge\cdots\wedge x_{i_n})_{0<i_1<\cdots<i_n\leqslant d}$, so $\mathsf{Alt}_A(M)$ is free of rank 2^d.

Proof. The case $d=1$ is nothing but example 1.6.21. The general case follows by induction, using corollary 1.6.27 for the symmetric algebra, and the second isomorphism above for the exterior power. □

Definition 1.6.30. Let M be a free A-module of rank d and $f \in \mathsf{End}_A(M)$. By functoriality, f induces an A-linear endomorphism $\mathsf{Alt}_A^d(f)\colon \mathsf{Alt}_A^d(M) \to \mathsf{Alt}_A^d(M)$, which is the multiplication by a scalar $\det(f) \in A$ since $\mathsf{Alt}_A^d(M)$ is free of rank 1 over A by corollary 1.6.29 (2). This scalar is called the *determinant* of f.

Remark 1.6.31. This definition matches the "usual" one: let $\mathfrak{B} = (e_1, \ldots, e_d)$ be a basis of M and $(\alpha_{i,j})_{1 \leqslant i,j \leqslant d} \in \mathsf{M}_d(A)$ the matrix of f in $\mathfrak{B}$, so that $f(e_i) = \sum\limits_{j=1}^{d} \alpha_{i,j} e_j$. We have $\mathsf{Alt}_A^d(M) = A\mathbf{e}$ where $\mathbf{e} = e_1 \wedge \cdots \wedge e_d$, so that:

$$\begin{aligned}
\mathsf{Alt}_A^d(f)(\mathbf{e}) &= \Big(\sum_{j=1}^{d} \alpha_{1,j} e_j\Big) \wedge \cdots \wedge \Big(\sum_{j=1}^{d} \alpha_{n,j} e_j\Big) \\
&= \sum_{1 \leqslant j_1, \ldots, j_d \leqslant d} \alpha_{1,j_1} \alpha_{2,j_2} \cdots \alpha_{d,j_d} \underbrace{e_{j_1} \wedge e_{j_2} \wedge \cdots \wedge e_{j_n}}_{=0 \text{ if } j_k = j_\ell \text{ with } k \neq \ell} \\
&= \sum_{\sigma \in \mathfrak{S}_d} \alpha_{1,\sigma(1)} \cdots \alpha_{d,\sigma(d)} \underbrace{e_{\sigma(1)} \wedge \cdots \wedge e_{\sigma(d)}}_{\varepsilon(\sigma)\mathbf{e}} \\
&= \Big(\sum_{\sigma \in \mathfrak{S}_d} \varepsilon(\sigma) \alpha_{1,\sigma(1)} \cdots \alpha_{d,\sigma(d)}\Big)\mathbf{e}
\end{aligned}$$

1.6.32. *Symmetric and anti-symmetric tensors.* Assume from now on that $n \in \mathbf{Z}_{\geqslant 2}$ and that $n! \in A^\times$. If $x_1, \ldots, x_n \in M^n$, put $f_s(x_1, \ldots, x_n) = \sum\limits_{\sigma \in \mathfrak{S}_n} x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)}$. This defines a map $f_s\colon M^n \to M^{\otimes n}$ which is n-linear and symmetric: it factors uniquely through an A-linear map $\iota_s\colon \mathsf{Sym}_A^n(M) \to M^{\otimes n}$ (the *symmetrization operator*). Likewise, put $f_a(m_1, \ldots, m_n) = \sum\limits_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(n)}$: this defines a map $f_a\colon M^n \to M^{\otimes n}$ which is n-linear and antisymmetrical (whence alternating given the hypothesis): it factors uniquely through an A-linear map $\iota_a\colon \mathsf{Alt}_A^n(M) \to M^{\otimes n}$ (the *anti-symmetrization operator*).
Endow $M^{\otimes n}$ with the action of $\mathfrak{S}_n$ given by $\sigma(m_1 \otimes \cdots \otimes m_n) = m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(n)}$. Then $\frac{1}{n!}\iota_s \circ \pi_s$ (where $\pi_s\colon M^{\otimes n} \to \mathsf{Sym}_A^n(M)$ is the canonical map) is a projector onto the subspace $\big(M^{\otimes n}\big)^{\mathfrak{S}_n}$ (of invariants under the action of $\mathfrak{S}_n$). Similarly, $\frac{1}{n!}\iota_a \circ \pi_a$ (where $\pi_a\colon M^{\otimes n} \to \mathsf{Alt}_A^n(M)$ is the canonical map) is a projector onto the subspace of anti-invariants, *i.e.* elements $x \in M^{\otimes n}$ such that $\sigma(x) = \varepsilon(\sigma)x$ for all $\sigma \in \mathfrak{S}_n$.

Remark 1.6.33. When $n = 2$, the previous projectors provide a decomposition $M^{\otimes 2} = \mathsf{Sym}_A^2(M) \oplus \mathsf{Alt}_A^2(M)$. Indeed, as $2 \in A^\times$ we have $(S(M) \cap M^{\otimes 2}) \oplus (A(M) \cap M^{\otimes 2}) = M^{\otimes 2}$ and they provide identifications $\mathsf{Sym}_A^2(M) = A(M) \cap M^{\otimes 2}$ and $\mathsf{Alt}_A^2(M) = S(M) \cap M^{\otimes 2}$.

1.7. Flatness.

Definition 1.7.1. • A *complex* of A-modules is a sequence of A-linear maps $\big(f_i\colon M_i \to M_{i+1}\big)_{i \in I}$ (where $I \subset \mathbf{Z}$ is an interval) such that $f_{i+1} \circ f_i = 0$ for all $i \in I$. It is *exact* when $\mathsf{Ker}(f_{i+1}) = \mathsf{Im}(f_i)$ for all $i \in I$.
• A *short exact sequence* of A-modules is an exact complex of the form

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

Remark 1.7.2. If $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact, then $M' \simeq \mathsf{Ker}(g)$ and $M'' \simeq \mathsf{Coker}(g)$.

Proposition 1.7.3. Let

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{♣}$$

be a diagram of A-modules. Then (♣) is an exact sequence if and only if for any A-module N, the sequence

$$0 \to \mathsf{Hom}_A(M'', N) \xrightarrow{\circ g} \mathsf{Hom}_A(M, N) \xrightarrow{\circ f} \mathsf{Hom}_A(M', N) \tag{♠}$$

is exact.

Proof. The exactness of the sequence (♠) for all A-module N means that for any A-linear map $v\colon M \to N$, the composite $v \circ f$ is zero if and only if v factors through g, *i.e.* if and only if there exists a (unique) A-linear map $u\colon M'' \to N$ such that $v = u \circ g$, which precisely means that $g\colon M \to M''$ has the universal property of the cokernel of f. This is thus equivalent to the exactness of (♣). □

Remark 1.7.4. (1) Proposition 1.7.3 implies in particular that if N is an A-module, the functor

$$\mathsf{Hom}_A(.,N)\colon \mathbf{Mod}(A) \to \mathbf{Mod}(A)$$

is left exact.

(2) Similarly, a diagram of A-modules $0 \to M' \xrightarrow{f} M \xrightarrow{g} M''$ is an exact sequence if and only if for any A-module N, the sequence $0 \to \mathsf{Hom}_A(N, M') \xrightarrow{f\circ} \mathsf{Hom}_A(N, M) \xrightarrow{g\circ} \mathsf{Hom}_A(N, M'')$ is exact. This implies in particular that for any A-module N, the functor $\mathsf{Hom}_A(N, .)\colon \mathbf{Mod}(A) \to \mathbf{Mod}(A)$ is left exact.

Proposition 1.7.5. Let N be an A-module. The functor $\mathbf{Mod}(A) \to \mathbf{Mod}(A)$; $M \mapsto M \otimes_A N$ is right exact. This means that if $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is an exact sequence of A-modules, then the complex

$$M' \otimes_A N \xrightarrow{f\otimes \mathsf{Id}_N} M \otimes_A N \xrightarrow{g\otimes \mathsf{Id}_N} M'' \otimes_A N \to 0$$

is exact.

Proof. By proposition 1.7.3, it is enough to check the exactness of the sequence

$$0 \to \mathsf{Hom}_A(M'' \otimes_A N, L) \to \mathsf{Hom}_A(M \otimes_A N, L) \to \mathsf{Hom}_A(M' \otimes_A N, L)$$

i.e. that of the sequence

$$0 \to \mathsf{Bil}_A(M'', N; L) \to \mathsf{Bil}_A(M, N; L) \to \mathsf{Bil}_A(M', N; L)$$

for any A-module L. This is trivial: an element φ lies in the kernel of $\mathsf{Bil}_A(M, N; L) \to \mathsf{Bil}_A(M', N; L)$ if and only if $\varphi(., y)$ vanishes on M' hence factors through M'' for all $y \in N$, *i.e.* if and only if $\varphi = \psi \circ (g \otimes \mathsf{Id}_N)$ for some unique $\psi \in \mathsf{Bil}_A(M'', N; L)$. □

Example 1.7.6. The sequence $0 \to \mathbf{Z} \xrightarrow{2} \mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0$ is exact. After tensoring by $\mathbf{Z}/2\mathbf{Z}$, we get the sequence

$$0 \to \mathbf{Z}/2\mathbf{Z} \xrightarrow{2=0} \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0.$$

Definition 1.7.7. An A-module N is called *flat* if the functor $\mathbf{Mod}(A) \to \mathbf{Mod}(A)$; $M \mapsto M \otimes_A N$ is exact, that is if for all exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$, the complex

$$0 \to M' \otimes_A N \xrightarrow{f\otimes \mathsf{Id}_N} M \otimes_A N \xrightarrow{g\otimes \mathsf{Id}_N} M'' \otimes_A N \to 0$$

is a short exact sequence.

Remark 1.7.8. By proposition 1.7.5, N is flat if and only if $M' \otimes_A N \xrightarrow{f\otimes \mathsf{Id}_N} M \otimes_A N$ is injective whenever $M' \to M$ is injective.

Proposition 1.7.9. An A-module N is flat over A if and only if for all ideal $I \subset A$ of finite type, the natural map $I \otimes_A N \to IN$ is injective.

Proof. • Assume N is flat over A. As $I \to A$ is injective, so is $I \otimes_A N \to N$.

• Conversely, assume that the natural map $I \otimes_A N \to IN$ is injective for every ideal of finite type $I \subset A$. Let $I \subset A$ be *any* ideal. An element $\xi \in \mathsf{Ker}(I \otimes_A N \to IN)$ can be written $\xi = \sum\limits_{k=1}^{r} \alpha_i \otimes x_i$ with $\alpha_1, \dots, \alpha_r \in I$ and $x_1, \dots, x_r \in N$. Let $J \subset A$ be the ideal generated by $\alpha_1, \dots, \alpha_r$, so that $\xi \in \mathsf{Ker}(J \otimes_A N \to JN)$. As J is of finite type, the map $J \otimes_A N \to JN$ is injective, hence $\xi = 0$ in $J \otimes_A N$, so $\xi = 0$ in $I \otimes_A N$. This shows that the natural map $I \otimes_A N \to IN$ is injective for *any* ideal $I \subset A$.

Let $M' \subset M$ be a submodule: we want to show that $M' \otimes_A N \to M \otimes_A N$ is injective. As above, we can reduce to the case where M is of finite type (this follows from the fact that tensor product commutes with direct limits, and that M is the direct limit of its sub-modules of finite type), in particular where M/M' is of finite type, so that there exist $m_1, \dots, m_r \in M$ such that $M = M' + Am_1 + \cdots + Am_r$. For $k \in \{0, \dots, r\}$, put $M_k = M' + Am_1 + \cdots + Am_k$, so that $M' = M_0 \subset M_1 \subset \cdots \subset M_{r-1} \subset M_r = M$. The map $M' \otimes_A N \to M \otimes_A N$ is the composite

$$M_0 \otimes_A N \to M_1 \otimes_A N \to \cdots \to M_{r-1} \otimes_A N \to M_r \otimes_A N$$

so it is enough to show the injectivity of each map $M_{k-1} \otimes_A N \to M_k \otimes_A N$: we can reduce to the case where $M = M' + Am$.

Put $I = \{a \in A\,;\, am \in M'\}$: this is an ideal in A. The map $\pi\colon M' \oplus A \to M$; $(x, a) \mapsto x + am$ is surjective. If $(x, a) \in \mathsf{Ker}(\pi)$, then $am = -x \in M'$, so $a \in I$. This implies that the map $\iota\colon I \to \mathsf{Ker}(\pi)$; $\lambda \mapsto (-\lambda m, \lambda)$ is an isomorphism. Form the exact sequence $0 \to I \xrightarrow{\iota} M' \oplus A \xrightarrow{\pi} M \to 0$ we get the exact sequence

$$I \otimes_A N \xrightarrow{\iota\otimes \mathsf{Id}_N} (M' \otimes_A N) \oplus N \xrightarrow{\pi\otimes \mathsf{Id}_N} M \otimes_A N \to 0$$

Let $\xi \in \mathsf{Ker}(M' \otimes_A N \to M \otimes_A N)$. Then $(\xi, 0) \in \mathsf{Ker}(\pi \otimes \mathsf{Id}_N)$, so there exists $\eta \in I \otimes_A N$ such that $(\xi, 0) = (\iota \otimes \mathsf{Id}_N)(\eta)$. Projecting on the second factor, the image of $\eta \in I \otimes_A N$ in N is zero. As the map $I \otimes_A N \to N$ in injective, we have $\eta = 0$, whence $\xi = 0$, as required. □

Remark 1.7.10. There is a more natural proof of this result using derived functors of the tensor product.

Proposition 1.7.11. (1) If N is *projective* over A (*i.e.* a direct summand in a free A-module), then N is flat. In particular, flatness is automatic when A is a field.
(2) If A is principal, that N is flat if and only if it is torsion-free.

Proof. (1) This is true when N is free by example 1.5.9 (2). In general, write $N \oplus S = L$ with L a free A-module. Let $f\colon M' \to M$ be an injective map of A-modules. By example 1.5.9 (2) again, the injective map $f \otimes \mathsf{Id}_L$ identifies with $(f \otimes \mathsf{Id}_N) \oplus (f \otimes \mathsf{Id}_S)$, so $f \otimes \mathsf{Id}_N$ is injective as well.
(2) Assume N is flat and let $\alpha \in A\backslash\{0\}$. The multiplication map $\alpha\colon A \to A$ is injective: so is $\alpha \otimes \mathsf{Id}_N\colon A \otimes_A N \to A \otimes_A N$. The latter identifies with the multiplication map $\alpha\colon N \to N$, so N has no α-torsion.
Assume N is torsion-free. If $I \subset A$ is a nonzero ideal, then $I = \alpha A$ with $\alpha \in A\backslash\{0\}$. The map $I \otimes_A N \to IN$ identifies to the multiplication by α on N : it is injective since N is torsion-free. This implies that N is flat over A by proposition 1.7.9. □

Remark 1.7.12. There are flat modules that are not projective. For instance $\mathbf{Q}$ is flat over $\mathbf{Z}$ (since it is torsion-free), but it is not projective (because it is divisible).

1.8. Localization.

Definition 1.8.1. A subset $S \subset A$ is called *multiplicative* if $0 \notin S$, $1 \in S$ and if S is stable under multiplication.

Example 1.8.2. (1) $A^\times$.
(2) $\{f^n\}_{n \in \mathbf{Z}_{\geqslant 0}}$ where $f \in A$ is not nilpotent.
(3) $A\backslash\mathfrak{p}$ where $\mathfrak{p} \subset A$ is a prime ideal.

Proposition 1.8.3. Let $S \subset A$ a multiplicative set. There exists an A-algebra $A \xrightarrow{\iota} S^{-1}A$, unique up to isomorphism, having the following universal property: if $f\colon A \to B$ is a ring homomorphism such that $(\forall s \in S)\ f(s) \in B^\times$, then there exists a unique ring homomorphism $\widetilde{f}\colon S^{-1}A \to B$ such that $f = \widetilde{f} \circ \iota$.

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\iota"'] & & B \\
& S^{-1}A \arrow[ur, "\widetilde{f}"'] &
\end{tikzcd}$$

Proof. Endow the set $A \times S$ with the binary relation $\sim$ defined by

$$(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow (\exists t \in S)\ t(a_1 s_2 - a_2 s_1) = 0$$

This is an equivalence relation. Denote by $S^{-1}A = (A \times S)/\sim$ the quotient set. If $(a, s) \in A \times S$, we denote by $\frac{a}{s}$ its image in $S^{-1}A$. Let $(a_1, s_1), (a_2, s_2) \in A \times S$. One checks easily that the elements $\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$ and $\frac{a_1}{s_1}.\frac{a_2}{s_2} := \frac{a_1 a_2}{s_1 s_2}$ only depend one $\frac{a_1}{s_1}$ and $\frac{a_2}{s_2}$, and that this defines two internal laws $+$ and . over $S^{-1}A$, making $S^{-1}A$ a commutative ring with unit $\frac{1}{1}$. Moreover, the map

$$\begin{aligned} \iota\colon A &\to S^{-1}A \\ a &\mapsto \tfrac{a}{1} \end{aligned}$$

is a ring homomorphism. Note that if $s \in S$, then $\iota(s) = \frac{s}{1}$ is invertible in $S^{-1}A$, with inverse $\frac{1}{s}$.
Let $f\colon A \to B$ a ring homomorphism such that $(\forall s \in S)\ f(s) \in B^\times$. The map

$$\begin{aligned} \widetilde{f}\colon S^{-1}A &\to B \\ \tfrac{a}{s} &\mapsto f(s)^{-1} f(a) \end{aligned}$$

is a well defined ring homomorphism, and it is the unique one such that $f = \widetilde{f} \circ \iota$. The unicity of $(S^{-1}A, \iota)$ follows from the universal property. □

Definition 1.8.4. The A-algebra $S^{-1}A$ is the *localization* of A with respect to the multiplicative set S.

Remark 1.8.5. (1) As usual, if $a \in A$, we will write a instead of $\iota(a)$ its image in $S^{-1}A$.
(2) In some sense, $S^{-1}A$ is the “minimal” A-algebra in which elements in S are invertible.
(3) When A is an integral domain, $\sim$ is nothing but the "usual" relation $(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow a_1 s_2 = a_2 s_1$. When A is not a domain, the latter is not an equivalence relation (why?), and the "t" is necessary.
(4) $\mathsf{Ker}(\iota) = \{a \in A\,;\ (\exists s \in S)\ sa = 0\}$, so ι is injective when A is an integral domain.
(5) Unless A is a factorial domain, there is no notion of “irreducible fraction”.

Example 1.8.6. (1) Assume A is an integral domain. Then $A\backslash\{0\}$ is multiplicative ($\{0\}$ is prime), and $(A\backslash\{0\})^{-1}A = \mathsf{Frac}(A)$ is the *fraction field* of A. For instance, $\mathsf{Frac}(\mathbf{Z}) = \mathbf{Q}$, and $\mathsf{Frac}(K[X]) = K(X)$ when K is a field.
If moreover $S \subset A$ is a multiplicative set, the universal property provides an injective ring homomorphism $S^{-1}A \to \mathsf{Frac}(A)$: localizations of A identify with subrings of $\mathsf{Frac}(A)$.
(2) More generally, if we do not assume integrity of A, the set $S = \{f \in A\,;\, f \text{ is not a zero-divisor in } A\} \subset A$ is multiplicative. In this case the localization $Q(A) := S^{-1}A$ is called the *total ring of fractions* of A.
(3) Let $f \in A$. We denote by $A_{(f)}$ the localization of A with respect to the multiplicative set $\{f^n\}_{n\in\mathbf{Z}_{\geqslant 0}}$. One can easily show that $A_{(f)} \simeq A[X]/\langle fX-1\rangle$. For instance, $\mathbf{Z}_{(10)}$ is nothing but the ring of decimal numbers.
(4) If $\mathfrak{p} \subset A$ is a prime ideal, we denote by $A_{\mathfrak{p}}$ the localization of A with respect to the multiplicative set $A\backslash\mathfrak{p}$. When A is an integral domain and $\mathfrak{p} = \{0\}$, one recovers $\mathsf{Frac}(A)$.
(5) Exercise: find multiplicative sets $S \subset \mathbf{Z}$ other than $\mathbf{Z}\backslash\{0\}$ such that $S^{-1}\,\mathbf{Z} = \mathbf{Q}$.

Definition 1.8.7. Let $S \subset A$ be a multiplicative set and M an A-module. The *localization* $S^{-1}M$ of M with respect to S is defined similarly as $S^{-1}A$: it is the quotient of the set $M \times S$ by the equivalence relation given by $(m_1, s_1) \sim (m_2, s_2) \Leftrightarrow (\exists t \in S)\ t(m_1s_2 - m_2s_1) = 0$. This is a $S^{-1}A$-module with the laws given by $\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{m_1s_2+m_2s_1}{s_1s_2}$ and $\frac{a}{s}.\frac{m}{s'} := \frac{am}{ss'}$. Moreover, an A-linear map $f\colon M \to N$ induces a $S^{-1}A$-linear map $f_S\colon S^{-1}M \to S^{-1}N$ (such that $f_S\big(\frac{m}{s}\big) = \frac{f(m)}{s}$ for all $m \in M$ and $s \in S$). It enjoys the following property: for any $S^{-1}A$-module N, the natural map

$$\mathsf{Hom}_{S^{-1}A}(S^{-1}M, N) \to \mathsf{Hom}_A(M, N)$$

is an isomorphism.

In particular, if $I \subset A$, is an ideal (*i.e.* a submodule of A), $S^{-1}I$ is an ideal in $S^{-1}A$.

Proposition 1.8.8. (1) $\big(\mathsf{Id}_M\big)_S = \mathsf{Id}_{S^{-1}M}$.
(2) If $f\colon M \to M'$ and $g\colon M' \to M''$ are A-linear maps, then $(g \circ f)_S = g_S \circ f_S$.
(3) If $M \subset N$, then $S^{-1}M \subset S^{-1}N$ and $S^{-1}(N/M) \simeq S^{-1}N/S^{-1}M$.
(4) If $f\colon M \to N$ is A-linear, then $\mathsf{Ker}(f_S) = S^{-1}\,\mathsf{Ker}(f)$ and $\mathsf{Coker}(f_S) = S^{-1}\,\mathsf{Coker}(f)$.

Proof. (3) The composite $M \subset N \xrightarrow{\iota} S^{-1}N$ extends into $i\colon S^{-1}M \to S^{-1}N$ (by $S^{-1}A$-linearity). Let $x \in S^{-1}M$: write $x = \frac{m}{s}$ with $m \in M$ and $s \in S$. If $i(x) = 0$, there exists $t \in S$ such that $tm = 0$ in $M \subset N$, which implies that $x = \frac{m}{s} = 0$ in $S^{-1}M$: the map i is injective. We consider it as an inclusion in $S^{-1}M \subset S^{-1}N$.
The canonical map $\pi\colon N \to N/M$ induces a $S^{-1}A$-linear map $S^{-1}N \xrightarrow{\pi_S} S^{-1}(N/M)$. It is surjective: if $x \in S^{-1}(N/M)$, there exists $\overline{n} \in N/M$ and $s \in S$ such that $x = \frac{\overline{n}}{s}$. Let $n \in N$ lifting $\overline{n}$: we have $\pi_S\big(\frac{n}{s}\big) = x$. Of course $S^{-1}M \subset \mathsf{Ker}(\pi_S)$. Conversely, if $x = \frac{n}{s} \in \mathsf{Ker}(\pi_S)$ (with $n \in N$ and $s \in S$), we have $\frac{\pi(n)}{s} = 0$ in $S^{-1}(N/M)$: there exists $t \in S$ such that $t\pi(n) = \pi(tn) = 0$ in N/M, *i.e.* $tn \in M$, thus $x = \frac{tn}{ts} \in S^{-1}M$. Hence $\mathsf{Ker}(\pi_S) = S^{-1}M$ and $S^{-1}N/S^{-1}M \xrightarrow{\sim} S^{-1}(N/M)$.
(4) Follows from (3). □

Proposition 1.8.9. Let M be an A-module and $S \subset A$ a multiplicative part. Then $S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M$ as $S^{-1}A$-modules. In particular, the A-algebra $S^{-1}A$ is flat.

Proof. (1) The map $S^{-1}A \times M \to S^{-1}M;\ \big(\frac{a}{s}, m\big) \mapsto \frac{am}{s}$ is bilinear so factors through an A-linear map $u\colon S^{-1}A \otimes_A M \xrightarrow{\sim} S^{-1}M$, such that $u\big(\frac{a}{s} \otimes m\big) = \frac{am}{s}$. Its inverse is nothing but the preimage of the A-linear map $M \to S^{-1}A \otimes_A M$ given by $m \mapsto 1 \otimes m$ under the isomorphism $\mathsf{Hom}_{S^{-1}}(S^{-1}M, S^{-1}A \otimes_A M) \xrightarrow{\sim} \mathsf{Hom}_A(M, S^{-1} \otimes_A M)$ (*cf* definition 1.8.7). It is in fact $S^{-1}A$-linear. Assume $\frac{m}{s} = \frac{m'}{s'}$ in $S^{-1}M$: there exists $t \in S$ such that $t(s'm - sm') = 0$, so $\frac{1}{s} \otimes m = \frac{ts'}{tss'} \otimes m = \frac{1}{tss'} \otimes (ts'm) = \frac{1}{tss'} \otimes (tsm') = \frac{ts}{tss'} \otimes m' = \frac{1}{s'} \otimes m'$. This implies that the map $v\colon S^{-1}M \to S^{-1}A \otimes_A M$ given by $v\big(\frac{m}{s}\big) = \frac{1}{s} \otimes m$ is well defined, and it is an inverse of u.
(2) This is a reformulation of proposition 1.8.8 (3) □

If $S, S' \subset A$ are multiplicative sets, then $SS' := \{ss'\,;\, s \in S,\, s' \in S'\}$ is also a multiplicative set of A.

Proposition 1.8.10. Let $\overline{S}$ be the image of S in $S'^{-1}A$, then there is an natural isomorphism of rings $\overline{S}^{-1}(S'^{-1}A) \xrightarrow{\sim} (SS')^{-1}A$.

Proof. Let $f\colon A \to B$ be an A-algebra such that $f(SS') \subset B^\times$. As $f(S') \subset B^\times$, the map f extends uniquely into a ring homomorphism $\widetilde{f}\colon S'^{-1}A \to B$. Similarly, $\widetilde{f}(\overline{S}) \subset B^\times$, so $\widetilde{f}$ extends uniquely into a ring homomorphism $\widehat{f}\colon \overline{S}^{-1}(S'^{-1}A) \to B$. This implies that $\overline{S}^{-1}(S'^{-1}A)$ has the universal property defining $(SS')^{-1}A$: there is an natural isomorphism of rings $\overline{S}^{-1}(S'^{-1}A) \xrightarrow{\sim} (SS')^{-1}A$. □

Corollary 1.8.11. If M is an A-module, there is a natural isomorphism $S^{-1}(S'^{-1}M) \xrightarrow{\sim} (SS')^{-1}M$.

Proof. Tensored with M, the isomorphism $S^{-1}A \otimes_A S'^{-1}A \xrightarrow{\sim} (SS')^{-1}A$ provides an isomorphism $(S^{-1}A \otimes_A S'^{-1}A) \otimes_A M \xrightarrow{\sim} (SS')^{-1}A \otimes_A M$ (*cf* proposition 1.8.9 (1)). As there are isomorphisms $S'^{-1}A \otimes_A M \xrightarrow{\sim} S'^{-1}M$ and $(SS')^{-1}A \otimes_A M \xrightarrow{\sim} (SS')^{-1}M$ (*cf* proposition 1.8.9 (1) again), we deduce a chain of isomorphisms

$$\begin{tikzcd}
S^{-1}A \otimes_A (S'^{-1}A \otimes_A M) \arrow[r, "\sim"] \arrow[d, "\wr"] & (S^{-1}A \otimes_A S'^{-1}A) \otimes_A M \arrow[d, "\wr"] \\
S^{-1}A \otimes_A (S'^{-1}M) \arrow[d, "\wr"] & (SS')^{-1}A \otimes_A M \arrow[d, "\wr"] \\
S^{-1}(S'^{-1}M) \arrow[r, dashed, "\sim"] & (SS')^{-1}M
\end{tikzcd}$$

□

Lemma 1.8.12. Let M be an A-module and N' a sub-$S^{-1}A$-module of $S^{-1}M$. Then $N' = S^{-1}N$ where N is the inverse image of N' under the natural map $M \to S^{-1}M$.

Proof. If $x = \frac{m}{s} \in N'$, then $sx = \frac{m}{1}$, *i.e.* $m \in N$, so $x \in S^{-1}N$. Conversely, $x = \frac{n}{s} \in S^{-1}N$ (with $n \in N$ and $s \in S$), then $\frac{n}{1} \in N'$, thus $x \in N'$ since N' is a $S^{-1}A$-module. □

Corollary 1.8.13. Let $S \subset A$ is a multiplicative set. Ideals in $S^{-1}A$ are localizations of ideals in A. In particular, A is noetherian implies $S^{-1}A$ is noetherian.

Notation. We denote by $\mathsf{Spec}(A)$ the set of prime ideals in A. It is called the *spectrum* of A.

Proposition 1.8.14. Let $S \subset A$ be a multiplicative set. The maps

$$\begin{aligned} \{\mathfrak{p} \in \mathsf{Spec}(A)\,;\, \mathfrak{p} \cap S = \varnothing\} &\leftrightarrow \mathsf{Spec}(S^{-1}A) \\ \mathfrak{p} &\mapsto S^{-1}\mathfrak{p} \\ \mathfrak{q} \cap A := \iota^{-1}(\mathfrak{q}) &\hookleftarrow \mathfrak{q} \end{aligned}$$

are increasing (for the inclusion) bijections inverse one to the other.

Proof. Let $\mathfrak{p} \in \mathsf{Spec}(A)$ such that $\mathfrak{p} \cap S = \varnothing$. Then $S^{-1}A/S^{-1}\mathfrak{p} \simeq S^{-1}(A/\mathfrak{p})$ (*cf* proposition 1.8.8). Let $\overline{S}$ be the image of S in $A/\mathfrak{p}$: as $\mathfrak{p} \cap S = \varnothing$, we have $0 \notin \overline{S}$, and $\overline{S}$ is a multiplicative set in $A/\mathfrak{p}$. As $A/\mathfrak{p}$ is an integral domain, so is its localization $S^{-1}(A/\mathfrak{p}) = \overline{S}^{-1}(A/\mathfrak{p}) \subset \mathsf{Frac}(A/\mathfrak{p})$, so that $S^{-1}\mathfrak{p}$ is prime in $S^{-1}A$.
Conversely, if $\mathfrak{q} \in \mathsf{Spec}(S^{-1}A)$, then $A/\iota^{-1}(\mathfrak{q}) \hookrightarrow S^{-1}A/\mathfrak{q}$ is an integral domain: we have $\mathfrak{q} \cap A \in \mathsf{Spec}(A)$. If $s \in (\mathfrak{q} \cap A) \cap S$, then $s \in \mathfrak{q}$. As s is invertible in $S^{-1}A$, we have $\mathfrak{q} = S^{-1}A$, which is not: we have $(\mathfrak{q} \cap A) \cap S = \varnothing$.
Let $\mathfrak{p} \in \mathsf{Spec}(A)$ be such that $\mathfrak{p} \cap S = \varnothing$. We have of course $\mathfrak{p} \subset S^{-1}\mathfrak{p} \cap A$. Conversely, let $a \in S^{-1}\mathfrak{p} \cap A$: write $a = \frac{\alpha}{s}$ with $\alpha \in \mathfrak{p}$ and $s \in S$. As $sa = \alpha \in \mathfrak{p}$ and $s \notin \mathfrak{p}$ (because $\mathfrak{p} \cap S = \varnothing$), we have $a \in \mathfrak{p}$, which proves the equality $\mathfrak{p} = S^{-1}\mathfrak{p} \cap A$.
Let $\mathfrak{q} \in \mathsf{Spec}(S^{-1}A)$. We have of course $S^{-1}(\mathfrak{q} \cap A) \subset \mathfrak{q}$. Conversely, let $x \in \mathfrak{q}$: write $x = \frac{a}{s}$ with $a \in A$ and $s \in S$. We have $sx = a \in \mathfrak{q} \cap A$, so $x = \frac{a}{s} \in S^{-1}(\mathfrak{q} \cap A)$, which proves the equality $\mathfrak{q} = S^{-1}(\mathfrak{q} \cap A)$. □

Remark 1.8.15. In particular we have $\mathsf{Spec}(S^{-1}A) \subset \mathsf{Spec}(A)$. The set $\mathsf{Spec}(A)$ can be equipped with a topological space structure (and even more...) and the bijection of proposition 1.8.14 identifies $\mathsf{Spec}(S^{-1}A)$ to an open subset of $\mathsf{Spec}(A)$, which explains the terminology of "localization".

Definition 1.8.16. A *local ring* is a ring having only one maximal ideal.

Exemples 1.8.17. (1) A field is a local ring.

(2) If K is a field, the ring of formal series $K[\![X]\!]$ is local, with maximal ideal $XK[\![X]\!]$.

(3) Exercise: A is local if and only if $A \backslash A^\times$ is an ideal[(7)]: it is then the maximal ideal of A.

Definition 1.8.18. Let A and B be local rings with maximal ideals $\mathfrak{m}_A$ and $\mathfrak{m}_B$ respectively. A ring homomorphism $f\colon A \to B$ is *local* when $f(\mathfrak{m}_A) \subset \mathfrak{m}_B$.

[(7)] If A is local with maximal ideal $\mathfrak{m}$, then $\mathfrak{m} \subset A \backslash A^\times$, and if $a \in A \backslash A^\times$, the ideal aA is strict: it is contained in a maximal ideal (*cf* theorem 1.1.7), hence $a \in \mathfrak{m}$, which proves the equality $\mathfrak{m} = A \backslash A^\times$. Conversely, if $\mathfrak{m} := A \backslash A^\times$ is an ideal, and if $I \subset A$ is a strict ideal, we have $I \cap A^\times = \varnothing$, *i.e.* $I \subset \mathfrak{m}$ and $\mathfrak{m}$ contains *all* ideals in A.

Example 1.8.19. Let A be a local ring, $\mathfrak{m}$ its maximal ideal, $k = A/\mathfrak{m}$ its residue field. Then the canonical projection $A \to k$ is a local homomorphism. Assume moreover that A is an integral domain, and let $K = \mathsf{Frac}(A)$ be its fraction field. Then the inclusion $A \to K$ is not local when A is not a field.

Corollary 1.8.20. If $\mathfrak{p} \in \mathsf{Spec}(A)$, then $\mathsf{Spec}(A_{\mathfrak{p}}) = \{\mathfrak{q}A_{\mathfrak{p}} \,;\, \mathfrak{q} \in \mathsf{Spec}(A),\ \mathfrak{q} \subset \mathfrak{p}\}$. In particular, $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$.

Proof. The equality follows from the equivalence $\mathfrak{q} \cap (A\backslash\mathfrak{p}) = \varnothing \Leftrightarrow \mathfrak{q} \subset \mathfrak{p}$ and proposition 1.8.14. Bijections of *loc. cit.* being increasing (for inclusions), maximal elements correspond. □

Lemma 1.8.21. Let M be an A-module. Then $M = \{0\}$ if and only if $M_{\mathfrak{m}} = \{0\}$ for all maximal ideal $\mathfrak{m} \subset A$.

Proof. Assume $M_{\mathfrak{m}} = \{0\}$ for all maximal ideal $\mathfrak{m} \subset A$. Let $m \in M$. Put $I = \{a \in A,\ am = 0\}$: this is an ideal in A. Assume $I \neq A$: there exists $\mathfrak{m} \subset A$ maximal such that $I \subset \mathfrak{m}$ (theorem 1.1.7). As $m = \frac{m}{1}$ is 0 in $M_{\mathfrak{m}}$, there exists $t \in A\backslash\mathfrak{m}$ such that $tm = 0$ in M, *i.e.* $t \in I$. We have thus $t \in I\backslash\mathfrak{m}$, which is a contradiction: $I = A$ and $m = 0$. □

Proposition 1.8.22. (Local-global principle). Let M be an A-module and M', M'' submodules of M. Then $M' \subset M''$ (resp. $M' = M''$) if and only if $M'_{\mathfrak{m}} \subset M''_{\mathfrak{m}}$ (resp. $M'_{\mathfrak{m}} = M''_{\mathfrak{m}}$) in $M_{\mathfrak{m}}$ for all maximal ideal $\mathfrak{m}$ of A.

Proof. If $M' \subset M''$, we already know that $M'_{\mathfrak{m}} \subset M''_{\mathfrak{m}}$ for all maximal ideal $\mathfrak{m}$ in A (proposition 1.8.8 (3)). Conversely, assume that $M'_{\mathfrak{m}} \subset M''_{\mathfrak{m}}$ for all maximal ideal $\mathfrak{m}$ in A. Put $\overline{M} = M/M''$ and $\pi\colon M \to \overline{M}$ the canonical map, so $\pi(M') \subset \overline{M}$. By assumption, we have $\pi(M')_{\mathfrak{m}} = \{0\}$ (because the image of $M'_{\mathfrak{m}} \subset M''_{\mathfrak{m}}$ in $\overline{M}_{\mathfrak{m}} = M_{\mathfrak{m}}/M''_{\mathfrak{m}}$ is zero, *cf* proposition 1.8.8 (3)) for all maximal ideal $\mathfrak{m}$ in A. By lemma 1.8.21, this implies that $\pi(M') = \{0\}$ in $\overline{M}$, *i.e.* $M' \subset M''$. □

Remark 1.8.23. An important special case of last proposition is the following: if I and J are ideals in A, then $I \subset J$ if and only if $I_{\mathfrak{m}} \subset J_{\mathfrak{m}}$ for all maximal ideal $\mathfrak{m}$ in A.

1.8.24. *Discrete valuation rings.*

Definition 1.8.25. A *discrete valuation ring* (DVR) is a PID having a unique nonzero prime ideal. A generator of this nonzero prime ideal is called a *uniformizer* of A.

Remark 1.8.26. Assume that A is a DVR. Its unique nonzero prime ideal $\mathfrak{m}$ is maximal: the ring A is local. Elements is $\mathfrak{m}$ are not invertible: as $\mathfrak{m} \neq 0$, the ring A is not a field.

Proposition 1.8.27. Assume that A is a DVR, and denote by $\mathfrak{m}$ its maximal ideal and π a uniformizer.
(1) Any element $a \in A\backslash\{0\}$ can be written uniquely $a = u\pi^{v(a)}$ with $u \in A^\times$ and $v(a) \in \mathbf{Z}_{\geqslant 0}$;
(2) nonzero ideals in A are of the form $\mathfrak{m}^i = \pi^i A$ (with $i \in \mathbf{Z}_{\geqslant 0}$);
(3) $\bigcap\limits_{i \in \mathbf{Z}_{\geqslant 0}} \mathfrak{m}^i = \{0\}$;

Proof. (1) As A is a PID, it is a UFD. As $\mathfrak{m} = \pi A$ is the only nonzero prime ideal, π is the only irreducible element (up to multiplication by an invertible element). The prime decomposition of $a \in A\backslash\{0\}$ is thus of the form $a = u\pi^{v(a)}$ where $u \in A^\times$ and $v(a) = v_\pi(a) \in \mathbf{Z}_{\geqslant 0}$ is the π-adic valuation of a.
(2) If $I \subset A$ is an ideal, it is principal: we have $I = aA$ with $a \in A$. If $I \neq \{0\}$, then $a \neq 0$, so $a = u\pi^i$ with $u \in A^\times$ and $i = v(a) \in \mathbf{Z}_{\geqslant 0}$, thus $I = \pi^i A = \mathfrak{m}^i$.
(3) If $a \in A\backslash\{0\}$, we have $a = u\pi^i$ with $u \in A^\times$ and $i = v(a)$, so $a \in \mathfrak{m}^i\backslash\mathfrak{m}^{i+1}$, and $a \notin \bigcap\limits_{i \in \mathbf{Z}_{\geqslant 0}} \mathfrak{m}^i$. Thus $\bigcap\limits_{i \in \mathbf{Z}_{\geqslant 0}} \mathfrak{m}^i = \{0\}$. □

1.9. **Integral extensions.** In what follows, $f\colon A \to B$ is an A-algebra.

Definition 1.9.1. (1) An element $b \in B$ is *integral* over A if there exists a *monic* polynomial $P \in A[X]$ such that $P(b) = 0$. The equality $P(b) = 0$ is then called an *equation of integral dependence* of b over A.
(2) We say that B is integral over A (or that $A \to B$ is integral) when all its elements are integral over A.

Example 1.9.2. $\sqrt{2} \in \mathbf{C}$ is integral over $\mathbf{Z}$, but $\frac{1}{\sqrt{2}}$ is not.

Proposition 1.9.3. Let $b \in B$. The following are equivalent:

(i) b is integral over A;
(ii) $A[b]$ is a finite A-algebra;

(iii) there exists a sub-A-module $B' \subset B$ of finite type such that B' contains an element which is not a zero divisor, and $bB' \subset B'$ (*i.e.* B' is stable under multiplication by b).

Proof. • Assume (i): let $P \in A[X]$ monic and such that $P(b) = 0$. If $\deg(P) = n$, the A-module $A[b]$ is generated by $\{1, b, \ldots, b^{n-1}\}$ (euclidean division), hence of finite type.
• Assume (ii): the A-module $B' = A[b]$ satisfies (iii).
• Assume (iii): let $(\beta_1, \ldots, \beta_n)$ be a generating family of the A-module B'. As $b\beta_i \in B'$, there exist $M = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(A)$ such that $b\beta_i = \sum\limits_{j=1}^{n} a_{i,j}\beta_j$ for all $i \in \{1, \ldots, n\}$. Put $X = (\beta_i)_{1 \leqslant i \leqslant n} \in \mathsf{M}_{n\times 1}(B)$: we have $MX = bX$, *i.e.*

$$(*) \qquad (b\,\mathrm{I}_n - M)X = 0.$$

Let $P(X) = \det(X\,\mathrm{I}_n - M)$: this is a monic polynomial of degree n, with coefficients in A. Multiplying equality $(*)$ by the transpose of the cofactors matrix of $b\,\mathrm{I}_n - M$, we get $P(b)X = 0$, so $P(b)B' = 0$, whence $P(b) = 0$ (since B' contains an element which is not a zero divisor by hypothesis). □

Lemma 1.9.4. Let $b_1, \ldots, b_n \in B$ such that b_i is integral over $A[b_1, \ldots, b_{i-1}]$ for all $i \in \{1, \ldots, n\}$. Then the A-algebra $A[b_1, \ldots, b_n]$ is finite.

Proof. By induction on $n \in \mathbf{Z}_{>0}$, the case $n = 1$ following from proposition 1.9.3. Let $n \in \mathbf{Z}_{>1}$ and put $A' = A[b_1, \ldots, b_{n-1}] \subset B$. By induction, the A-algebra A' is finite. As b_n is integral over A', the A'-algebra $A'[b_n]$ is finite: the A-algebra $A[b_1, \ldots, b_n] = A'[b_n]$ is finite. □

Proposition 1.9.5. The A-algebra B is finite if and only if it is integral and of finite type.

Proof. If B is finite over A, it is integral by proposition 1.9.3 (implication (iii)⇒(i) with $B' = B$). Moreover, if $\{b_1, \ldots, b_n\}$ generates the A-module B, the morphism of A-algebras $A[X_1, \ldots, X_n] \to B$ sending X_i to b_i is surjective, so that B is of finite type (as an algebra) over A.
Conversely, assume B is integral and of finite type over A. We can write $B = A[b_1, \ldots, b_n]$, and as $b_1, \ldots, b_n$ are integral over A, the A-module B is of finite type by lemma 1.9.4. □

Proposition 1.9.6. If $A \to B$ and $B \to C$ are integral, so is $A \to C$.

Proof. Let $c \in C$ and $P(c) = 0$, with $P(X) = X^n + b_1X^{n-1} + \cdots + b_n \in B[X]$, an equation of integral dependence. As $A \to B$ is integral, the elements $b_1, \ldots, b_n$ are integral over A: by lemma 1.9.4, $B' = A[b_1, \ldots, b_n]$ is finite over A. As $B'[c]$ is finite over B, it is finite over A, which implies that c is integral over A (proposition 1.9.3, noting that $1 \in B'[c]$). □

Corollary 1.9.7. Let $b, b' \in B$ be integral over A. Then $b - b'$ and bb' are integral over A.

Proof. By lemma 1.9.4, the morphism $A \to A[b, b']$ is finite hence integral: as $b - b', bb' \in A[b, b']$, they are integral over A. □

Remark 1.9.8. If $b \in B^\times$ is integral over A, the inverse $b^{-1} \in B$ is not integral over A in general.

Definition 1.9.9. (1) By corollary 1.9.7, the set of elements in B that are integral over A is a sub-A-algebra of B, which is called the *integral closure* of A in B.
(2) Assume A is an integral domain and put $K = \mathsf{Frac}(A)$. The *integral closure* of A is its integral closure in K. We say that A is *integrally closed* if it is equal to its integral closure, *i.e.* when the only element in K that are integral over A are elements in A.

Proposition 1.9.10. UFD are integrally closed. In particular, PID are integrally closed.

Proof. Assume that A is a UFD, put $K = \mathsf{Frac}(A)$ and let $x \in K$ integral over A. Write $x = a/b$ with $a \in A$ and $b \in A\backslash\{0\}$ coprime. Let $x^n + \alpha_1x^{n-1} + \cdots + \alpha_n = 0$ be an equation of integral dependence (with $\alpha_1, \ldots, \alpha_n \in A$). Multiplying by b^n, we get

$$a^n + \alpha_1a^{n-1}b + \cdots + \alpha_nb^n = 0$$

so that b divides a^n. As a and b are coprime, this implies that $b \in A^\times$, whence $x = ab^{-1} \in A$. □

Example 1.9.11. Let F be a field, t an indeterminate, and put $A = F[t^2, t^3] \subset B = F[t]$. Then we have $\mathsf{Frac}(A) = \mathsf{Frac}(B) = F(t)$. As B is a PID, it is integrally closed by proposition 1.9.10. The element t is integral over A, but $t \notin A$, so that A is not integrally closed (hence not a UFD by proposition 1.9.10).

Proposition 1.9.12. Assume that A is an integral domain, put $K = \mathsf{Frac}(A)$ and let L/K be an algebraic field extension. Denote by B the integral closure of A in L. If $x \in L$, there exists $a \in A\backslash\{0\}$ such that $ax \in B$. In particular[8] $L = \mathsf{Frac}(B)$ and B is integrally closed.

[8] As the proof shows, we have in fact $L = (A\backslash\{0\})^{-1}B$.

Proof. Let $X^d+\alpha_1X^{d-1}+\cdots+\alpha_d \in K[X]$ be the minimal polynomial of x over K, and $a \in A\backslash\{0\}$ such that $a\alpha_i \in A$ for all $i \in \{1,\ldots,d\}$. The minimal polynomial of ax over K is then $X^d+a\alpha_1X^{d-1}+\cdots+a^d\alpha_n \in A[X]$, so $ax \in B$. This implies that $\mathsf{Frac}(B) = L$. If $x \in L$ is integral over B, then it is integral over A (proposition 1.9.6), *i.e.* $x \in B$, and B is integrally closed. □

Proposition 1.9.13. (Integral closure commutes to localization). Under the hypothesis of proposition 1.9.12, let $S \subset A$ be a multiplicative part. The integral closure of $S^{-1}A \subset K$ in L is $S^{-1}B$.

Proof. Let $b \in B$ and $b^n + a_1b^{n-1} + \cdots + a_n = 0$ an equation of integral dependence over A. If $s \in S$ and $x = \frac{b}{s} \in S^{-1}B$, then $x^n + \frac{a_1}{s}x^{n-1} + \cdots + \frac{a_n}{s^n} = 0$, which shows that x is integral over $S^{-1}A$. Conversely, let $x \in L$ integral over $S^{-1}A$ and $x^n + \alpha_1x^{n-1} + \cdots + \alpha_n = 0$ an equation of integral dependence over $S^{-1}A$. There exists $s \in S$ such that $a_i := s\alpha_i \in A$ for all $i \in \{1,\ldots,n\}$ (take a common denominator to the α_i). Put $b = sx \in L$: we have $b^n + a_1b^{n-1} + sa_2b^{n-2} + \cdots + s^{n-2}a_{n-1}b + s^{n-1}a_n = 0$, so that b is integral over A. We thus have $b \in B$, and $x \in S^{-1}B$. □

Definition 1.9.14. Recall that a *number field* is a finite extension of $\mathbf{Q}$ (usually seen as a subfield of $\mathbf{C}$). If K is a number field, its *ring of integers* is the integral closure $\mathcal{O}_K$ of $\mathbf{Z}$ in K. By last proposition, it is an integrally closed ring and $K = (\mathbf{Z}\backslash\{0\})^{-1}\mathcal{O}_K$.

Proposition 1.9.15. Assume A is integrally closed, let $K = \mathsf{Frac}(A)$ and L/K be an algebraic extension. An element in L is integral over A if and only if its minimal polynomial over K has coefficients in A.

Proof. Let $x \in L$ and $P \in K[X]$ its minimal polynomial over K. If $P \in A[X]$, the equality $P(x) = 0$ is an equation of integral dependence, and x is integral over A. Conversely, if $x \in L$ is integral over A, fix an algebraic closure $\overline{L}$ of L, and let $x_1,\ldots,x_n$ be the roots of P in $\overline{L}$ (*i.e.* the conjugates of x, counted with multiplicities). If $i \in \{1,\ldots,n\}$, there exists a K-isomorphism of fields $f\colon K(x) \to K(x_i)$ mapping x to x_i (isomorphism extension theorem). If $Q(x) = 0$ is an equation of integral dependence (with $Q \in A[X]$), then $Q(x_i) = Q(f(x)) = f(Q(x)) = 0$, so that x_i is integral over A for all $i \in \{1,\ldots,n\}$. From corollary 1.9.7, so are the coefficients of P (which are, up to a sign, symmetric polynomials in $x_1,\ldots,x_n$). As those coefficients belong to K and A is integrally closed in K by hypothesis, we have $P \in A[X]$. □

Example 1.9.16. $\frac{\sqrt{2}}{2}$ is not integral over $\mathbf{Z}$ (its minimal polynomial over $\mathbf{Q}$ is $X^2 - \frac{1}{2} \notin \mathbf{Z}[X]$).

Exercise 1.9.17. Let $d \in \mathbf{Z}\backslash\{0,1\}$ without square factor and $K = \mathbf{Q}(\sqrt{d})$. Then

$$\mathcal{O}_K = \begin{cases} \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \mod 4\,\mathbf{Z} \\ \mathbf{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \mod 4\,\mathbf{Z} \end{cases}$$

Proposition 1.9.18. Assume $A \to B$ is *injective* and that B is an integral domain[(9)] and integral over A. then A is a field if and only if B is a field.

Proof. • Assume A is a field, and let $b \in B\backslash\{0\}$. As B is integral over A, there is an equation of integral dependence $b^n + a_1b^{n-1} + \cdots + a_n = 0$ with $a_1,\ldots,a_n \in A$. As B is an integral domain, we can assume that $a_n \neq 0$ (otherwise we can divide the equation by b): we have $bc = 1$ with

$$c = -a_n^{-1}(b^{n-1} + a_1b^{n-2} + \cdots + a_{n-1}) \in B$$

so that b is invertible in B, and B is a field.
• Conversely, assume that B is a field. If $a \in A\backslash\{0\}$, then a has a nonzero (by injectivity of $A \to B$) hence invertible image in B: let $a^{-1} \in B$ be its inverse. As B is integral over A, there is a equation of integral dependence $(a^{-1})^n + \alpha_1(a^{-1})^{n-1} + \cdots + \alpha_n = 0$ with $\alpha_1,\ldots,\alpha_n \in A$ and

$$a^{-1} = -\alpha_1 - \alpha_2a - \cdots - \alpha_na^{n-1} \in A$$

so that A is a field. □

Proposition 1.9.19. Assume $f\colon A \to B$ is integral.
(1) If $\mathfrak{M} \subset B$ is a maximal ideal, then $\mathfrak{M} \cap A$ is a maximal ideal in A.
(2) If f is injective and $\mathfrak{m} \subset A$ is a maximal ideal, there exists a prime ideal $\mathfrak{M} \subset B$ such that $\mathfrak{m} = \mathfrak{M} \cap A$, and any such $\mathfrak{M}$ is maximal in B.

[(9)] This implies that A is an integral domain.

Proof. (1) Assume $\mathfrak{M} \subset B$ is maximal, and put $\mathfrak{m} = \mathfrak{M} \cap A$. the morphism $A/\mathfrak{m} \to B/\mathfrak{M}$ is injective. The $A/\mathfrak{m}$-algebra $B/\mathfrak{M}$ is integral because B is over A (if $b \in B$ and $P(b) = 0$ is an equation of integral dependence with $P \in A[X]$, we have $\overline{P}(\overline{b}) = 0$ where $\overline{P} \in (A/\mathfrak{m})[X]$ and $\overline{b} \in B/\mathfrak{M}$ denote the reductions of P modulo $\mathfrak{m}A[X]$ and of b modulo $\mathfrak{M}$ respectively). As $B/\mathfrak{M}$ is a field, so is $A/\mathfrak{m}$ by proposition 1.9.18, and $\mathfrak{m}$ is maximal in A.
(2) Let $\mathfrak{m} \subset A$ be a maximal ideal. Assume that $\mathfrak{m}B = B$, *i.e.* $1 \in \mathfrak{m}B$: we can write

$$(*) \qquad 1 = \sum_{i=1}^{r} \alpha_i b_i$$

with $\alpha_1, \ldots, \alpha_n \in \mathfrak{m}$ and $b_1, \ldots, b_n \in B$. As B is integral over A, so is $B' = A[b_1, \ldots, b_n]$. As B' is of finite type over A, the A-algebra B' is in fact finite (*cf* proposition 1.9.5): we can write $B' = A\beta_1 + \cdots + A\beta_n$. On the other hand, equality $(*)$ implies that $\mathfrak{m}B' = B'$: for all $i \in \{1, \ldots, n\}$, there exists $\lambda_{i,1}, \ldots, \lambda_{i,n} \in \mathfrak{m}$ such that

$$\beta_i = \sum_{j=1}^{n} \lambda_{i,j}\beta_j.$$

If $M = (\lambda_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(A)$ and $X = (\beta_i)_{1 \leqslant i \leqslant n} \in \mathsf{M}_{n\times 1}(B')$, we have $MX = X$, thus $(\mathrm{I}_n - M)X = 0$: multiplying by the transpose of the cofactor matrix of $\mathrm{I}_n - M$, we get $\det(\mathrm{I}_n - M)X = 0$, *i.e.* $\det(\mathrm{I}_n - M)B' = 0$, thus $\det(\mathrm{I}_n - M) = 0$ in B since $1 \in B'$. Because f is injective, we have $\det(\mathrm{I}_n - M) = 0$ in A: as $\det(\mathrm{I}_n - M) \equiv 1 \mod \mathfrak{m}$, we deduce that $1 \in \mathfrak{m}$ which is absurd, so we necessarily have $\mathfrak{m}B \neq B$.
As the ideal $\mathfrak{m}B \subset B$ is strict, there exists a maximal ideal $\mathfrak{M} \subset B$ such that $\mathfrak{m}B \subset \mathfrak{M}$ (*cf* theorem 1.1.7). We of course $\mathfrak{m} \subset \mathfrak{M} \cap A$, whence $\mathfrak{m} = \mathfrak{M} \cap A$ since $\mathfrak{m}$ is maximal in A.
If $\mathfrak{P} \subset B$ is a prime ideal such that $\mathfrak{m} = \mathfrak{P} \cap A$, the morphism $A/\mathfrak{m} \to B/\mathfrak{P}$ is injective. It makes $B/\mathfrak{P}$ an integral $A/\mathfrak{m}$-algebra since B is over A, and $B/\mathfrak{P}$ is an integral domain: as $A/\mathfrak{m}$ is a field, so is $B/\mathfrak{P}$ (*cf* proposition 1.9.18), *i.e.* $\mathfrak{P}$ is maximal in B. □

1.10. **Discriminants.** Let A be a ring.

1.10.1. *Traces and norms.*

Definition 1.10.2. (1) Let M be a free[10] A-module of finite rank and $f \in \mathsf{End}_A(M)$. If $\mathfrak{B}$ is an A-basis of M, we can describe f by its matrix $(a_{i,j})_{1 \leqslant i,j \leqslant n}$ in $\mathfrak{B}$ (where $n = \mathsf{rk}_A(M)$). The *trace*, the *determinant* and the *characteristic polynomial* of f are

$$\mathsf{Tr}(f) = \sum_{i=1}^{n} a_{i,i} \in A, \quad \det(f) = \det(a_{i,j})_{1 \leqslant i,j \leqslant n} \in A,$$

$$\text{and} \quad \chi_f(X) = \det\big(X\mathrm{I}_n - (a_{i,j})_{1 \leqslant i,j \leqslant n}\big) \in A[X]$$

respectively. They depend on f and not on the choice of the basis $\mathfrak{B}$. Recall that $\mathsf{Tr}(f + \alpha g) = \mathsf{Tr}(f) + \alpha\,\mathsf{Tr}(g)$, $\det(fg) = \det(f)\det(g)$ and $\det(\alpha f) = \alpha^n \det(f)$ for $\alpha \in A$ and $f, g \in \mathsf{End}_A(M)$.
(2) Let B be a free A-algebra[11] of finite rank over A. If $x \in B$, let $m_x \in \mathsf{End}_A(B)$ be the map defined by $m_x(b) = xb$ for all $b \in B$. Put

$$\mathsf{Tr}_{B/A}(x) = \mathsf{Tr}(m_x) \in A, \quad \mathsf{N}_{B/A}(x) = \det(m_x) \in A \quad \text{and} \quad \chi_{x,B/A} = \chi_{m_x} \in A[X]$$

that we call the *trace*, the *norm* and the *characteristic polynomial* of x respectively (note that χ_{m_x} is monic).

Proposition 1.10.3. Let B be a free A-algebra of rank n, $x, y \in B$ and $a \in A$. Then

(1) $\mathsf{Tr}_{B/A}(x + y) = \mathsf{Tr}_{B/A}(x) + \mathsf{Tr}_{B/A}(y)$;
(2) $\mathsf{Tr}_{B/A}(a) = na$;
(3) $\mathsf{N}_{B/A}(xy) = \mathsf{N}_{B/A}(x)\,\mathsf{N}_{B/A}(y)$;
(4) $\mathsf{N}_{B/A}(a) = a^n$.

Proposition 1.10.4. Let L/K be a finite field extension, $x \in L$, and $x_1, \ldots, x_n$ the roots (in some algebraic closure $\overline{K}$ of K, counted with multiplicities) of the minimal polynomial P of x over K. Then

$$\mathsf{Tr}_{L/K}(x) = [L : K(x)] \sum_{i=1}^{n} x_i, \quad \mathsf{N}_{L/K}(x) = \Big(\prod_{i=1}^{n} x_i\Big)^{[L:K(x)]} \quad \text{and } \chi_{x,L/K} = P^{[L:K(x)]}$$

[10] It is possible to extend the following definitions to the case where M is a *projective* module of finite rank. This generalization is useful when working with extension of number fields whose ring of integers is not a PID for instance.

[11] *I.e.* such that B is free seen as an A-module.

Proof. Assume first that $L = K(x)$. Let $\mathfrak{B} = (1, x, \ldots, x^{n-1})$: this is a basis of L over K. Let $P \in K[X]$ be the minimal polynomial of x over K: write $P(X) = X^n - \lambda_1 X^{n-1} - \cdots - \lambda_n$. The matrix of multiplication by x in $\mathfrak{B}$ is the companion matrix:

$$C = C(\lambda_1, \ldots, \lambda_n) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & \lambda_n \\ 1 & \ddots & & \vdots & \lambda_{n-1} \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & 1 & 0 & \lambda_2 \\ 0 & \cdots & 0 & 1 & \lambda_1 \end{pmatrix} \in \mathsf{M}_n(K)$$

We have $\chi_C(X) = \det(X\mathrm{I}_n - C) = X^n - \lambda_1 X^{n-1} - \cdots - \lambda_n$, so that $\chi_{x,L/K} = P$. In particular, we have $\mathsf{Tr}_{L/K}(x) = \lambda_1 = \sum\limits_{i=1}^{n} x_i$ and $\mathsf{N}_{L/K}(x) = (-1)^{n-1}\lambda_n = \prod\limits_{i=1}^{n} x_i$.

In general, let $d = [L : K(x)]$ and $(y_1, \ldots, y_d)$ be basis of L over $K(x)$, so that $L = K(x)y_1 \oplus \cdots \oplus K(x)y_d$. As the multiplication by x preserves each factor $K(x)y_i$, we have $\mathsf{Tr}_{L/K}(x) = d\,\mathsf{Tr}_{K(x)/K}(x) = d \sum\limits_{i=1}^{n} x_i$, $\mathsf{N}_{L/K}(x) = \mathsf{N}_{K(x)/K}(x)^d = \Big(\prod\limits_{i=1}^{n} x_i\Big)^d$ and $\chi_{x,L/K} = \chi^d_{x,K(x)/K} = P^d$. □

Corollary 1.10.5. Assume L/K is not separable. Then $\mathsf{Tr}_{L/K} = 0$.

Proof. We have $\mathsf{char}(K) = p > 0$. Let $x \in L$, and $x_1, \ldots, x_n$ the roots (in some algebraic closure $\overline{K}$ of K, counted with multiplicities) of its minimal polynomial P over K. If x is separable over K, then $L/K(x)$ is not separable, hence $p \mid [L : K(x)]$, thus $\mathsf{Tr}_{L/K}(x) = [L : K(x)] \sum\limits_{i=1}^{n} x_i = 0$. If x is not separable over K, we have $P(X) = Q(X^{p^e})$ with $e \in \mathbf{Z}_{>0}$ and $Q \in K[X]$ separable: each root of P has multiplicity p^e. This implies that $\sum\limits_{i=1}^{n} x_i = 0$, hence $\mathsf{Tr}_{L/K}(x) = [L : K(x)] \sum\limits_{i=1}^{n} x_i = 0$. □

Example 1.10.6. (1) Let K be a field, x algebraic over K and $P(X) = X^n + a_1 X + \cdots + a_n \in K[X]$ its minimal polynomial. We have $\mathsf{Tr}_{K(x)/K}(x) = -a_1$, $\mathsf{N}_{K(x)/K}(x) = (-1)^n a_n$ and $\chi_{x,L/K} = P$.
(2) If L/K is a *separable* finite extension, $\overline{K}$ an algebraic closure of K and $\mathsf{Hom}_{K\text{-alg}}(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_d\}$, we have $d = [L : K]$, and

$$\mathsf{Tr}_{L/K}(x) = \sum_{i=1}^{d} \sigma_i(x) \quad \text{and} \quad \mathsf{N}_{L/K}(x) = \prod_{i=1}^{d} \sigma_i(x)$$

(3) Let $d \in \mathbf{Z}\backslash\{0,1\}$ be a squarefree integer and $K = \mathbf{Q}(\sqrt{d})$. We have $K = \mathbf{Q} \oplus \mathbf{Q}\sqrt{d}$ and $\mathsf{Gal}(K/\mathbf{Q}) = \{\mathsf{Id}_K, \sigma\}$ where $\sigma(\sqrt{d}) = -\sqrt{d}$. If $z = x + y\sqrt{d} \in K$ (with $x, y \in \mathbf{Q}$), we thus have $\mathsf{Tr}_{K/\mathbf{Q}}(z) = 2x$ and $\mathsf{N}_{K/\mathbf{Q}}(z) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$.

Corollary 1.10.7. Let A be an integrally closed domain, $K = \mathsf{Frac}(A)$, L/K a finite extension and B the integral closure of A in L. If $b \in B$, then $\mathsf{Tr}_{L/K}(b), \mathsf{N}_{L/K}(b) \in A$ and $\chi_{b,L/K} \in A[X]$. Moreover, we have $b \in B^\times \Leftrightarrow \mathsf{N}_{L/K}(b) \in A^\times$.

Proof. As the conjugates of b are also integral over A (because its minimal polynomial has coefficients in A, *cf* proposition 1.9.15), so are their sum, their product, and more generally any symmetric polynomial evaluated on these conjugates. This implies that $\mathsf{Tr}_{L/K}(b), \mathsf{N}_{L/K}(b) \in A$ and $\chi_{b,L/K} \in A[X]$.
Let $b \in B\backslash\{0\}$ and P its minimal polynomial over K. By proposition 1.9.15, we have $P \in A[X]$. Write $P(X) = X^d + a_1 X^{d-1} + \cdots + a_d$: the minimal polynomial of b^{-1} over K is then $X^d + \frac{a_{d-1}}{a_d} X^{d-1} + \cdots + \frac{a_1}{a_d} X + \frac{1}{a_d}$. By proposition 1.9.15, we have thus $b \in B^\times \Leftrightarrow a_d \in A^\times$. We conclude since $\mathsf{N}_{L/K}(b) = \big((-1)^d a_d\big)^{[L:K(b)]}$. □

Exemples 1.10.8. (1) Let $d \in \mathbf{Z}\backslash\{0,1\}$ be a squarefree integer and $K = \mathbf{Q}(\sqrt{d})$. If $d \not\equiv 1 \mod 4\,\mathbf{Z}$, we have $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$. If $z = x + y\sqrt{d} \in \mathbf{Z}[\sqrt{d}]$, then $\mathsf{N}_{K/\mathbf{Q}}(z) = x^2 - dy^2$ (*cf* example 1.10.6 (3)). As $\mathbf{Z}^\times = \{\pm 1\}$, we thus have $z \in \mathbf{Z}[\sqrt{d}]^\times \Leftrightarrow x^2 - dy^2 \in \{\pm 1\}$. When $d < 0$, this is equivalent to $x^2 - dy^2 = 1$: if $d \leqslant -2$, we have $\mathbf{Z}[\sqrt{d}]^\times = \{\pm 1\}$ and when $d = -1$, we have $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$.
(2) Let p be an odd prime number, $\zeta \in \mathbf{C}$ a primitive p-th root of unity and $K = \mathbf{Q}(\zeta)$. The minimal polynomial of ζ over $\mathbf{Q}$ is $P(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. We thus have $\mathsf{Tr}_{K/\mathbf{Q}}(\zeta) = -1$ and $\mathsf{N}_{K/\mathbf{Q}}(\zeta) = 1$, so $\mathsf{Tr}_{K/\mathbf{Q}}(\zeta - 1) = \mathsf{Tr}_{K/\mathbf{Q}}(\zeta) - \mathsf{Tr}_{K/\mathbf{Q}}(1) = -p$. The minimal polynomial of $\zeta - 1$ over $\mathbf{Q}$ is $P(X+1)$, whence $\mathsf{N}_{K/\mathbf{Q}}(\zeta - 1) = P(1) = p$. Similarly, the minimal polynomial of $\zeta + 1$ over $\mathbf{Q}$ is $P(X-1)$, thus $\mathsf{N}_{K/\mathbf{Q}}(\zeta + 1) = P(-1) = 1$ (which shows that $\frac{1}{\zeta+1}$ is integral over $\mathbf{Z}$ by the preceding corollary).

Proposition 1.10.9. (Transitivity). If L/K and K/F are finite field extensions, we have

$$\mathsf{Tr}_{L/F} = \mathsf{Tr}_{K/F} \circ \mathsf{Tr}_{L/K} \quad \text{and} \quad \mathsf{N}_{L/F} = \mathsf{N}_{K/F} \circ \mathsf{N}_{L/K}$$

Lemma 1.10.10. Let L/K and K/F be algebraic extension, and $\overline{F}$ an algebraic closure of F. There exists a bijection

$$\mathsf{Hom}_{F\text{-alg}}(L,\overline{F}) \xrightarrow{\sim} \mathsf{Hom}_{K\text{-alg}}(L,\overline{F}) \times \mathsf{Hom}_{F\text{-alg}}(K,\overline{F}).$$

Proof. For each $\rho \in \mathsf{Hom}_{F\text{-alg}}(K,\overline{L})$, fix an extension $\widehat{\rho} \in \mathsf{Hom}_{F\text{-alg}}(\overline{F},\overline{F})$ (use Steinitz' theorem). If $\sigma \in \mathsf{Hom}_{F\text{-alg}}(L,\overline{F})$ let σ_K denote its restriction to K and put $\sigma^K = \widehat{\sigma_{|K}}^{-1} \circ \sigma$. By construction, the field K is invariant under σ^K: we have $\sigma^K \in \mathsf{Hom}_{K\text{-alg}}(L,\overline{F})$. We thus have a map

$$\begin{aligned}\mathsf{Hom}_{F\text{-alg}}(L,\overline{F}) &\to \mathsf{Hom}_{K\text{-alg}}(L,\overline{F}) \times \mathsf{Hom}_{F\text{-alg}}(K,\overline{F})\\ \sigma &\mapsto (\sigma^K,\sigma_K)\end{aligned}$$

It is injective because $\sigma = \widehat{\sigma_K} \circ \sigma^K$. It is surjective since $(\rho,\tau) \in \mathsf{Hom}_{K\text{-alg}}(L,\overline{F}) \times \mathsf{Hom}_{F\text{-alg}}(K,\overline{F})$, and if $\sigma = \widehat{\rho} \circ \tau$, then we have $\sigma_K = \rho$ and $\sigma^K = \tau$. □

Proof of proposition 1.10.9. • Case where L/F is separable. Keep notations from lemma 1.10.10. Let $x \in L$: by example 1.10.6, we have

$$\begin{aligned}\mathsf{Tr}_{L/F}(x) &= \sum_{\sigma\in\mathsf{Hom}_{F\text{-alg}}(L,\overline{F})} \sigma(x) \qquad \text{(because } L/F \text{ is separable, } \textit{cf} \text{ example 1.10.6 (2))}\\ &= \sum_{\substack{\tau\in\mathsf{Hom}_{K\text{-alg}}(L,\overline{F})\\ \rho\in\mathsf{Hom}_{F\text{-alg}}(K,\overline{F})}} \widehat{\rho}\big(\tau(x)\big) \qquad \text{(by lemma 1.10.10)}\\ &= \sum_{\rho\in\mathsf{Hom}_{F\text{-alg}}(K,\overline{F})} \widehat{\rho}\Big(\sum_{\tau\in\mathsf{Hom}_{K\text{-alg}}(L,\overline{F})} \tau(x)\Big)\\ &= \sum_{\rho\in\mathsf{Hom}_{F\text{-alg}}(K,\overline{F})} \widehat{\rho}(\mathsf{Tr}_{L/K}(x)) \qquad \text{(because } L/K \text{ is separable, } \textit{cf} \text{ example 1.10.6 (2))}\end{aligned}$$

As $\mathsf{Tr}_{L/K}(x) \in K$, we have $\widehat{\rho}(\mathsf{Tr}_{L/K}(x)) = \rho(\mathsf{Tr}_{L/K}(x))$ for all $\rho \in \mathsf{Hom}_{F\text{-alg}}(K,\overline{F})$, which implies that $\mathsf{Tr}_{L/F}(x) = \mathsf{Tr}_{K/F}(\mathsf{Tr}_{L/K}(x))$ (*cf* example 1.10.6 (2)). The proof is the same for the norm, replacing sums by products.

• Case where L/F is not separable. By corollary 1.10.5, we have $\mathsf{Tr}_{L/F} = 0$. Also, one among L/K and K/F is not separable, so $\mathsf{Tr}_{L/K} = 0$ or $\mathsf{Tr}_{K/F} = 0$ (*cf* corollary 1.10.5), so the statement on traces is clear. Let $x \in L$. By proposition 1.10.4, we have $\mathsf{N}_{L/F}(x) = \mathsf{N}_{F(x)/F}(x)^{[L:F(x)]} = \big(\mathsf{N}_{F(x)/F}(x)^{[K(x):F(x)]}\big)^{[L:K(x)]}$ and $\mathsf{N}_{L/K}(x) = \mathsf{N}_{K(x)/K}(x)^{[L:K(x)]}$: the statement on norms is equivalent to the equality

$$(*) \qquad \mathsf{N}_{F(x)/F}(x)^{[K(x):F(x)]} = \mathsf{N}_{K/F}(\mathsf{N}_{K(x)/K}(x)).$$

When $x \in K$, we have $K(x) = K$ so the equality follows from proposition 1.10.4 in that case. In general, let $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$ be the minimal polynomial of x over K, so that $\mathsf{N}_{K(x)/K}(x) = (-1)^n a_0$, whence $\mathsf{N}_{K/F}(\mathsf{N}_{K(x)/K}(x)) = (-1)^{nd}\mathsf{N}_{K/F}(a_0)$ where $d = [K:F]$. Fix a basis $\mathfrak{B} = (e_1,\ldots,e_d)$ of K over F. Then $\widetilde{\mathfrak{B}} = (e_ix^j)_{\substack{1\leqslant i\leqslant d\\ 0\leqslant j<n}} = (e_1,\ldots,e_d,xe_1,\ldots,xe_d,\ldots,x^{n-1}e_1,\ldots,x^{n-1}e_d)$ is a basis of $K(x)$ over F. As $x^n = -a_0 - a_1x - \cdots - a_{n-1}x^{n-1}$, the matrix of the multiplication by x in the basis $\widetilde{\mathfrak{B}}$ is

$$M = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -M_0\\ \mathrm{I}_n & \ddots & & \vdots & -M_1\\ 0 & \ddots & \ddots & \vdots & \vdots\\ \vdots & \ddots & \ddots & 0 & \vdots\\ 0 & \cdots & 0 & \mathrm{I}_n & -M_{n-1}\end{pmatrix} \in \mathsf{M}_{nd}(F)$$

(companion matrix by blocks), where M_i is the matrix of the multiplication by a_i in the basis $\mathfrak{B}$. Then[12] we have $\mathsf{Tr}_{K(x)/F}(x) = \det(M) = (-1)^{(nd-d)d}\det(-M_0) = (-1)^{(n-1)d^2}(-1)^d\,\mathsf{N}_{K/F}(a_0) = (-1)^{nd}\,\mathsf{N}_{K/F}(a_0)$ (because $\det(M_0) = \mathsf{N}_{K/F}(a_0)$ and $(-1)^{d^2} = (-1)^d$), proving equality $(*)$. □

1.10.11. *Discriminant.*

Definition 1.10.12. Let B be a free A-algebra of rank n and $x_1,\ldots,x_n \in B$. The *discriminant* of $(x_1,\ldots,x_n)$ is

$$\mathrm{D}(x_1,\ldots,x_n) = \det\Big(\big(\mathsf{Tr}_{B/A}(x_ix_j)\big)_{1\leqslant i,j\leqslant n}\Big) \in A$$

[12] This follows from the equality $\det\left(\begin{smallmatrix}0 & X\\ I_r & Y\end{smallmatrix}\right) = (-1)^{rs}\det(X)$ whenever $X \in \mathsf{M}_s(F)$, an equality which follows from a straightforward induction on r (developing the determinant along the first column).

Proposition 1.10.13. Under the hypothesis of definition 1.10.12, let $M = (a_{i,j})_{1\leqslant i,j\leqslant n} \in \mathsf{M}_n(A)$ and $y_i = \sum\limits_{j=1}^{n} a_{i,j}x_j \in B$ for $i \in \{1,\ldots,n\}$. Then

$$\mathrm{D}(y_1,\ldots,y_n) = \det(M)^2\,\mathrm{D}(x_1,\ldots,x_n)$$

Proof. Put $X = \big(\mathsf{Tr}_{B/A}(x_ix_j)\big)_{1\leqslant i,j\leqslant n}$ and $Y = \big(\mathsf{Tr}_{B/A}(y_iy_j)\big)_{1\leqslant i,j\leqslant n}$. For all $i,j \in \{1,\ldots,n\}$, we have

$$y_iy_j = \Big(\sum_{k=1}^{n} a_{i,k}x_k\Big)\Big(\sum_{l=1}^{n} a_{j,l}x_l\Big) = \sum_{k=1}^{n}\sum_{l=1}^{n} a_{i,k}x_kx_la_{j,l}$$

hence

$$\mathsf{Tr}_{B/A}(y_iy_j) = \sum_{k=1}^{n}\sum_{l=1}^{n} a_{i,k}\,\mathsf{Tr}_{B/A}(x_kx_l)a_{j,l}$$

thus $Y = MX{}^{\mathrm{t}}M$, hence $\det(Y) = \det(M)^2\det(X)$ *i.e.* $\mathrm{D}(y_1,\ldots,y_n) = \det(M)^2\,\mathrm{D}(x_1,\ldots,x_n)$. □

Corollary 1.10.14. Under the hypothesis of definition 1.10.12, let $(x_1,\ldots,x_n)$ and $(y_1,\ldots,y_n)$ be bases of B over A. Then

$$\mathrm{D}(y_1,\ldots,y_n)A = \mathrm{D}(x_1,\ldots,x_n)A$$

Proof. There exists $M = (a_{i,j})_{1\leqslant i,j\leqslant n} \in \mathsf{GL}_n(A)$ such that $y_i = \sum\limits_{j=1}^{n} a_{i,j}x_j \in B$ for $i \in \{1,\ldots,n\}$. We have then $\mathrm{D}(y_1,\ldots,y_n) = \det(M)^2\,\mathrm{D}(x_1,\ldots,x_n)$ (1.10.13): as $\det(M) \in A^\times$, we have $\mathrm{D}(y_1,\ldots,y_n)A = \mathrm{D}(x_1,\ldots,x_n)A$. □

Remark 1.10.15. When $\mathfrak{B} = (x_1,\ldots,x_n)$ is a basis of B over A, the element $\mathrm{D}(x_1,\ldots,x_n)$ is the discriminant of the bilinear form $B\times B \to A$; $(x,y) \mapsto \mathsf{Tr}_{B/A}(xy)$ in the basis $\mathfrak{B}$.

Definition 1.10.16. By corollary 1.10.14, under the hypothesis of definition 1.10.12, the ideal $\mathrm{D}(x_1,\ldots,x_n)A$ does not depend of basis $(x_1,\ldots,x_n)$ of B over A. This principal ideal is called the ***discriminant*** of B over A and is denoted $\mathfrak{d}_{B/A}$.

Proposition 1.10.17. Under the hypothesis of definition 1.10.12, let $S \subset A$ be a multiplicative part. then $S^{-1}B$ is free over $S^{-1}A$ and

$$\mathfrak{d}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{d}_{B/A}.$$

Proof. This is obvious since a basis of B over A provides a basis of $S^{-1}B$ over $S^{-1}A$. □

Remark 1.10.18. The previous proposition shows that the definition of the ideal $\mathfrak{d}_{B/A}$ sheafifies: one can define it for locally free sheaves on a scheme. This shows in particular that it generalizes to the case where B is projective over A.

Proposition 1.10.19. Under the hypothesis of definition 1.10.12, if $\mathfrak{d}_{B/A}$ contains an element which is not a zero divisor, and if $x_1,\ldots,x_n \in B$, the following conditions are equivalent:

(i) $(x_1,\ldots,x_n)$ is a basis of B over A ;

(ii) $\mathrm{D}(x_1,\ldots,x_n)$ generates $\mathfrak{d}_{B/A}$.

Proof. Implication (i)⇒(ii) follows from definition of the ideal $\mathfrak{d}_{B/A}$. Conversely, assume that $\mathrm{D}(x_1,\ldots,x_n)$ generates $\mathfrak{d}_{B/A}$. Let $(b_1,\ldots,b_n)$ be a basis of B over A and $d = \mathrm{D}(b_1,\ldots,b_n)$ so that $\mathfrak{d}_{B/A} = dA$. There exists $M = (a_{i,j})_{1\leqslant i,j\leqslant n} \in \mathsf{M}_n(A)$ such that $x_i = \sum\limits_{j=1}^{n} a_{i,j}b_j$ for all $i \in \{1,\ldots,n\}$. By proposition 1.10.13, we have $\mathrm{D}(x_1,\ldots,x_n) = \det(M)^2d$. As $\mathrm{D}(x_1,\ldots,x_n)$ generates $\mathfrak{d}_{B/A} = dA$, there exists $u \in A^\times$ such that $\mathrm{D}(x_1,\ldots,x_n) = ud$, so that $d(u-\det(M)^2) = 0$. As d is not a zero divisor (otherwise $\mathfrak{d}_{B/A}$ would only contain zero didisors, which is excluded by the hypothesis), we have $\det(M)^2 = u$ thus $\det(M) \in A^\times$, so that $M \in \mathsf{GL}_n(A)$, which implies that $(x_1,\ldots,x_n)$ is a basis of B over A. □

Corollary 1.10.20. Under the hypothesis of definition 1.10.12, assume moreover that A is a UFD. Let $x_1,\ldots,x_n \in B$ be such that $d = \mathrm{D}(x_1,\ldots,x_n) \in A\backslash\{0\}$ is squarefree. Then $(x_1,\ldots,x_n)$ is a basis of B over A, and $\mathfrak{d}_{B/A} = dA$.

Proof. Let $(e_1,\ldots,e_n)$ be a basis of B over A: there exists $M = (a_{i,j})_{1\leqslant i,j\leqslant n} \in \mathsf{M}_n(A)$ such that for all $i \in \{1,\ldots,n\}$, we have $x_i = \sum\limits_{j=1}^{n} a_{i,j}e_j$. We have $\mathrm{D}(x_1,\ldots,x_n) = \det(M)^2\,\mathrm{D}(e_1,\ldots,e_n)$ (proposition 1.10.13), *i.e.* $dA = \det(M)^2\mathfrak{d}_{B/A}$. As d is squarefree by hypothesis, we have $\det(M) \in A^\times$, so that $(x_1,\ldots,x_n)$ is a basis of B over A. □

Theorem 1.10.21. (Dedekind). Let K/F and L/F be extensions. Then elements in $\mathsf{Hom}_{F\text{-alg}}(K,L)$ are linearly independent in the L-vector space $\mathsf{Hom}_{F\text{-lin}}(K,L)$.

Proof. Assume the contrary. Let $\sum\limits_{i=1}^{r} \lambda_i\sigma_i = 0$ with $\lambda_i \in L$ and $\sigma_i \in \mathsf{Hom}_{F\text{-alg}}(K,L)$ for $i \in \{1,\dots,r\}$ be a non trivial linear dependence relation such that r is *minimal.* By minimality, we have $\lambda_i \neq 0$ for all $i \in \{1,\dots,r\}$, and the σ_i are pairwise distinct. After dividing the relation by λ_r, we may assume that $\lambda_r = 1$. For all $x \in K$, we have thus

$$(*) \qquad \sum_{i=1}^{r-1} \lambda_i\sigma_i(x) + \sigma_r(x) = 0.$$

Equality $(*)$ applied to the product of $x, y \in K$ gives

$$\sum_{i=1}^{r-1} \lambda_i\sigma_i(x)\sigma_i(y) + \sigma_r(x)\sigma_r(y) = 0$$

Subtracting $\sigma_r(y)$ times $(*)$ to the preceding equality gives

$$\sum_{i=1}^{r-1} \lambda_i\sigma_i(x)(\sigma_i(y) - \sigma_r(y)) = 0$$

for all $x, y \in K$. In particular, y being fixed, we have

$$\sum_{i=1}^{r-1} \lambda_i(\sigma_i(y) - \sigma_r(y))\sigma_i = 0.$$

By minimality of r, the coefficients of this linear combination are all zero: we have $\sigma_i(y) = \sigma_r(y)$ for all $y \in K$. The σ_i being pairwise distinct, this implies $r = 1$, which is impossible. □

Proposition 1.10.22. Let L/K be a finite separable field extension, $\overline{K}$ an algebraic closure of K, and $x_1,\dots,x_n$ a basis of L over K. Write $\mathsf{Hom}_{K\text{-alg}}(L,\overline{K}) = \{\sigma_1,\dots,\sigma_n\}$ (this has n elements since L/K is separable). Then

$$\mathrm{D}(x_1,\dots,x_n) = \det\big((\sigma_i(x_j))_{1\leqslant i,j\leqslant n}\big)^2 \neq 0.$$

Proof. Recall that $\mathsf{Tr}_{L/K}(x) = \sum\limits_{k=1}^{n} \sigma_k(x)$ for all $x \in L$ (exemple 1.10.6 (2)). We have

$$\mathsf{Tr}_{L/K}(x_ix_j) = \sum_{k=1}^{n} \sigma_k(x_ix_j) = \sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j)$$

so that $\big(\mathsf{Tr}_{L/K}(x_ix_j)\big)_{1\leqslant i,j\leqslant n} = {}^{\mathrm{t}}MM$ where $M = (\sigma_i(x_j))_{1\leqslant i,j\leqslant n} \in \mathsf{M}_n(\overline{K})$. We have thus

$$\mathrm{D}(x_1,\dots,x_n) = \det\big({}^{\mathrm{t}}MM\big) = \det(M)^2 = \det\big((\sigma_i(x_j))_{1\leqslant i,j\leqslant n}\big)^2.$$

It remains to check that $\det(M) \neq 0$. Let $X = (\lambda_i)_{1\leqslant i\leqslant n} \in \mathsf{M}_{1\times n}(\overline{K})$ such that $XM = 0$. We have then $\sum\limits_{i=1}^{n} \lambda_i\sigma_i(x_j) = 0$ for all $j \in \{1,\dots,n\}$. By K-linearity, this implies $\sum\limits_{i=1}^{n} \lambda_i\sigma_i = 0$ in $\mathsf{Hom}_{K\text{-lin}}(L,\overline{K})$. Dedekind's theorem (theorem 1.10.21) implies that $X = 0$: the matrix M is invertible, and $\det(M) \neq 0$. □

Corollary 1.10.23. Let L/K be a separable field extension of degree n. A family $(x_1,\dots,x_n) \in L^n$ is a K-basis of L if and only if $\mathrm{D}(x_1,\dots,x_n) \neq 0$.

Proposition 1.10.24. (Transitivity of discriminant). Let K/F and L/K be two finite separable field extensions, $x_1,\dots,x_n$ a basis of K over F and $(y_1,\dots,y_m)$ a basis of L over K. Then

$$\mathrm{D}(x_iy_j)_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} = \mathrm{D}(x_1,\dots,x_n)^{[L:K]}\,\mathsf{N}_{K/F}(\mathrm{D}(y_1,\dots,y_m)).$$

Proof. Write $\mathsf{Hom}_{F\text{-alg}}(K,\overline{F}) = \{\rho_1,\dots,\rho_n\}$ and $\mathsf{Hom}_{K\text{-alg}}(L,\overline{F}) = \{\tau_1,\dots,\tau_n\}$ (where $\overline{F}$ is an algebraic closure of F). Fix liftings $\widehat{\rho}_1,\dots,\widehat{\rho}_n \in \mathsf{Hom}_{F\text{-alg}}(\overline{F},\overline{F})$ of $\rho_1,\dots,\rho_n$: we have $\mathsf{Hom}_{F\text{-alg}}(L,\overline{F}) = \big\{\widehat{\rho}_i\tau_j\big\}_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}$ (*cf* lemma 1.10.10). On the other hand, we have $\mathrm{D}(x_iy_j)_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} = \det(M)^2$ where $M \in \mathsf{M}_{mn}(\overline{F})$ is the matrix with entries $\widehat{\rho}_i\tau_j(x_ky_\ell) = \rho_i(x_k)\widehat{\rho}_i\tau_j(y_\ell)$ for $(i,j),(k,\ell) \in \big(\{1,\dots,n\}\times\{1,\dots,m\}\big)^2$ (*cf* proposition 1.10.22). Put $Y = (\tau_j(y_\ell))_{1\leqslant j,\ell\leqslant m} \in \mathsf{M}_m(\overline{F})$: we have $M = \begin{pmatrix} \rho_1(x_1)\widehat{\rho}_1(Y) & \cdots & \rho_1(x_n)\widehat{\rho}_1(Y) \\ \vdots & & \vdots \\ \rho_n(x_1)\widehat{\rho}_n(Y) & \cdots & \rho_n(x_n)\widehat{\rho}_n(Y) \end{pmatrix} = M_1M_2$ (block matrix) where $M_1 = \mathsf{diag}\big(\widehat{\rho}_1(Y),\ldots,\widehat{\rho}_n(Y)\big) \in \mathsf{M}_{mn}(\overline{F})$ and $M_2 = \begin{pmatrix} \rho_1(x_1)\,\mathrm{I}_m & \cdots & \rho_1(x_n)\,\mathrm{I}_m \\ \vdots & & \vdots \\ \rho_n(x_1)\,\mathrm{I}_m & \cdots & \rho_n(x_n)\,\mathrm{I}_m \end{pmatrix} \in \mathsf{M}_{mn}(\overline{F})$. We have $\det(M_1)^2 = \prod_{\rho\in\mathsf{Hom}_{\text{-alg}}\,F(K,\overline{F})} \widehat{\rho}(\det(Y)^2) = \mathsf{N}_{K/F}(\mathrm{D}(y_1,\ldots,y_m))$. On the other hand, there exists a permutation matrix $P \in \mathsf{GL}_{mn}(\mathbf{Z})$ such that $P^{-1}M_2P = \mathsf{diag}(X,\ldots,X)$ with $X = (\rho_i(x_k))_{1\leqslant i,k\leqslant n} \in \mathsf{M}_n(\overline{F})$. We thus have $\det(M_2) = \det(X)^m$, whence $\det(M_2)^2 = \mathrm{D}(x_1,\ldots,x_n)^{[L:K]}$ (because $[L:K] = m$). At the end, we have $\mathrm{D}(x_iy_j)_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} = \det(M)^2 = \det(M_1)^2\det(M_2)^2 = \mathrm{D}(x_1,\ldots,x_n)^{[L:K]}\,\mathsf{N}_{K/F}(\mathrm{D}(y_1,\ldots,y_m))$. □

Corollary 1.10.25. (Transitivity of discriminant). Let A be an integral domain, $F = \mathsf{Frac}(A)$ and K/F and L/K finite separable fields extensions. Let B (resp. C) be the integral closure of A in K (resp. L). Assume B is free over A and C is free over B. Then $\mathfrak{d}_{C/A} = \mathfrak{d}_{B/A}^{\mathsf{rk}_B(C)}\,\mathsf{N}_{B/A}(\mathfrak{d}_{C/B})$ (where[13] $\mathsf{N}_{B/A}(dB) = \mathsf{N}_{B/A}(d)A$).

1.10.26. *Discriminant of polynomials.*

Definition 1.10.27. Let K a field, $P \in K[X]$ monic and $\alpha_1,\ldots,\alpha_n \in \overline{K}$ the roots of P in an algebraic closure $\overline{K}$ of K (counted with multiplicities). The *discriminant* of P is

$$\mathsf{disc}(P) = \prod_{1\leqslant i<j\leqslant n}(\alpha_i-\alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}}\prod_{1\leqslant i\neq j\leqslant n}(\alpha_i-\alpha_j)$$

It is a symmetric polynomial in the roots of P, hence a polynomial in the coefficients of P, and $\mathsf{disc}(P) \in K$. By definition, P is separable if and only if $\mathsf{disc}(P) \neq 0$.

Lemma 1.10.28. With notations of definition 1.10.27, we have

$$\mathsf{disc}(P) = (-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^n P'(\alpha_i)$$

Proof. We have $P'(X) = \sum\limits_{i=1}^n \prod\limits_{1\leqslant j\neq i\leqslant n}(X-\alpha_j)$, hence $P'(\alpha_i) = \prod\limits_{1\leqslant j\neq i\leqslant n}(\alpha_i-\alpha_j)$ which implies that $\prod\limits_{i=1}^n P'(\alpha_i) = \prod\limits_{1\leqslant i\neq j\leqslant n}(\alpha_i-\alpha_j) = (-1)^{\frac{n(n-1)}{2}}\,\mathsf{disc}(P)$. □

Example 1.10.29. (1) The discriminant of X^2+aX+b is a^2-4b. That of X^3+pX+q is $-4p^3-27q^2$ (exercise).
(2) Let $n \in \mathbf{Z}_{>0}$ and $P(X) = X^n - 1 \in \mathbf{Q}[X]$. Put $\mu_n = \{z \in \mathbf{C}\,;\, z^n = 1\}$: we have $P(X) = \prod\limits_{\zeta\in\mu_n}(X-\zeta)$. For $\zeta \in \mu_n$, we have $P'(\zeta) = n\zeta^{n-1}$: as $\prod\limits_{\zeta\in\mu_n}\zeta = (-1)^{n+1}$, we have $\prod\limits_{\zeta\in\mu_n}P'(\zeta) = n^n(-1)^{n^2-1}$, and thus

$$\mathsf{disc}(P) = (-1)^{\frac{n(n-1)}{2}}\prod_{\zeta\in\mu_n}P'(\zeta) = (-1)^{\frac{n^2+n-2}{2}}n^n$$

Remark 1.10.30. Up to a normalization, the discriminant is nothing but the resultant of P and P'.

Proposition 1.10.31. Let L/K a separable field extension of degree d, $\alpha \in L$ such that $L = K[\alpha]$ and $P \in K[X]$ the minimal polynomial of α over K. Then $(1,\alpha,\alpha^2,\ldots,\alpha^{n-1})$ is a basis of L over K and

$$\mathrm{D}(1,\alpha,\alpha^2,\ldots,\alpha^{n-1}) = \mathsf{disc}(P) = (-1)^{\frac{n(n-1)}{2}}\,\mathsf{N}_{L/K}(P'(\alpha))$$

Proof. Let $\overline{K}$ be an algebraic closure of K and $\mathsf{Hom}_{K\text{-alg}}(L,\overline{K}) = \{\sigma_1,\ldots,\sigma_n\}$. the conjugates of α are the $\alpha_i := \sigma_i(\alpha)$ for $i \in \{1,\ldots,n\}$. The extension L/K is separable: by proposition 1.10.22, we have

$$\mathrm{D}(1,\alpha,\ldots,\alpha^{n-1}) = \det\big((\sigma_i(\alpha^{j-1}))_{1\leqslant i,j\leqslant n}\big)^2 = \det\big((\alpha_i^{j-1})_{1\leqslant i,j\leqslant n}\big)^2$$

As $\det\big((\alpha_i^{j-1})_{1\leqslant i,j\leqslant n}\big) = \prod\limits_{1\leqslant i<j\leqslant n}(\alpha_i-\alpha_j)$ (Vandermonde determinant), this proves the first equality.

By lemma 1.10.28, we have $\mathsf{disc}(P) = (-1)^{\frac{n(n-1)}{2}}\prod\limits_{i=1}^n P'(\alpha_i)$. For $i \in \{1,\ldots,n\}$, we have $\alpha_i = \sigma_i(\alpha)$, hence $\prod\limits_{i=1}^n P'(\alpha_i) = \prod\limits_{i=1}^n \sigma(P'(\alpha)) = \mathsf{N}_{L/K}(P'(\alpha))$, proving the second equality. □

[13] This does not depend on the choice of the generator d.

Example 1.10.32. Let K be a field and $P(X) = X^n + aX + b \in K[X]$, that we assume irreducible and separable. If α is a root of P in an algebraic closure of K, we have[14]

$$\begin{aligned} \mathrm{D}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \mathsf{disc}(P) &= (-1)^{\frac{n(n-1)}{2}} \mathsf{N}_{K(\alpha)/K}(P'(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} \big(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n\big) \end{aligned}$$

For $n \in \{2, 3\}$, we recover formulas of example 1.10.29 (1).

1.10.33. *Integral closure in a separable extension.*

Proposition 1.10.34. Let L/K be a finite separable field extension.

$$\begin{aligned} L \times L &\to K \\ (x, y) &\mapsto \mathsf{Tr}_{L/K}(xy) \end{aligned}$$

is a non degenerate pairing.

Proof. Bilinearity follows from proposition 1.10.3. Let $x \in L$ be such that $\mathsf{Tr}_{L/K}(xy) = 0$ for all $y \in L$. Let $\overline{K}$ an algebraic closure de K and $\mathsf{Hom}_{K\text{-alg}}(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$, we have $\mathsf{Tr}_{L/K}(xy) = \sum\limits_{i=1}^{n} \sigma_i(x)\sigma_i(y)$, so that $\sum\limits_{i=1}^{n} \sigma_i(x)\sigma_i$. As $\{\sigma_1, \ldots, \sigma_n\}$ is linearly independent in $\mathsf{Hom}_{K\text{-lin}}(L, \overline{K})$ (Dedekind's theorem, *cf* theorem 1.10.21), this implies $\sigma_i(x) = 0$ for all $i \in \{1, \ldots, n\}$, thus $x = 0$. The kernel of the bilinear map is zero: it is non degenerate. □

Remark 1.10.35. By corollary 1.10.5, the preceding proposition is an equivalence.

Corollary 1.10.36. Let L/K be a finite separable field extension. The map

$$\begin{aligned} L &\to \mathsf{Hom}_{K\text{- lin}}(L, K) \\ x &\mapsto \big(y \mapsto \mathsf{Tr}_{L/K}(xy)\big) \end{aligned}$$

is an isomorphism of K-vector spaces. If $(x_1, \ldots, x_n)$ is a basis de L over K, there exists a unique basis $(y_1, \ldots, y_n)$ of L over K such that $\mathsf{Tr}_{L/K}(x_i y_j) = \delta_{i,j}$ for all $i, j \in \{1, \ldots, n\}$: it is called the *dual basis* of $(x_1, \ldots, x_n)$.

Proof. The map $f \colon L \to \mathsf{Hom}_{K\text{- lin}}(L, K)$ is is the linear map associated to the symmetric bilinear map $(x, y) \mapsto \mathsf{Tr}_{L/K}(xy)$. As the latter is not degenerate, the map f is injective: it is an isomorphism since $\dim_K\big(\mathsf{Hom}_{K\text{- lin}}(L, K)\big) = \dim_K(L)$. If $(x_1, \ldots, x_n)$ is a basis of L over K, the family $(f(x_1), \ldots, f(x_n))$ is a basis of $\mathsf{Hom}_{K\text{- lin}}(L, K)$ over K. The family $(y_1, \ldots, y_n)$ satisfies $\mathsf{Tr}_{L/K}(x_i y_j) = f(x_i)(y_j) = \delta_{i,j}$ for all $i, j \in \{1, \ldots, n\}$ if and only if it is the dual basis of $(f(x_1), \ldots, f(x_n))$ in L: it exists and is unique. □

Proposition 1.10.37. Let A be an integrally closed domain, K its fraction field and L/K a finite separable field extension. Let B be the integral closure of A in L. Then B contains a basis of L over K, and it is a sub-A-module of a free A-module of rank $[L : K]$ contained in L.

Proof. If $(e_1, \ldots, e_n)$ is a basis of L over K, there exists $a \in A \backslash \{0\}$ such that $x_i := ae_i \in B$ for all $i \in \{1, \ldots, n\}$ (*cf* proposition 1.9.12). The family $(x_1, \ldots, x_n)$ is still a basis of L over K, made of elements in B.
Let $(y_1, \ldots, y_n)$ be the dual basis of $(x_1, \ldots, x_n)$ for the trace form, and B' the sub-A-module of L generated by $\{y_1, \ldots, y_n\}$. As $(y_1, \ldots, y_n)$ is a basis of L over K, the A-module B' is free of rank $n = [L : K]$. If $x \in B$, write $x = \sum\limits_{j=1}^{n} \lambda_j y_j$ with $\lambda_1, \ldots, \lambda_n \in K$: as $x_i x \in B$ thus $\mathsf{Tr}_{L/K}(x_i x) = \sum\limits_{j=1}^{n} \lambda_j \mathsf{Tr}_{L/K}(x_i y_j) = \lambda_i \in A$ for all $i \in \{1, \ldots, n\}$ (corollary 1.10.7), we have $x \in B'$. □

Proposition 1.10.38. Under the hypothesis of proposition 1.10.37, we have in fact the following more explicit statement. If $(x_1, \ldots, x_n)$ is a basis of L over K made of elements in B, we have

$$B \subset \frac{1}{d}\big(Ax_1 \oplus \cdots \oplus Ax_n\big)$$

where $d = \mathrm{D}(x_1, \ldots, x_d)$.

[14] We have $P'(\alpha) = n\alpha^{n-1} + a = n\frac{-a\alpha-b}{\alpha} + a = -\frac{nb}{\alpha} - (n-1)a$. The minimal polynomial of α^{-1} being $X^n + \frac{a}{b}X^{n-1} + \frac{1}{b}$, that of $-\frac{nb}{\alpha}$ is $Q(X) = X^n - naX^{n-1} + (-n)^n b^{n-1}$ and that of $P'(\alpha)$ is thus $Q(X + (n-1)a)$: we have $\mathsf{N}_{K(\alpha)/K}(P'(\alpha)) = (-1)^n Q((n-1)a) = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n$.

Proof. By the proof of proposition 1.10.37, if $(y_1, \ldots, y_n)$ is the dual basis of $(x_1, \ldots, x_n)$, we have

$$B \subset B' = Ay_1 \oplus \cdots \oplus Ay_n$$

Write $y_i = \sum\limits_{j=1}^{n} \alpha_{i,j} x_j$ with $\alpha_{i,j} \in K$ for all $i, j \in \{1, \ldots, n\}$. We have

$$\delta_{i,j} = \mathsf{Tr}_{L/K}(x_i y_j) = \sum_{k=1}^{n} \alpha_{j,k} \mathsf{Tr}_{L/K}(x_i x_k)$$

so that if $M = \big(\mathsf{Tr}_{L/K}(x_i x_j)\big)_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(A)$ and $N = (\alpha_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(K)$, we have $M{}^{\mathrm{t}}N = \mathrm{I}_n$, *i.e.* ${}^{\mathrm{t}}N = M^{-1} \in \frac{1}{d}\mathsf{M}_n(A)$ by Cramer's formulas: we have $\alpha_{i,j} \in \frac{1}{d}A$ for all $i, j \in \{1, \ldots, n\}$. □

Corollary 1.10.39. Under the hypothesis of proposition 1.10.37, we have:

(1) if A is noetherian, then B is a finite A-algebra (in particular, B is noetherian);
(2) if A is a PID, then B is a free A-module of rank $[L : K]$.

Proof. By proposition 1.10.37, there exists a sub-A-module B' of L which is free of rank $[L : K]$ and such that $B \subset B'$.
(1) If A is noetherian, so is B' (proposition 1.3.4): the A-module B is of finite type (thus noetherian by proposition 1.3.4).
(2) If A is a PID, B is free of finite rank as a sub-A-module of the free A-module of finite rank B' (theorem 1.4.11). As it contains a basis de L over K (proposition 1.10.37), its rank is $[L : K]$. □

Remark 1.10.40. Under the hypothesis of proposition 1.10.37, assume moreover that A is a PID. By corollary 1.10.20, if $x_1, \ldots, x_n \in B$ are such that $\mathrm{D}(x_1, \ldots, x_n)$ is squarefree in A (which is a PID hence a UFD), then $(x_1, \ldots, x_n)$ is a basis of B over A.

1.11. Inverse limits.

1.11.1. *Generalities.* Let $\mathscr{C}$ be a category and $(I, \leqslant)$ a directed set[15] (*i.e.* a preordered[16] set in which every pair of elements has an upper bound: $(\forall i, j \in I)\,(\exists k \in I)\ i \leqslant k,\ j \leqslant k)$).

Definition 1.11.2. • A *inverse system* in $\mathscr{C}$ indexed by I is a pair $\big(\{X_i\}_{i \in I}, \{u_{i,j}\}_{\substack{i,j \in I \\ i \leqslant j}}\big)$ where $\{X_i\}_{i \in I}$ is a family of objects of $\mathscr{C}$, and $\{u_{i,j}\}_{\substack{i,j \in I \\ i \leqslant j}}$ a family of morphisms $X_j \xrightarrow{u_{i,j}} X_i$ (called *transition morphisms*) such that $u_{i,k} = u_{i,j} \circ u_{j,k}$ whenever $i \leqslant j \leqslant k$ in I. As often, it will be denoted by $(X_i)_{i \in I}$ alone.
• Let $\big(\{X_i\}_{i \in I}, \{u_{i,j}\}_{\substack{i,j \in I \\ i \leqslant j}}\big)$ be a inverse system in $\mathscr{C}$ indexed by I. Its *inverse limit*[17] (or simply *limit*) is an object $X \in \mathscr{C}$ with morphisms $\pi_i \colon X \to X_i$ for all $i \in I$ such that $(\forall i \leqslant j \in I)\ \pi_i = u_{i,j} \circ \pi_j$, having the following universal property: whenever $Y \in \mathscr{C}$ and $\psi_i \colon Y \to X_i$ are morphisms such that $(\forall i \leqslant j \in I)\ \psi_i = u_{i,j} \circ \psi_j$, then there exists a unique morphism $\widetilde{\psi} \colon Y \to X$ such that $(\forall i \in I)\ \psi_i = \pi_i \circ \widetilde{\psi}$.

$$\begin{tikzcd}
 & & X_j \arrow[d, "u_{i,j}"] \\
Y \arrow[r, dotted, "\widetilde{\psi}"] \arrow[rru, bend left, "\psi_j"] \arrow[rrd, bend right, "\psi_j"'] & X \arrow[ru, "\pi_j"] \arrow[rd, "\pi_i"'] & \\
 & & X_i
\end{tikzcd}$$

Being the solution of a universal problem, the inverse limits of $\big(\{X_i\}_{i \in I}, \{u_{i,j}\}_{\substack{i,j \in I \\ i \leqslant j}}\big)$, if it exists, is unique up to isomorphism: it is denoted $\varprojlim\limits_{I} X_i$.
• A *direct system* in $\mathscr{C}$ indexed by I is an inverse system in $\mathscr{C}^{\mathsf{op}}$ indexed by I. Its *inductive limit* (or *colimit*) is the corresponding inverse limit.

Remark 1.11.3. An inverse system in $\mathscr{C}$ indexed by I is nothing but a contravariant functor $I \to \mathscr{C}$. There is the obvious inclusion functor $i \colon \mathscr{C} \to \mathscr{C}^{I^{\mathrm{op}}}$ that maps an object to the corresponding constant inverse

[15] Which can be seen as a category whose objects are elements of I and there is exactly one arrow $i \to j$ if $i \leqslant j$, and no arrow otherwise.

[16] Reflexive and transitive *i.e.* an order without the antisymmetry condition.

[17] "Limite projective" in French.

system. If $\big(\{X_i\}_{i\in I}, \{u_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ is an inverse system in $\mathscr{C}$ indexed by I, its inverse limits, if it exists, is characterized by

$$\mathsf{Hom}_{\mathscr{C}^{I^{\mathrm{op}}}}\big(i(Y),(X_i)_{i\in I}\big) \xrightarrow{\sim} \mathsf{Hom}_{\mathscr{C}}\big(Y, \varprojlim_I X_i\big)$$

for all $Y\in\mathscr{C}$, *i.e.* is a final object in the category of pairs (Y,ψ) where $Y\in\mathscr{C}$ and $\psi\colon i(Y)\to(X_i)_{i\in I}$ (one can also say that it represents the contravariant functor $Y\mapsto \mathsf{Hom}_{\mathscr{C}^{I^{\mathrm{op}}}}\big(i(Y),(X_i)_{i\in I}\big)$).

Example 1.11.4. (1) When I is trivial (*i.e.* $i\leqslant j \Leftrightarrow i=j$), the inverse limit is the product $\prod\limits_I X_i$.

(2) If $\mathscr{C}$ is preabelian[18] and $u\in\mathsf{Hom}_{\mathscr{C}}(X,Y)$, the kernel of u is the inverse limit of $X\xrightarrow{u}Y\leftarrow 0$.
(3) Assume that $\mathscr{C}$ is a subcategory of **Set** that admits products indexed by I. Then

$$\varprojlim_I X_i \cong \Big\{(x_i)_{i\in I}\in\prod_{i\in I}X_i\,;\,(\forall i,j\in I)\ i\leqslant j\Rightarrow u_{i,j}(x_j)=x_i\Big\}\subset\prod_{i\in I}X_i.$$

The map $\pi_k\colon \varprojlim\limits_I X_i\to X_k$ is the restriction of the projection on the factor of index k. In particular, inverse limits exist in **Set**, **Gr**, $\mathbf{Mod}_R$ (where R is a commutative ring) and **Top**.
(4) An inverse limit $\varprojlim\limits_I X_i$ in **Gr** (resp. $\mathbf{Mod}_R$, resp. **Top**) coincide with the inverse limit in **Set**, endowed with the structure of group (resp. R-module, resp. topological space) induced by the inclusion $\varprojlim\limits_I X_i\subset\prod\limits_{i\in I}X_i$.

Remark 1.11.5. Assume $I=\mathbf{Z}_{\geqslant 0}$ (endowed with the natural order). The data of an inverse system is equivalent to that Of a sequence of sets $(X_n)_{n\in\mathbf{Z}_{\geqslant 0}}$, and for each $n\in\mathbf{Z}_{\geqslant 0}$, a map $\rho_n\colon X_{n+1}\to X_n$. The inverse limits is then simply:

$$\varprojlim_n X_n := \Big\{(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}\in\prod_{n=0}^{\infty}X_n\,;\,(\forall n\in\mathbf{Z}_{\geqslant 0})\,\rho_n(x_{n+1})=x_n\Big\}\subset\prod_{n=0}^{\infty}X_n.$$

Definition 1.11.6. A *morphism of inverse systems* $\big(\{X_i\}_{i\in I},\{u_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)\to\big(\{Y_i\}_{i\in I},\{v_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ is a family of morphisms $(f_i\colon X_i\to Y_i)_{i\in I}$ such that $f_i\circ u_{i,j}=u_{i,j}\circ f_j$ whenever $i\leqslant j$.

Proposition 1.11.7. (FUNCTORIALITY OF INVERSE LIMITS). Let $(f_i\colon X_i\to Y_i)_{i\in I}$ be a morphism of inverse systems in a category $\mathscr{C}$. Assume that the inverse limits $X=\varprojlim\limits_{i\in I}X_i$ and $Y=\varprojlim\limits_{i\in I}Y_i$ exist in $\mathscr{C}$. Then there exists a unique map $f\colon X\to Y$ such that $f_i\circ\pi_{X,i}=\pi_{Y,i}\circ f$ (where $\pi_{X,i}\colon X\to X_i$ and $\pi_{Y,i}\colon Y\to Y_i$ are the projections).

Proof. This follows from the universal property of Y:

$$\begin{tikzcd}
 & X_j \arrow[rr, "f_j"] \arrow[dd, "u_{i,j}"] & & Y_j \arrow[dd, "v_{i,j}"] \\
X \arrow[ur, "\pi_{X,j}"] \arrow[dr, "\pi_{X,i}"'] \arrow[rr, dotted, "f"'] & & Y \arrow[ur, "\pi_{Y,j}"] \arrow[dr, "\pi_{Y,i}"'] & \\
 & X_i \arrow[rr, "f_i"'] & & Y_j
\end{tikzcd}$$

□

1.11.8. *Exactness properties.* References for this section are [12, §1.12] and [24, Section 0594]. Here, we assume that $\mathscr{C}$ is a subcategory of **Gr** that is stable under inverse limits (hence under kernels) and cokernels (hence under images).

Definition 1.11.9. An *exact sequence* in $\mathscr{C}$ is a sequence of morphisms $(f_n\colon X_n\to X_{n+1})_{n\in J}$ (where $J\subset\mathbf{Z}$ is an interval)

$$\cdots\to X_n\xrightarrow{f_n}X_{n+1}\xrightarrow{f_{n+1}}X_{n+2}\to\cdots$$

such that $\mathsf{Im}(f_n)=\mathsf{Ker}(f_{n+1})$ for all $n\in J$. A short exact sequence is an exact sequence of the form

$$0\to X'\to X\to X''\to 0.$$

Proposition 1.11.10. The inverse limit functor $\varprojlim\limits_I\colon\mathscr{C}^{I^{\mathrm{op}}}\to\mathscr{C}$ is left exact.

[18] Which means that $\mathscr{C}$ is additive and has kernels and cokernels.

Proof. Let $0 \to \big(\{X'_i\}_{i\in I}, \{u'_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big) \xrightarrow{(f_i)_{i\in I}} \big(\{X_i\}_{i\in I}, \{u_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big) \xrightarrow{(g_i)_{i,j\in I}} \big(\{X''_i\}_{i\in I}, \{u''_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big) \to 0$ be an exact sequence of inverse systems of groups. The first row in

$$\begin{tikzcd}
0 \arrow[r] & \prod\limits_{i\in I} X'_i \arrow[r, "f"] & \prod\limits_{i\in I} X_n \arrow[r, "g"] & \prod\limits_{i\in I} X''_i \arrow[r] & 0 \\
& \varprojlim\limits_{i\in I} X'_i \arrow[u, phantom, "\bigcup"] \arrow[r, "f"] & \varprojlim\limits_{i\in I} X_i \arrow[u, phantom, "\bigcup"] \arrow[r, "g"] & \varprojlim\limits_{i\in I} X''_i \arrow[u, phantom, "\bigcup"] &
\end{tikzcd}$$

is exact. This implies the injectivity of $f\colon \varprojlim\limits_{i\in I} X'_i \to \varprojlim\limits_{i\in I} X_i$. Let $x = (x_i)_{i\in I} \in \varprojlim\limits_{i\in I} X_i$ be such that $g(x) = e$ (the unit in $\varprojlim\limits_{i\in I} X''_i$). By the exactness of the first row, we have $x = f(x')$ for a unique $x' = (x'_i)_{i\in I} \in \prod\limits_{i\in I} X'_i$. If $i \leqslant j$ in I, we have $x_i = u_{i,j}(x_j)$ *i.e.* $f_i(x'_i) = u_{i,j}(f_j(x'_j)) = f_i(u'_{i,j}(x'_j))$, thus $x'_i = u'_{i,j}(x'_j)$ by injectivity of f_i. Since this holds for all $i \leqslant j$ in I, we get $x' \in \varprojlim\limits_{i\in I} X'_i$, and the proposition follows. □

Remark 1.11.11. The inverse limit functor is not exact in general. For instance, passing to the inverse limit on the exact sequences $0 \to p^n\,\mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}/p^n\,\mathbf{Z} \to 0$ gives the exact sequence $0 \to 0 \to \mathbf{Z} \to \mathbf{Z}_p$, and $\mathbf{Z} \to \mathbf{Z}_p$ is not surjective.

Definition 1.11.12. Let $\big(\{X_i\}_{i\in I}, \{u_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ be an inverse system in **Set**. If $i \in I$, the family $(u_{i,j}(X_j))_{j\in I}$ of subsets of X_i is decreasing, in the sense that $i \leqslant j_1 \leqslant j_2 \Rightarrow u_{i,j_2}(X_{j_2}) \subset u_{i,j_1}(X_{j_1}) \subset X_i$. We say that $\big(\{X_i\}_{i\in I}, \{u_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ satisfies the *Mittag-Leffler* condition if for any $i \in I$, the family $(u_{i,j}(X_j))_{j\in I}$ stabilizes, *i.e.* there exists $n(i) \geqslant i$ such that

$$(\forall j \geqslant n(i))\, u_{i,j}(X_j) = u_{i,n(i)}(X_{n(i)}) \subset X_i.$$

Remark 1.11.13. If the maps $u_{i,j}$ are all surjective, then $\big(\{X_i\}_{i\in I}, \{u_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ satisfies the Mittag-Leffler condition. Conversely, assume that $\big(\{X_i\}_{i\in I}, \{u_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ satisfies the Mittag-Leffler condition. If $i \in I$, let $n(i) \geqslant i$ be such that $j \geqslant n(i) \Rightarrow u_{i,j}(X_j) = u_{i,n(i)}(X_{n(i)}) =: \widetilde{X}_i \subset X_i$. If $i \leqslant j$ in I and $x \in \widetilde{X}_j$, let $k \in I$ be such that $k \geqslant n(i)$ and $k \geqslant n(j)$: we can write $x = u_{j,k}(y)$ with $y \in X_k$, and $u_{i,j}(x) = u_{i,k}(y) \in \widetilde{X}_i$ (since $k \geqslant n(i)$). Moreover, if $z \in \widetilde{X}_i$, there exists $\widehat{z} \in X_k$ such that $z = u_{i,k}(\widehat{z}) = u_{i,j}(u_{j,k}(\widehat{z})) \in u_{i,j}(\widetilde{X}_j)$, which shows that the maps $u_{i,j}\colon X_j \to X_j$ induce surjective maps $u_{i,j}\colon \widetilde{X}_j \to \widetilde{X}_i$. By functoriality, the inclusions $\widetilde{X}_i \subset X_i$ induce an injective map $\varprojlim\limits_{i\in I} \widetilde{X}_i \to \varprojlim\limits_{i\in I} X_i$. The latter is in fact an equality: if $(x_i)_{i\in I} \in \varprojlim\limits_{i\in I} X_i$, then $x_i = u_{i,j}(x_j) \in u_{i,j}(X_j)$ for all $j \geqslant i$, hence $x_i \in \widetilde{X}_i$ for all $i \in I$.

Lemma 1.11.14. Assume that I is countable. Let $\big(\{X_i\}_{i\in I}, \{u_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ be an inverse system of nonempty sets satisfying the Mittag-Leffler condition. Then $\varprojlim\limits_{i\in I} X_i \neq \varnothing$.

Proof. This is obvious when $(I, \leqslant) = (\mathbf{Z}_{\geqslant 0}, \leqslant)$: we reduce to this case as follows. Write $I = \{i_n\}_{n\in\mathbf{Z}_{\geqslant 0}}$: one constructs inductively a strictly increasing map $\varphi\colon\ \mathbf{Z}_{\geqslant 0} \to \mathbf{Z}_{\geqslant 0}$ such that $\varphi(0) = 0$ and $i_{\varphi(n)} \geqslant i_n$ and $i_{\varphi(n)} \geqslant i_{\varphi(n-1)}$ for all $n \in \mathbf{Z}_{>0}$. Using notations of remark 1.11.13, we have $\widetilde{X}_{i_n} = u_{i_n, i_{\varphi(m)}}(X_{i_{\varphi(m)}})$ for some $m \gg n$. As the sets $X_{i_{\varphi(m)}}$ are nonempty, so are the sets $\widetilde{X}_{i_n}$. As the transition maps of the inverse system $\big(\{\widetilde{X}_i\}_{i\in I}, \{u_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ are surjective, we can find inductively a sequence $(\xi_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in \varprojlim\limits_{n\in\mathbf{Z}_{\geqslant 0}} \widetilde{X}_{i_{\varphi(n)}}$: choose any $\xi_0 \in \widetilde{X}_0$, and $\xi_0, \ldots, \xi_n$ being constructed, choose $\xi_{n+1} \in \widetilde{X}_{i_{\varphi(n+1)}}$ such that $u_{i_{\varphi(n)}, i_{\varphi(n+1)}}(\xi_{n+1}) = \xi_n$. If $i \in I$, let $x_i = u_{i, i_{\varphi(n)}}(\xi_n)$ for $n \in \mathbf{Z}_{\geqslant 0}$ large enough so that $i \leqslant i_{\varphi(n)}$. Then $(x_i)_{i\in I} \in \varprojlim\limits_{i\in I} \widetilde{X}_i = \varprojlim\limits_{i\in I} X_i$, so the latter is nonempty □

Remark 1.11.15. Some examples that show that the hypothesis are really necessary in the previous lemma.
(1) Put $I = \mathbf{Z}_{\geqslant 0}$, $X_n = \mathbf{Z}_{\geqslant 0}$, and $u_{n,m}\colon\ \mathbf{Z}_{\geqslant 0} \to \mathbf{Z}_{\geqslant 0};\ x \mapsto x + m - n$ if $n \leqslant m$. An element in $X = \varprojlim\limits_{n} X_n$ is thus a sequence $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ such that $x_n = x_{n+1} + 1$, so that $x_n = x_0 - n$ for all $n \in \mathbf{Z}_{\geqslant 0}$. Such sequences do not exist, so $X = \varnothing$.
(2) Put $I = \mathbf{Z}_{\geqslant 0}$, $X_n =]0, 1[$, and $u_{n,m}\colon X_m \to X_n;\ x \mapsto \frac{x}{2^{m-n}}$. Then $u_{0,n}(X_n) = \big]0, \frac{1}{2^n}\big[$, so that if $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in X = \varprojlim\limits_{n} X_n$, we have $x_0 \in \bigcap\limits_{n=0}^{\infty} \big]0, \frac{1}{2^n}\big[= \varnothing$.

(3) For each finite subset $A \subset \mathbf{R}$, let X_A be the set of injections $A \to \mathbf{N}$. If $A \subset B$, the restriction provides a surjective map $X_B \to X_A$, so we get an inverse system (indexed by the finite subsets of $\mathbf{R}$, partially ordered by the inclusion) with surjective transition maps. However, the inverse limit is the set of injections from $\mathbf{R}$ to $\mathbf{N}$: it is empty (this example is due to Waterhouse).

Proposition 1.11.16. Let

$$0 \to \big(\{X'_i\}_{i\in I}, \{u'_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big) \xrightarrow{(f_i)_{i\in I}} \big(\{X_i\}_{i\in I}, \{u_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big) \xrightarrow{(g_i)_{i,j\in I}} \big(\{X''_i\}_{i\in I}, \{u''_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big) \to 0$$

be an exact sequence of inverse systems indexed by I in $\mathbf{Mod}_R$ (where R is a commutative ring). Assume that I is countable and that $\big(\{X'_i\}_{i\in I}, \{u'_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ has the Mittag-Leffler property. Then the sequence

$$0 \to \varprojlim_{i\in I} X'_i \xrightarrow{f} \varprojlim_{i\in I} X_i \xrightarrow{g} \varprojlim_{i\in I} X''_i \to 0$$

is exact.

Proof. By proposition 1.11.10, it is enough to show the surjectivity of g. Let $x'' = (x''_i)_{i\in I} \in \varprojlim_{i\in I} X''_i$. For $i \in I$, put $E_i = g_i^{-1}(\{x''_i\}) \subset X_i$: the set E_i is nonempty since g_i is surjective. If $j \geqslant i$ in I and $\xi \in E_j$, then $g_i(u_{i,j}(\xi)) = u''_{i,j}(g_j(\xi)) = u''_{i,j}(x''_j) = x''_i$ so that $u_{i,j}(\xi) \in E_i$. This implies that $(E_i, u_{i,j|E_j})_{i,j\in I}$ is a sub-inverse system of $(X_i, u_{i,j})_{i,j\in I}$: we have an inclusion $E := \varprojlim_{i\in I} E_i \subset \varprojlim_{i\in I} X_i$, and $g(x) = x''$ for any $x \in \varprojlim_{i\in I} E_i$. We have thus to show that E is nonempty. As I is countable, it is enough to check that the inverse system $\big(\{E_i\}_{i\in I}, \{u_{i,j|E_j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ satisfies the Mittag-Leffler condition (*cf* lemma 1.11.14).

As $\big(\{X'_i\}_{i\in I}, \{u'_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ has the Mittag-Leffler property, for each $i \in I$, there exists $n(i) \geqslant i$ in I such that $u_{i,j}(X'_j) = u_{i,n(i)}(X'_{n(i)})$ for all $j \geqslant n(i)$. Let $j \geqslant n(i)$. We have $u_{i,j}(E_j) \subset u_{i,n(i)}(E_{n(i)})$. Conversely, let $\xi \in E_{n(i)}$. If η is any element in E_j, we have $g_{n(i)}(u_{n(i),j}(\eta)) = u''_{n(i),j}(g_j(\eta)) = u''_{n(i),j}(x''_j) = x''_{n(i)} = g_{n(i)}(\xi)$, so that $\xi - u_{n(i),j}(\eta) \in \mathsf{Ker}(g_{n(i)}) = \mathsf{Im}(f_{n(i)})$: we can write $\xi - u_{n(i),j}(\eta) = f_{n(i)}(\lambda)$ with $\lambda \in X'_{n(i)}$. We have $u_{i,n(i)}(\xi) = u_{i,j}(\eta) + u_{i,n(i)}(f_{n(i)}(\lambda)) = u_{i,j}(\eta) + f_i(u'_{i,n(i)}(\lambda))$. As $u'_{i,n(i)}(\lambda) \in u'_{i,n(i)}(X'_{n(i)}) = u'_{i,j}(X'_j)$, there exists $\mu \in X'_j$ such that $u'_{i,n(i)}(\lambda) = u'_{i,j}(\mu)$, hence $u_{i,n(i)}(\xi) = u_{i,j}(\eta) + f_i(u'_{i,j}(\mu)) = u_{i,j}(\eta + f_j(\mu))$. As $\eta + f_j(\mu) \in E_j$, this shows that $u_{i,n(i)}(\xi) \in u_{i,j}(E_j)$, showing that the inverse system $\big(\{E_i\}_{i\in I}, \{u_{i,j|E_j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ satisfies the Mittag-Leffler condition indeed. □

1.11.17. *Profinite groups.*

Definition 1.11.18. A inverse limit of finite sets (resp. groups) is called a *profinite set* (resp. a *profinite group*). We endow these finite sets with the discrete topology, their product with the product topology and their inverse limit with the induced topology. Let p be a prime integer. A *pro-p-group* is an inverse limit of p-groups.

Proposition 1.11.19. Profinite sets are compact[(19)].

Proof. Let $\big(\{X_i\}_{i\in I}, \{u_{i,j}\}_{\substack{i,j\in I\\ i\leqslant j}}\big)$ be a inverse system of finite sets. Being finite, each X_i is compact: by Tychonoff's theorem, the product $\prod_{i\in I} X_i$ is compact as well. If $J \subset I$ is finite, let $\pi_J \colon \prod_{i\in I} X_i \to \prod_{i\in J} X_i$ be the projection on factors of index $\in J$, and $\varprojlim_J X_j$ the inverse limit of $\big(\{X_j\}_{j\in J}, \{u_{i,j}\}_{\substack{i,j\in J\\ i\leqslant j}}\big)$. Then $\pi_J(\varprojlim_I X_i) \subset \varprojlim_J X_j$, and $\varprojlim_I X_i = \bigcap_{\substack{J\subset I\\ J \text{ finite}}} \pi_J^{-1}(\varprojlim_J X_j)$. Since $\prod_J X_j$ is finite, $\varprojlim_J X_j$ is closed, so $\pi_J^{-1}(\varprojlim_J X_j)$ is closed in $\prod_{i\in I} X_i$ (by definition of the product topology). Being an intersection of closed subsets, $\varprojlim_I X_i$ is closed in $\prod_J X_j$, hence compact[(20)]. □

[(19)] Recall it means Hausdorff (*i.e.* separated) and quasi-compact.

[(20)] Another way of formulating it: $X = \bigcap_{i\leqslant j} (\pi_i, u_{i,j}\circ\pi_j)^{-1}(\Delta_P)$ where $P = \prod_{k\in I} X_k$ and $\Delta_P = \{(x,x)\,;\, x \in P\}$ is the diagonal of P. As Δ_P is closed in $P \times P$, the sets $(\pi_i, u_{i,j}\circ\pi_j)^{-1}(\Delta_P)$ are closed in P for all $i \leqslant j$, so that X is closed in P. As P is compact (by Tychonof's theorem), this shows that X is compact as well.

Remark 1.11.20. If G is a profinite group and $H \subset G$ an open subgroup, then H is closed as well: indeed $G \backslash H = \bigcup_{g \notin H} gH$ is a union of open subsets, so it is open. Similarly, if $H \leqslant G$ is a subgroup of finite index, it is open if and only if it is closed in G.

Proposition 1.11.21. Let G be a topological group. Then G is profinite if and only if it is compact, and admits a basis of neighborhoods of 1 consisting of normal subgroups.

Proof. Assume G is profinite: $G = \varprojlim_I G_i$. Since $\prod_I G_i$ is separated (each G_i is), so is G. Moreover G is compact thanks to the previous proposition. Finally, a basis of neighborhoods of 1 is given by $\{\mathsf{Ker}(\pi_i)\}_{i\in I}$ where π_i is the projection to the factor of index i, which consists of normal subgroups.
Conversely, assume G is Hausdorff, compact, and admits a basis of neighborhoods of 1 consisting of normal subgroups. Let $\{N_i\}_{i\in I}$ be the family of open normal subgroups. As G is compact, the quotient $G_i := G/N_i$ is finite for all $i \in I$. Write $i \leqslant j$ if $N_i \supset N_j$, so that I becomes a directed set (an upper bound of N_i and N_j is given by $N_i \cap N_j$). The family $\{G_i\}_{i\in I}$ is then a inverse system. The canonical maps $\pi_i\colon G \to G_i$ induce a canonical morphism $\psi\colon G \to \varprojlim_I G_i$. Its kernel is $\bigcap_I N_i = \{1\}$ (since $\{N_i\}_{i\in I}$ is a basis of neighborhoods of 1), so ψ is injective. A sub-basis of neighborhoods of 1 in $\prod_I G_i$ is given by $U_S = \prod_{i\in I\backslash S} G_i \times \prod_{i\in S}\{1\}$, where S runs through the finite subsets of I. As $\psi^{-1}(U_S) = \bigcap_{i\in S} N_i$ is open, the map ψ is continuous. In particular, as G is compact, $\psi(G)$ is compact hence closed inside $\varprojlim_I G_i$. In fact, ψ is surjective, because $\psi(G)$ is dense in $\varprojlim_I G_i$. Indeed, let $\underline{g} = (g_i)_{i\in I} \in \varprojlim_I G_i$ and S a finite subset of I; let $k \in I$ be such that $N_k = \bigcap_{i\in S} N_i$, and $g \in G$ a lift of $g_k \in G_k = G/N_k$. Then $g_i = g \mod N_i$ for all $i \in S$, so $\psi(g) \in \underline{g}(U_S \cap \psi(\varprojlim_I G_i))$. As ψ is a continuous and G is compact, it maps closed subsets to closed subsets: it is open. This shows that ψ is an isomorphism and a homeomorphism. □

Remark 1.11.22. If G is any group, its *profinite completion* is the natural map $G \to \varprojlim_{\substack{N \trianglelefteq G\\ [G:N]<\infty}} G/N$. In the previous proof, we have seen that G is profinite if and only if this is an isomorphism and a homeomorphism.

Example 1.11.23. (1) If p is a prime number, $\mathbf{Z}_p := \varprojlim_{n\in\mathbf{N}_{>0}} \mathbf{Z}/p^n\mathbf{Z}$.
(2) If we endow $\mathbf{N}_{>0}$ with the order given by $n \leqslant m \Leftrightarrow n \mid m$, then $\{\mathbf{Z}/n\mathbf{Z}\}_{n\in\mathbf{N}_{>0}}$ is an inverse system, whose inverse limit is denoted by $\widehat{\mathbf{Z}}$. This is the profinite completion of $\mathbf{Z}$.

Remark 1.11.24. The maps $\mathbf{Z} \to \mathbf{Z}_p$ and $\mathbf{Z} \to \widehat{\mathbf{Z}}$ are injective, but are not isomorphisms: their image is only dense (because $\mathbf{Z}/p^n\mathbf{Z} \to \mathbf{Z}_p/p^n\mathbf{Z}_p$ and $\mathbf{Z}/n\mathbf{Z} \to \widehat{\mathbf{Z}}/n\widehat{\mathbf{Z}}$ are isomorphisms for all $n \in \mathbf{N}_{>0}$).

Example 1.11.25. The natural map $\widehat{\mathbf{Z}} \xrightarrow{\sim} \prod_{p\in\mathbf{P}} \mathbf{Z}_p$ is an isomorphism and a homeomorphism. This follows from the Chinese remainder theorem.

1.11.26. *Completion of a ring with respect to an ideal.* References for this section are [17, §8] and [21, II §5]. Let $I \subset A$ be an ideal.

Definition 1.11.27. Let M be an A-module.
(1) The *I-adic topology* on M is the topology for which $\{I^nM\}_{n\in\mathbf{Z}_{>0}}$ is a basis of neighborhoods of 0.
(2) The *I-adic completion* of M is $\widehat{M} = \varprojlim_{n\in\mathbf{Z}_{>0}} M/I^nM$. The A-module M is *I-adically complete* when the natural map $M \to \widehat{M}$ is bijective.

Remark 1.11.28. (1) The I-adic topology on M is separated if and only if $\bigcap_{n=1}^{\infty} I^nM = \{0\}$.
(2) The addition $M \times M \to M$ and the multiplication $A \times M \to M$ are continuous[21]. In particular, the ring operations are continuous on A for the I-adic topology.
(3) Each I^nM is open in M, hence also closed since its complement in M is the open $\bigcup_{m\notin I^nM} (m + I^nM)$: the quotient module M/I^nM is discrete.

[21] If $x, x', y, y' \in M$ are such that $x - x', y - y' \in I^nM$, then $(x + y) - (x' + y') \in I^nM$; moreover, if $a, a' \in A$ are such that $a - a' \in I^n$, then $ax - a'x' = a(x - x') + (a - a')x' \in I^nM$.

(4) $\widehat{M}$ is an $\widehat{A}$-module.
(5) If $f\colon M_1 \to M_2$ is an A-linear map, then $f(I^n M_1) \subset I^n M_2$, so f induces a map $M_1/I^n M_1 \to M_2/I^n M_2$ for all $n \in \mathbf{Z}_{>0}$, hence a map $\widehat{f}\colon \widehat{M_1} \to \widehat{M_2}$ between the I-adic completions.
(6) In general, $\widehat{M}$ is I-adically separated, but if $n \in \mathbf{Z}_{>0}$, the natural map $M/I^n M \to \widehat{M}/I^n\widehat{M}$ may *not* be an isomorphism, and the map $\widehat{M} \to \widehat{\widehat{M}}$ not an isomorphism, *i.e.* $\widehat{M}$ may not be complete for the I-adic topology.

Lemma 1.11.29. Let A be a ring, $\mathfrak{m} \subset A$ a maximal ideal. Denote by $\widehat{A}$ (resp. $\widehat{A_\mathfrak{m}}$) the completion of A (resp. $A_\mathfrak{m}$) with respect to the $\mathfrak{m}$-adic (resp. $\mathfrak{m}A_\mathfrak{m}$-adic) topology. The natural map $\widehat{A} \to \widehat{A_\mathfrak{m}}$ is an isomorphism.

Proof. Let $n \in \mathbf{Z}_{>0}$. As localization is an exact functor, we have $A_\mathfrak{m}/\mathfrak{m}^n A_\mathfrak{m} = \overline{S}^{-1}(A/\mathfrak{m}^n)$ where $\overline{S}$ denotes the image of $S = A\backslash\mathfrak{m}$ in $A/\mathfrak{m}^n$. If $x \in \overline{S}$, the image of x in $A/\mathfrak{m}$ is nonzero, hence invertible since $\mathfrak{m}$ is maximal: there exists $y \in A/\mathfrak{m}^n$ such that $xy \equiv 1 \mod \mathfrak{m}/\mathfrak{m}^n$, so that $xy - 1$ is nilpotent. This implies that xy hence x is invertible in $A/\mathfrak{m}^n$. In particular, the map $A/\mathfrak{m}^n \to A_\mathfrak{m}/\mathfrak{m}^n A_\mathfrak{m}$ induced by $A \to A_\mathfrak{m}$ is an isomorphism for all $n \in \mathbf{Z}_{>0}$: passing to the limit, the map $\widehat{A} \to \widehat{A_\mathfrak{m}}$ is an isomorphism. □

Example 1.11.30. Assume $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are pairwise distinct maximal ideals in A and $e_1, \ldots, e_r \in \mathbf{Z}_{>0}$. Put $I = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_r^{e_r}$. Denote by $\widehat{A}_{\mathfrak{m}_i}$ the completion of the local ring $A_{\mathfrak{m}_i}$ with respect to the $\mathfrak{m}_i A_{\mathfrak{m}_i}$-topology. The natural map

$$\widehat{A} \to \bigoplus_{i=1}^{r} \widehat{A}_{\mathfrak{m}_i}$$

is an isomorphism. Indeed, for all $n \in \mathbf{Z}_{>0}$, the natural map

$$A/I^n A \to \bigoplus_{i=1}^{r} A/\mathfrak{m}_i^{ne_i}$$

is an isomorphism (by the Chinese remainder theorem, *cf* 1.1.14). Passing to inverse limits provides an isomorphism $\widehat{A} \to \bigoplus\limits_{i=1}^{r} \varprojlim\limits_{n} A/\mathfrak{m}_i^{ne_i}$: we conclude by lemma 1.11.29.

Lemma 1.11.31. An A-module M is separated and complete for the I-adic topology if and only if Cauchy sequences in M converge.

Proof. The A-module M is separated and complete if and only if for any sequence $(m_k)_{k\in\mathbf{Z}_{>0}}$ such that $(\forall k \in \mathbf{Z}_{>0})\, m_{k+1} - m_k \in I^k M$, there exists a unique $m \in M$ such that $(\forall k \in \mathbf{Z}_{>0})\, m_k \equiv m \mod I^k M$. This certainly holds if Cauchy sequences converge. Conversely, assume that M is separated and complete and let $(x_i)_{i\in\mathbf{Z}_{>0}}$ be a Cauchy sequence in M. If $k \in \mathbf{Z}_{>0}$, there exists $\varphi(k) \in \mathbf{Z}_{>0}$ such that $i, j \geqslant \varphi(k) \Rightarrow x_i - x_j \in I^k M$. We can assume that the map φ is strictly increasing. Put $m_k = x_{\varphi(k)} \in M$: we have $m_{k+1} - m_k \in I^k M$ for all $k \in \mathbf{Z}_{>0}$, so there is a $m \in M$ such that $m_k \equiv m \mod I^k M$ for all $k \in \mathbf{Z}_{>0}$. If $i \geqslant \varphi(k)$, we have thus $x_i - m_{\varphi(k)}, m_{\varphi(k)} - m \in I^k M$, whence $x_i \equiv m \mod I^k M$, showing that $(x_i)_{i\in\mathbf{Z}_{>0}}$ converges to m. □

Corollary 1.11.32. If M is an A-module which is separated and complete for the I-adic topology, then a series $\sum\limits_{n=0}^{\infty} m_n$ converges in M if and only if its general term m_n tends towards 0.

Theorem 1.11.33. (Hensel's lemma). Let A be a local ring, $\mathfrak{m} \subset A$ its maximal ideal and $k = A/\mathfrak{m}$ its residue field. Assume that A is $\mathfrak{m}$-adically separated and complete, and let $F \in A[X]$ be a monic polynomial. Assume there are monic polynomials $g, h \in k[X]$ such that $\mathsf{gcd}(g, h) = 1$ and $gh = \overline{F}$, where $\overline{F}$ is the image of F in $k[X]$. Then there exist monic polynomials $F, G \in A[X]$ such that $F = GH$, and whose images in $k[X]$ are g and h respectively.

Proof. Note that the assumption imply that $\deg(g) + \deg(h) = d := \deg(P)$. Let $i \in \{0, \ldots, d-1\}$. As $\mathsf{gcd}(g, h) = 1$, there exist $u_i, v_i \in k[X]$ such that $gu_i - hv_i = X^i$. Replacing u_i by its remainder modulo h and v_i by its remainder modulo g, we may further assume[22] that $\deg(u_i) < \deg(h)$ and $\deg(v_i) < \deg(g)$. Choose lifts $U_i, V_i \in A[X]$ of u_i and v_i respectively such that $\deg(U_i) = \deg(u_i)$ and $\deg(V_i) = \deg(v_i)$.

[22] Let indeed $\tilde{u}_i$ and $\tilde{v}_i$ be these remainders: we have $u_i = \tilde{u}_i + h\delta_i$ with $\delta_i \in k[X]$, so that $g(\tilde{u}_i + h\delta_i) - hv_i = X^i$, *i.e.* $g\tilde{u}_i - h(v_i - g\delta_i) = X^i$. This implies that $\deg(h(v_i - g\delta_i)) = \deg(g\tilde{u}_i - X^i) < d$, thus $\deg(v_i - g\delta_i) < \deg(g)$, *i.e.* $v_i - g\delta_i = \tilde{v}_i$, and $g\tilde{u}_i - h\tilde{v}_i = X^i$.

Let $G_1, H_1 \in A[X]$ be *monic* lifts of g and h respectively (so that $\overline{G}_1 = g$ and $\overline{H}_1 = h$). We construct by induction *monic* polynomials $G_n, H_n \in A[X]$ such that

$$(*) \qquad \begin{cases} G_nH_n \equiv P \mod \mathfrak{m}^n[X] \\ G_{n+1} \equiv G_n \mod \mathfrak{m}^n[X] \\ H_{n+1} \equiv H_n \mod \mathfrak{m}^n[X] \end{cases}$$

for all $n \in \mathbf{Z}_{>0}$. Let $n \in \mathbf{Z}_{>0}$ be such that $\{G_i\}_{1\leqslant i\leqslant n}$ and $\{H_i\}_{1\leqslant i\leqslant n}$ have been constructed. Conditions $(*)$ imply that $\overline{G}_n = g$ and $\overline{H}_n = h$, and that[23] $\deg(G_n) = \deg(g)$ and $\deg(H_n) = \deg(h)$. This implies in particular that $\deg(G_nU_i - H_nV_i) < d$ and that $G_nU_i - H_nV_i \equiv X^i \mod \mathfrak{m}[X]$. Write $P - G_nH_n = \sum\limits_{i=0}^{d-1} \alpha_i X^i$ with $\alpha_0, \ldots, \alpha_{d-1} \in \mathfrak{m}^n$: we have $P - G_nH_n \equiv \sum\limits_{i=0}^{d-1} \alpha_i(G_nU_i - H_nV_i) \mod \mathfrak{m}^{n+1}[X]$. Put

$$\begin{cases} G_{n+1} = G_n - \sum\limits_{i=0}^{d-1} \alpha_i V_i \\ H_{n+1} = H_n + \sum\limits_{i=0}^{d-1} \alpha_i U_i \end{cases}$$

so that $G_{n+1} \equiv G_n \mod \mathfrak{m}^n[X]$ and $H_{n+1} \equiv H_n \mod \mathfrak{m}^n[X]$. We have

$$\begin{aligned} G_{n+1}H_{n+1} &\equiv G_nH_n + \sum_{i=0}^{d-1} \alpha_i(G_nU_i - H_nV_i) \mod \mathfrak{m}^{2n}[X] \\ &\equiv P \mod \mathfrak{m}^{n+1}[X] \end{aligned}$$

(as $n + 1 \leqslant 2n$), which completes the construction of the sequences $(G_n)_{n\in\mathbf{Z}_{>0}}$ and $(H_n)_{n\in\mathbf{Z}_{>0}}$. As A is separated and complete for the $\mathfrak{m}$-adic topology, these sequences converge in $A[X]$ (note that both are given by d sequences of coefficients): denote by G and H their limits. By construction we have $F = GH$. □

From now on, A is assumed to be *noetherian.*

Notation. • Put $\overline{A} = \bigoplus\limits_{n=0}^{\infty} I^n$: this is naturally an A-algebra (the product of x in the factor I^n with y in the factor I^m is xy in the factor I^{n+m}). As I is of finite type, so is $\overline{A}$ as an A-algebra: it is noetherian.
• More generally, let M be an A-module endowed with a decreasing filtration, *i.e.* a decreasing sequence of sub-A-modules $(M_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ such that $IM_n \subset M_{n+1}$ for all $n \in \mathbf{Z}_{\geqslant 0}$. The *associated graded group* is $\overline{M} = \bigoplus\limits_{n=0}^{\infty} M_n$. It is naturally endowed with an $\overline{A}$-module structure (the product of a in the factor I^n with m in the factor M_m is am in the factor M_{n+m}).

Lemma 1.11.34. Assume M is of finite type over A. The following properties are equivalent:

(i) $M_{n+1} = IM_n$ for n sufficiently large;
(ii) there exists $c \in \mathbf{Z}_{\geqslant 0}$ such that $M_{n+c} = I^nM_c$ for all $n \in \mathbf{Z}_{\geqslant 0}$;
(iii) $\overline{M}$ is a finitely generated $\overline{A}$-module.

Proof. (i)⇔(ii) is trivial. If (ii) holds then $\overline{M}$ is generated by $\sum\limits_{i=0}^{c} M_i$, so that we have (iii). Conversely, assume (iii): the $\overline{A}$-module $\overline{M}$ can be generated by finitely many elements $x_1, \ldots, x_r$, with x_i homogeneous, *i.e.* belonging to some factor $M_{n_i} \subset \overline{M}$ for $i \in \{1, \ldots, r\}$. Then $M_{n+1} = IM_n$ for all $n \geqslant c := \max\limits_{1\leqslant i\leqslant r} n_i$. □

Theorem 1.11.35. (Artin-Rees lemma). Let M be an A-module of finite type. If $N \subset M$ is a submodule, there exists $c \in \mathbf{Z}_{\geqslant 0}$ such that for every $n \in \mathbf{Z}_{\geqslant 0}$, we have $I^{n+c}M \cap N = I^n(I^cM \cap N)$ for all $n \in \mathbf{Z}_{\geqslant 0}$.

Proof. For $n \in \mathbf{Z}_{\geqslant 0}$, put $M_n = I^nM$ and $N_n = M_n \cap N$: we have $\overline{N} \subset \overline{M}$. As $\overline{A}$ is noetherian and $\overline{M}$ finitely generated as an $\overline{A}$-module (by lemma 1.11.34), so is $\overline{N}$: by lemma 1.11.34 again, there exists $c \in \mathbf{Z}_{\geqslant 0}$ such that $N_{n+c} = I^nN_c$ *i.e.* $I^{n+c}M \cap N = I^n(I^cM \cap N)$. □

Remark 1.11.36. This theorem essentially says that the I-adic topology on N coincides with the topology induced on N by the I-adic topology on M.

Corollary 1.11.37. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of A-modules of finite type. The sequence $0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0$ is exact.

[23] The degree of a monic polynomial is equal to that of its reduction modulo $\mathfrak{m}$.

Proof. By right exactness of the tensor product (*cf* proposition 1.7.5), the sequence

$$M'/I^nM' \to M/I^nM \to M''/I^nM'' \to 0$$

is exact (recall that $M/I^nM \simeq M \otimes_A (A/I^n))$ for all $n \in \mathbf{Z}_{\geqslant 0}$. On the other hand, there exists $c \in \mathbf{Z}_{\geqslant 0}$ such that $I^nM \cap M' = I^{n-c}(I^cM \cap M')$ for integers $n \geqslant c$ (Artin-Rees lemma, *cf* theorem 1.11.35). This implies that for $n \in \mathbf{Z}_{\geqslant c}$, we have

$$I^nM' \subset I^nM \cap M' = I^{n-c}(I^cM \cap M') \subset I^{n-c}M'$$

and the sequence

$$0 \to M'/(I^{n-c}(I^cM \cap M')) \to M/I^nM \to M''/I^nM'' \to 0$$

is exact. This gives an exact sequence of inverse systems. The inverse system $(M'/(I^{n-c}(I^cM \cap M')))_{n \in \mathbf{Z}_{>0}}$ has the Mittag-Leffler property (the transition maps are *surjective*): by proposition 1.11.16, the sequence

$$0 \to \varprojlim_n M'/(I^{n-c}(I^cM \cap M')) \to \widehat{M} \to \widehat{M}'' \to 0$$

is exact. Moreover, the surjective maps

$$M'/I^nM' \to M'/(I^{n-c}(I^cM \cap M')) \to M'/I^nM'$$

provide surjective maps $\widehat{M}' \to \varprojlim_n M'/(I^{n-c}(I^cM \cap M')) \to \widehat{M}'$ (here again the surjectivity follows from the Mittag-Leffler condition satisfied by the kernels of these maps), whose composite is the identity: we have $\varprojlim_n M'/(I^{n-c}(I^cM \cap M')) \xrightarrow{\sim} \widehat{M}'$ hence the result. □

Corollary 1.11.38. Let M be an A-module of finite type. Then $\widehat{A} \otimes_A M \xrightarrow{\sim} \widehat{M}$.

Proof. This is obvious when M is free. In the general case, let $L_1 \to L_0 \to M \to 0$ be an exact sequence where L_0 and L_1 are free of finite rank (such a sequence exists since M in of finite type and A noetherian). The exactness of completion on short exact sequences of A-modules of finite type imply that the sequence $\widehat{L}_1 \to \widehat{L}_0 \to \widehat{M} \to 0$ is exact. We thus have the following commutative diagram with exact rows

$$\begin{tikzcd}
\widehat{A} \otimes_A L_1 \arrow[r] \arrow[d, "\phi_1"'] & \widehat{A} \otimes_A L_0 \arrow[r] \arrow[d, "\phi_0"'] & \widehat{A} \otimes_A M \arrow[r] \arrow[d, "\phi"'] & 0 \\
\widehat{L}_1 \arrow[r] & \widehat{L}_0 \arrow[r] & \widehat{M} \arrow[r] & 0
\end{tikzcd}$$

As ϕ_0 and ϕ_1 are isomorphisms, so is ϕ. □

Corollary 1.11.39. $\widehat{A}$ is flat over A.

Proof. This follows from corollaries 1.11.37 and 1.11.38. □

1.12. **Exercises.** The following two exercises show that the ring $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ is not euclidean, though a PID.

Exercise 1.12.1. Put $A = \mathbf{Z}[\zeta]$ where $\zeta^2 - \zeta + 5 = 0$. We denote by N the norm of the number field $\mathbf{Q}[\zeta]$.
(1) Compute $N(x + y\zeta)$ for $x, y \in \mathbf{Q}$ an determine $\mathbf{Z}[\zeta]^\times$.
(2) Let $a, b \in \mathbf{Z}[\zeta]\backslash\{0\}$. Show that there exist $q, r \in \mathbf{Z}[\zeta]$ such that: ($r = 0$ or $N(r) < N(b)$) and ($a = bq + r$ or $2a = bq + r$).
(3) Show that the ideal $2\,\mathbf{Z}[\zeta]$ is maximal in A.
(4) Show that A is a PID.

Exercise 1.12.2. Let A be an integral domain which is not a field. We construct (by induction on $n \in \mathbf{Z}_{\geqslant 0}$) a sequence of subsets of A by: $A_0 = \{0\}$ and $A_{n+1} = A_n \cup \{x \in A\,;\, A = xA + A_n\}$ for all $n \in \mathbf{Z}_{\geqslant 0}$. For $x \in \bigcup_{n=0}^{\infty} A_n$, we put $\phi(x) = \inf\{n \in \mathbf{Z}_{\geqslant 0}\,;\, x \in A_n\}$.

(1) Assume that $A = \bigcup_{n=0}^{\infty} A_n$. Show that A euclidean for the euclidean function ϕ.
(2) Assume that A is euclidean for a euclidean function $\psi\colon A\backslash\{0\} \to \mathbf{Z}_{>0}$. Show that:
  (i) $\phi(x) \leqslant \psi(x)$ for all $x \in \bigcup_{n \in \mathbf{N}} A_n$;
  (ii) $A = \bigcup_{n=0}^{\infty} A_n$ [Hint: reductio ad absurdum using (i));
  (iii) A is euclidean for the euclidean function ϕ;
  (iv) if a divides b in A, then $\phi(a) \leqslant \phi(b)$;

(v) there exists $x \in A \backslash A^\times$ such that the restriction of the projection $A \to A/xA$ to $A^\times \cup \{0\}$ is surjective.

(3) Determine ϕ in the following cases: $A = \mathbf{Z}$ and $A = k[X]$ (where k is a field).

(4) Let $A = \mathbf{Z}[\zeta] \subset \mathbf{C}$ where $\zeta^2 - \zeta + 5 = 0$.

(i) Show that the equation $z^2 - z + 5 = 0$ has no solution in $\mathbf{F}_2$ nor in $\mathbf{F}_3$.

(ii) Deduce that A is not euclidean [Hint: reductio ad absurdum using (2-v)].

Exercise 1.12.3. Let A be a domain.
(1) Show that if A is a UFD if and only if non-zero elements can be factored into a product of irreducible elements, and irreducible elements are prime in A.
(2) Show that if A is noetherian, non-zero elements can be factored into a product of irreducible elements.
(3) Give an example of non noetherian UFD.

Exercise 1.12.4. Let A be a UFD, and $S \subset A$ a multiplicative part. Show that $S^{-1}A$ is a UFD.

Exercise 1.12.5. Let A be a domain and $f, g \in A$ such that $A\big[\frac{1}{f}\big] \cap A\big[\frac{1}{g}\big] = A \subset \mathsf{Frac}(A)$. Show that the map $A[X] \to A\big[\frac{f}{g}\big]; P \mapsto P\big(\frac{f}{g}\big)$ (resp. $A\big[X, \frac{1}{X}\big] \to A\big[\frac{f}{g}, \frac{g}{f}\big]; P \mapsto P\big(\frac{f}{g}\big)$) is surjective, with kernel $\langle gX - f\rangle$ (resp. $\big\langle gX - f, \frac{f}{X} - g\big\rangle$).

Exercise 1.12.6. Let A be a ring, M an A-module of finite type and $\varphi\colon M \to A^n$ a surjective morphism. Show that $M = N \oplus \mathsf{Ker}(\varphi)$, where N is a submodule of M isomorphic to A^n through φ. Show that $\mathsf{Ker}(\varphi)$ is of finite type.

Exercise 1.12.7. Let A be an integral domain and M an A-module. Assume that M can be generated by n elements, and contains a submodule which is free of rank n. Show that M is free of rank n.

Exercise 1.12.8. (1) Let L/K is a finite Galois extension with group G. Show that the natural map

$$\begin{aligned} L \otimes_K L &\to \bigoplus_{\sigma \in G} L \\ x \otimes y &\mapsto (x\sigma(y))_{\sigma \in G} \end{aligned}$$

is an isomorphism of L-algebras (for the left structure on the LHS, and the componentwise on the RHS).
(2) More generally, let L/K be a finite separable extension, and F/K be any extension. Show that $L \otimes_K F$ is isomorphic, as an F-algebra, to a finite product of separable extensions of F.
(3) Is it still true when L/K is not assumed to be separable?

Exercise 1.12.9. (Nakayama's lemma). Let A be a ring, $I \subset A$ an ideal and M an A-module of finite type such that $IM = M$.
(1) Show that there exists an element $a \in A$ such that $a \equiv 1 \mod I$ and $aM = \{0\}$.
(2) Deduce that if $I \subset \mathsf{rad}(A)$, then $M = \{0\}$.
(3) Assume that A is local and denote by k its residue field. Show that if $k \otimes_A M = \{0\}$, then $M = \{0\}$.
(4) Give a counter-example of (3) when M is not assumed to be of finite type.

Exercise 1.12.10. (Nakayama's lemma, continuation). Assume that A is local, with residue field k, and let M be an A-module of finite type, N an A-module.
(1) If N is of finite type over A and $M \otimes_A N = \{0\}$, show that $M = \{0\}$ or $N = \{0\}$.
(2) Let $f\colon N \to M$ be an A-linear map such that $\mathsf{Id}_k \otimes f\colon k \otimes_A N \to k \otimes_A M$ is surjective. Show that f is surjective.

Exercise 1.12.11. Let A be a ring and $I \subset A$ be an ideal of finite type such that $I^2 = I$. Show that I is generated by an element $e \in I$ such that $e^2 = e$.

Exercise 1.12.12. Let A be a ring, M an A-module of finite type and $f \in \mathsf{End}_A(M)$ a surjective endomorphism. Show that f is injective.

Exercise 1.12.13. Let A be a ring. Show the following:
(i) if $A^n \simeq A^m$ then $n = m$;
(ii) if there exists a surjective A-linear map $A^n \to A^m$ then $n \geqslant m$;
(iii) [difficult] if there exists an injective A-linear map $A^n \to A^m$, then $n \leqslant m$.

Exercise 1.12.14. Let A be a domain and M an torsion-free A-module. Let Σ be a set of maps $\sigma\colon M \to M$, each of which is semi-linear with respect to a ring endomorphism σ of A, *i.e.* such that $\sigma(am) = \sigma(a)\sigma(m)$ for all $a \in A$ and $m \in M$. If $\mathsf{Frac}(A)^\Sigma = A^\Sigma$, show that the natural map $\alpha\colon B \otimes_{B^\Sigma} M^\Sigma \to M$ is injective.

Exercise 1.12.15. Let A be a ring. An A-module P is *projective* if the functor $\mathsf{Hom}_A(P, .)$ is exact, *i.e.* whenever a sequence

$$0 \to M' \to M \to M'' \to 0$$

is exact, so is the sequence

$$0 \to \mathsf{Hom}_A(P, M') \to \mathsf{Hom}_A(P, M) \to \mathsf{Hom}_A(P, M'') \to 0.$$

(1) Show that a free module is projective.
(2) Show that an A-module is projective if and only if it is a direct factor of a free module.

Definition 1.12.16. Let A be a ring. An A-module M is *of finite presentation* if there exists an exact sequence

$$L' \to L \to M \to 0$$

where L, L' are free A-modules of finite rank, *i.e.* if there exists a surjective A-linear map $u\colon L \to M$ such that L is free of finite rank and $\mathsf{Ker}(u)$ of finite type. Being of finite presentation implies being of finite type, but the converse is false in general. It holds true when A is noetherian.

Exercise 1.12.17. (Snake lemma). Let A be a commutative ring.
(1) Assume there is a commutative diagram of A-modules

$$\begin{tikzcd}
 & M' \arrow[r, "a"] \arrow[d, "u"'] & M \arrow[r, "b"] \arrow[d, "v"'] & M'' \arrow[r] \arrow[d, "w"'] & 0 \\
0 \arrow[r] & N' \arrow[r, "c"] & N \arrow[r, "d"] & N'' &
\end{tikzcd}$$

with exact rows. Show that there is an exact sequence of A-modules

$$\mathsf{Ker}(u) \xrightarrow{a} \mathsf{Ker}(v) \xrightarrow{b} \mathsf{Ker}(w) \xrightarrow{\delta} \mathsf{Coker}(u) \xrightarrow{b} \mathsf{Coker}(v) \xrightarrow{d} \mathsf{Coker}(w).$$

(2) Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of A-modules with M of finite type and M'' of finite presentation. Show that M' is of finite type.

Exercise 1.12.18. Let A be a local ring, with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$.
(1) Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of A-modules with M'' flat over A. Show that the sequence $0 \to k \otimes_A M' \to k \otimes_A M \to k \otimes_A M'' \to 0$ is exact.
(2) Let M be an A-module. Show that the following are equivalent:

(i) M is flat of finite presentation;
(ii) M is free of finite rank.

(in particular, when A is noetherian, then M is free of finite rank if and only if it is flat of finite type).
(3) Deduce that an A-module is projective of finite type if and only if it is free of finite rank.

Exercise 1.12.19. Let A be a ring and M an A-module. Show that the following are equivalent:

(i) M is projective of finite type over A;
(ii) M is flat and finitely presented over A.

Exercise 1.12.20. Let A be a local ring with maximal ideal $\mathfrak{m}$ and $k = A/\mathfrak{m}$ its residue field. Let $u\colon M \to N$ be an A-linear map such that M is of finite type, N is projective, and $k \otimes u\colon k \otimes_A M \to k \otimes_A N$ is injective.
(1) Show that M is free of finite rank.
(2) Show that u is left invertible (*i.e.* there exists an A-linear map $v\colon N \to M$ such that $v \circ u = \mathsf{Id}_M$).

Exercise 1.12.21. Let R be a ring, $M = R^{\mathbf{Z}_{>0}}$ and $A = \mathsf{End}_R(M)$: this is a noncommutative ring. Use the maps

$$\begin{aligned}\varphi_1 &\colon M \to M;\ (x_1, x_2, \ldots) \mapsto (x_1, x_3, x_5, \ldots)\\ \varphi_2 &\colon M \to M;\ (x_1, x_2, \ldots) \mapsto (x_2, x_4, x_6, \ldots)\\ \psi_1 &\colon M \to M;\ (x_1, x_2, \ldots) \mapsto (x_1, 0, x_2, 0, \ldots)\\ \psi_2 &\colon M \to M;\ (x_1, x_2, \ldots) \mapsto (0, x_1, 0, x_2, \ldots)\end{aligned}$$

to show that $A^2 \simeq A$ (as left A-modules), so that the rank of a free module is not well defined in the non commutative setting.

Exercise 1.12.22. Let K be a field and A the sub-K-algebra of $K[X, Y]$ generated by $\{X^kY^{k+1}\}_{k\in\mathbf{Z}_{\geqslant 0}}$. Show that $A[XY]$ is included in a sub-A-module of $K[X, Y]$ of finite type, but that XY is not integral over A.

Exercise 1.12.23. Let $A \subset B$ be a ring extension with A noetherian, $x \in B^\times$, and $y \in A[x] \cap A[x^{-1}]$. Show that there exists $n \in \mathbf{Z}_{\geqslant 0}$ such that the sub-A-module $M = A + Ax + \cdots + Ax^n \subset B$ is stable under multiplication by y, and that y is integral over A.

Exercise 1.12.24. Let A be a domain and $\alpha \in A\backslash\{0\}$. Assume that $A/\alpha A$ is reduced and that $A[\alpha^{-1}]$ is integrally closed. Show that A is integrally closed.

Exercise 1.12.25. Let $A \to B$ be an integral morphism of rings, $\mathfrak{p}_1 \subset \mathfrak{p}_2$ prime ideals in B such that $\mathfrak{p}_1 \cap A = \mathfrak{p}_2 \cap A$. Show that $\mathfrak{p}_1 = \mathfrak{p}_2$.

Exercise 1.12.26. Let A be a ring, $A \subset B$ a finitely generated integral extension, and $\mathfrak{p} \subset A$ a prime ideal. Show that B has only a finite number of prime ideals lying over $\mathfrak{p}$.

Exercise 1.12.27. (1) Let $(X_n, \rho_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ be an inverse system of finite and non empty sets. Show that $X = \varprojlim_n X_n$ is non empty. [Hint: reduce to the case where the maps ρ_n are surjective.]
(2) Give an example of an inverse system (indexed by $\mathbf{Z}_{\geqslant 0}$) of non empty sets whose inverse limit is empty.

Exercise 1.12.28. Prove that any continuous bijection from one profinite group to another is a homeomorphism.

Exercise 1.12.29. Let G and H be profinite groups, and let $f\colon G \to H$ be a continuous group homomorphism. Prove that $\mathsf{Ker}(f)$ is a closed normal subgroup of G, that $f(G)$ is a closed subgroup of H, and that f induces an isomorphism $G/\mathsf{Ker}(f) \xrightarrow{\sim} f(G)$ of profinite groups (here $G/\mathsf{Ker}(f)$ has the quotient topology induced by the topology on G, and $f(G)$ has the relative topology induced by the topology on H.

Exercise 1.12.30. The profinite completion of a group G is the profinite group $\widehat{G} = \varprojlim_N G/N$, with N ranging over the set of normal subgroups of G of finite index in G, ordered by containment, the transition maps being the natural ones.
(1) Prove that there is a natural group homomorphism $\varphi_G\colon G \to \widehat{G}$, and that its image is dense in G. Find a group G for which it is not injective.
(2) Prove that φ_G is an isomorphism if and only if G is profinite.
(3) What is the profinite completion of the additive group of $\mathbf{Z}$?

Exercise 1.12.31. Let p be a prime number.
(1) Show that there is a group G whose profinite completion is isomorphic to the additive group $\mathbf{Z}_p$. Can you find such a G that is countable?
(2) Let A be the product of a countably infinite collection of copies of $\mathbf{Z}/p\mathbf{Z}$. Is there a countable group G such that A is isomorphic to the profinite completion of G?

Exercise 1.12.32. Show that for a profinite group G the following are equivalent:

(i) the topology of G is induced by a metric;

(ii) $G \simeq \varprojlim_n G_n$, with G_n finite and $G_{n+1} \to G_n$ surjective for all $n \in \mathbf{Z}_{\geqslant 0}$;

(iii) the number of open subgroups of G is countable.

Show that the equivalent conditions (i)-(iii) imply that G contains a countable dense subset (so G is *separable* as a topological space), and give an example showing that the converse does not hold.

Exercise 1.12.33. Let p be a prime. Give examples of groups that are not separated for the p-adic topology.

Exercise 1.12.34. Let A be a topological group. We say that A is profinite when the underlying abelian group is profinite.
(1) Show that if A is profinite, then the natural map $A \to \varprojlim_I A/I$ is an isomorphism (where I runs through the closed ideals of finite index in A).
(2) Assume that A is noetherian, local and that its topology is given by the powers if its maximal ideal. Show that A is profinite if and only if its residue field is finite.

Exercise 1.12.35. Find examples where Artin-Rees lemma's conclusion does not hold because one of its assumptions is not fulfilled [Hint: try $A = \mathbf{Q}[X, Z, Y_1, Y_2, \ldots]/\langle X - Z^i Y_i\rangle_{i \in \mathbf{Z}_{>0}}$ for the non noetherian case.]

Exercise 1.12.36. Let A be a ring, $I \subset A$ and $f\colon N \to M$ a surjective A-linear map. Show that the map induced on the I-adic completions $\widehat{f}\colon \widehat{N} \to \widehat{M}$ is surjective. Deduce that if M is an A-module of finite type, the natural map $\widehat{A} \otimes_A M \to \widehat{M}$ is surjective.

Exercise 1.12.37. Let A be a ring, $\alpha \in A$ and $M \subset N$ two A-modules. Assume that M is complete and N separated for the α-adic topology and that the induced map $M \to N/\alpha N$ is surjective. Show that $M = N$.

Exercise 1.12.38. (1) Let A be a ring, $\alpha \in A$ and N a torsion-free A-module which is separated and complete for the α-adic topology. Let $M \subset N$ be a sub-A-module: the inclusion extends into an A-linear map $f\colon \widehat{M} \to N$ where $\widehat{M} = \varprojlim_n M/\alpha^n M$ is the α-adic completion of M. Show that if $\alpha^i N \cap M \subset \alpha M$ for some $i \in \mathbf{Z}_{>0}$, then f is injective [hint: show that $\alpha^{i+k} N \cap M \subset \alpha^{k+1} M$ for all $k \in \mathbf{Z}_{\geqslant 0}$].
(2) Let p be a prime, $A = \mathbf{Z}_p$, $N = \mathbf{Z}_p[\![X]\!]$ and $M = \mathbf{Z}_p(pT) \oplus \bigoplus_{n=1}^{\infty} \mathbf{Z}_p(pT^{n+1} + T^n) \subset N$. Show that $x = pt - p(pT^2 + T) + p^2(pT^3 + T^2) - \cdots$ defines a non-zero element in $\widehat{M}$, whose image in N is zero.

Exercise 1.12.39. Let A be a ring, $I \subset A$ an ideal and $0 \to M_1 \to M_2 \to M_3 \to 0$ an exact sequence of A-modules. Assume M_3 is annihilated by a power of I. Then completion produces an exact sequence $0 \to \widehat{M_1} \to \widehat{M_2} \to M_3 \to 0$.

Exercise 1.12.40. Let A be a ring, $I \subset A$ and M an A-module. Denote by $\widehat{M}$ the I-adic completion of M.
(1) Show that $\widehat{M}$ is I-adically separated.
(2) Show that the following are equivalent:

(i) the A-module $\widehat{M}$ is I-adically complete;

(ii) for all $n \in \mathbf{Z}_{>0}$, the natural map $M/I^n M \to \widehat{M}/I^n\widehat{M}$ is surjective;

(iii) for all $n \in \mathbf{Z}_{>0}$, we have $I^n\widehat{M} = \mathsf{Ker}(\pi_n)$ where $\pi_n\colon \widehat{M} \to M/I^n M$ is the canonical map.

(3) Let K be a field, $A = K[X_i]_{i \in \mathbf{Z}_{>0}}$ and $I = \langle X_i\rangle_{i \in \mathbf{Z}_{>0}} \subset A$. Show that $\widehat{A}$ is *not* I-adically complete.
(4) Assume that I is finitely generated. Show that $I^n\widehat{M} = \mathsf{Ker}(\widehat{M} \to M/I^n M) = \widehat{I^n M}$ for all $n \in \mathbf{Z}_{\geqslant 0}$ and that $\widehat{M}$ is I-adically complete.

Exercise 1.12.41. Let A be ring, $I \subset A$ an ideal and M an A-module.
(1) Show that if A is I-adically separated and complete, then $I \subset \mathsf{rad}(A)$.
(2) Show that if M is I-adically separated and complete and $a \in I$, the multiplication by $1 + a$ is an automorphism of M.

Exercise 1.12.42. (Completion is not an exact functor.) Let K be a field, $A = K[X]$, $M = A^{(\mathbf{Z}_{>0})}$ and $C = \bigoplus\limits_{n=1}^{\infty} A/X^nA$. Show that the completion for the X-adic topology of the natural exact sequence $0 \to M \to M \to C \to 0$ is not exact.

Exercise 1.12.43. (Formal Nakayama's lemma). Let A be a ring, $I \subset A$ an ideal such that A is I-adically separated and complete, and M an A-module of finite type.
(1) Show that if $M = IM$, then $M = \{0\}$.
(2) Assume that $f\colon M' \to M$ is an A-linear map such that $f \otimes (A/I)$ is surjective. Show that f is surjective.

Exercise 1.12.44. Let A be a ring, $I \subset A$ an ideal and M an A-module. Assume that A is I-adically separated and complete, and that M is separated for the I-adic topology. Assume there are $m_1, \dots, m_r \in M$ whose images $\overline{m}_1, \dots, \overline{m}_r \in M/IM$ generate M/IM. Show that $m_1, \dots, m_r$ generate the A-module M.

Exercise 1.12.45. Let A be a noetherian local ring, with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$. Show that the $\mathfrak{m}$-adic completion $\widehat{A}$ of A is a local ring with maximal ideal $\mathfrak{m}\widehat{A}$, and residue field k.

Exercise 1.12.46. Let A be a DVR, $\mathfrak{m}$ its maximal ideal, and $\widehat{A}$ the $\mathfrak{m}$-adic completion of A. Show that $\widehat{A}$ is a DVR.

Exercise 1.12.47. Let A be a complete DVR with uniformizer π and M an A-module. Let $K = \mathsf{Frac}(A)$ and $k = A/\pi A$ the residue field. Put $M_K := K \otimes_A M$ and $M_k = K \otimes_A M$. Assume that M is flat (*i.e.* torsion-free) and that $\dim_K(M_K) = \dim_k(M_k) < +\infty$. Show that M is free of finite rank over A. Give a counter-example without the flatness assumption.

Exercise 1.12.48. (Krull intersection theorem). Let A be a noetherian ring and $I \subset A$ an ideal.
(1) Let M be an A-module of finite type and $N = \bigcap\limits_{n=0}^{\infty} I^nM$. Then there exists $a \in A$ such that $a \equiv 1 \mod I$ and $aN = 0$.
(2) If $I \subset \mathsf{rad}(A)$, then any A-module of finite type is I-adically separated, and its submodules are all closed.
(3) If A is a domain and I a proper ideal, then $\bigcap\limits_{n=0}^{\infty} I^n = \{0\}$.

Exercise 1.12.49. Let A be a noetherian ring and $I = \langle \xi_1, \dots, \xi_n \rangle$ be an ideal. Let $\widehat{A}$ be the I-adic completion of A. Then there is a isomorphism

$$A[\![X_1, \dots, X_n]\!]/\langle X_1 - \xi_1, \dots, X_n - \xi_n \rangle \xrightarrow{\sim} \widehat{A}$$

that maps X_i to ξ_i for all $i \in \{1, \dots, n\}$.

Exercise 1.12.50. Let A be a noetherian ring and $I, J \subset A$ ideals. Assume that A is both I-adically and J-adically separated and complete. Show that A is $I + J$-adically separated and complete.

Exercise 1.12.51. Let A be a noetherian ring and $J \subset I \subset A$ ideals such that A is I-adically separated and complete. Show that A is also J-adically separated and complete.

Exercise 1.12.52. Let A be a ring, $I = \langle f_1, \dots, f_r \rangle \subset A$ a finitely generated ideal, M an A-module and $\widehat{M}$ its I-adic completion.
(1) Show that if $M \to \varprojlim\limits_{n} M/f_i^nM$ is surjective for each $i \in \{1, \dots, r\}$, then $M \to \widehat{M}$ is surjective.
(2) Let $J \subset A$ be an ideal such that $I \subset J$. Show that if M is J-adically complete, then M is I-adically complete.

Exercise 1.12.53. (1) Let $g \in \mathbf{Z}_{>1}$, and define $\mathbf{Z}_g = \varprojlim\limits_{n} \mathbf{Z}/g^n\mathbf{Z}$. Prove that $\mathbf{Z}_g$ is a profinite group isomorphic to $\prod\limits_{p|g} \mathbf{Z}_p$, the product ranging over the primes p dividing g.
(2) Prove that $\widehat{\mathbf{Z}} \simeq \prod\limits_{p} \mathbf{Z}_p$, the product ranging over all primes p.

Exercise 1.12.54. (1) Prove that each $a \in \hat{\mathbf{Z}}$ has a unique representation as $a = \sum_{n=1}^{\infty} c_n n!$, with $c_n \in \{0, \ldots, n\}$ for all $n \in \mathbf{Z}_{>0}$. Give this representation for $a = -1$.
(2) Let $b \in \mathbf{Z}_{\geqslant 0}$, and define the sequence $(a_n)_{n \in \mathbf{Z}_{\geqslant 0}}$ of non-negative integers by $a_0 = b$ and $a_{n+1} = 2^{a_n}$. Prove that $(a_n)_{n \in \mathbf{Z}_{\geqslant 0}}$ converges in $\hat{\mathbf{Z}}$ and that the limit is independent of the choice of b.
(3) Let $a = \lim_{n \to \infty} a_n$ be the limit of the sequence in (2), and write $a = \sum_{n=1}^{\infty} c_n n!$. Determine c_n for $1 \leqslant n \leqslant 10$.

Exercise 1.12.55. Show that $\hat{\mathbf{Z}} \simeq \mathsf{End}(\mathbf{Q}/\mathbf{Z})$ and $\hat{\mathbf{Z}}^\times \simeq \mathsf{Aut}(\mathbf{Q}/\mathbf{Z})$.

Exercise 1.12.56. (1) Prove that for every positive integer n the natural map $\mathbf{Z}/n\mathbf{Z} \to \hat{\mathbf{Z}}/n\hat{\mathbf{Z}}$ is an isomorphism.
(2) Prove that there is a bijection from the set of positive integers to the set of open subgroups of $\hat{\mathbf{Z}}$ mapping n to $n\hat{\mathbf{Z}}$.
(3) Can you classify all closed subgroups of $\hat{\mathbf{Z}}$?

Exercise 1.12.57. Let p be a prime number and view $\mathbf{Z}_p = \varprojlim_n \mathbf{Z}/p^n\mathbf{Z}$ as a closed subset of $A = \prod_{n=1}^{\infty} \mathbf{Z}/p^n\mathbf{Z}$.
(1) Prove that $A/\mathbf{Z}_p \simeq A$ as profinite groups.
(2) Prove that A and $\mathbf{Z}_p \times (A/\mathbf{Z}_p)$ are isomorphic as groups, but not as profinite groups.

Exercise 1.12.58. Prove that $\hat{\mathbf{Z}}^\times \simeq \hat{\mathbf{Z}} \times \prod_{n=1}^{\infty} \mathbf{Z}/n\mathbf{Z}$ as profinite groups.

2. Dedekind rings

2.1. Definition, first properties.

Definition 2.1.1. Assume that A is an integral domain. We say that A is a *Dedekind ring* if:

(0) A is not a field;
(1) A is noetherian;
(2) A is integrally closed;
(3) nonzero prime ideals of A are maximal.

Proposition 2.1.2. PID that are not fields are Dedekind rings.

Proof. If A is a PID, it is an integral domain and noetherian by definition. It is integrally closed by proposition 1.9.10. Its nonzero prime ideals are maximal by proposition 1.1.30. □

Theorem 2.1.3. Let A be a Dedekind ring, K its fraction field, L/K a finite separable field extension, and B the integral closure of A in L. Then B is a Dedekind ring.

Proof. The ring A is noetherian: by corollary 1.10.39 (1), the ring B is noetherian. It is integrally closed by proposition 1.9.12. Finally, if $\mathfrak{P} \subset B$ is a nonzero prime ideal, the ideal $\mathfrak{p} = \mathfrak{P} \cap A$ is prime and nonzero (it contains $\mathsf{N}_{L/K}(b) \neq 0$ for all $b \in \mathfrak{P} \backslash \{0\}$), hence maximal. This implies that $\mathfrak{P}$ is maximal (*cf* proposition 1.9.19). □

Corollary 2.1.4. The ring of integers of a number field is a Dedekind ring.

2.2. Local characterization of Dedekind rings.

Proposition 2.2.1. Let A be a Dedekind ring and $S \subset A$ a muliplicative part. Then $S^{-1}A$ is a field or a Dedekind ring.

Proof. The ring $S^{-1}A$ is noetherian by corollary 1.8.13. As A is integrally closed, so is $S^{-1}A$ by proposition 1.9.13. Also, proposition 1.8.14 provides an increasing bijection (for inclusion)

$$\begin{aligned} \{\mathfrak{p} \in \mathsf{Spec}(A)\,;\, \mathfrak{p} \cap S = \varnothing\} &\leftrightarrow \mathsf{Spec}(S^{-1}A) \\ \mathfrak{p} &\mapsto S^{-1}\mathfrak{p} \\ \mathfrak{q} \cap A := \iota^{-1}(\mathfrak{q}) &\leftarrow\!\shortmid \mathfrak{q} \end{aligned}$$

As nonzero elements in $\mathsf{Spec}(A)$ are maximal, so are nonzero elements in $\mathsf{Spec}(S^{-1}A)$. □

Lemma 2.2.2. A local Dedekind ring is a DVR.

Proof. Assume that A is a local Dedekind ring: we have to show that A is a PID (*cf* definition 1.8.25). As A is not a field: its maximal ideal $\mathfrak{m}$ is nonzero, so $\mathsf{Spec}(A) = \{(0), \mathfrak{m}\}$.

• Let $\alpha \in \mathfrak{m} \backslash \{0\}$. We first show that there exists $r \in \mathbf{Z}_{>0}$ such that $\mathfrak{m}^r \subset \alpha A$. As A is noetherian, the ideal $\mathfrak{m}$ is of finite type: there exists $f_1, \ldots, f_n \in A \backslash \{0\}$ such that $\mathfrak{m} = \sum\limits_{i=1}^{n} f_i A$. Let $i \in \{1, \ldots, n\}$. By proposition 1.8.14, we have $\mathsf{Spec}(A_{(f_i)}) = \{\mathfrak{p} \in \mathsf{Spec}(A)\,;\, f_i \notin \mathfrak{p}\} = \{(0)\}$, hence $A_{(f_i)}$ is a field (thus $A_{(f_i)} = \mathsf{Frac}(A)$). The element α is thus invertible in $A_{(f_i)}$: there exists $r_i \in \mathbf{Z}_{\geqslant 0}$ and $a_i \in A$ such that $\frac{1}{\alpha} = \frac{a_i}{f_i^{r_i}}$. We have of course $r_i > 0$ (because $\alpha \notin A^\times$ since $\alpha \in \mathfrak{m}$), and $f_i^{r_i} \in \alpha A$. If $r = r_1 + \cdots + r_n \in \mathbf{Z}_{>0}$, we have indeed

$$\mathfrak{m}^r = (f_1 A + \cdots + f_n A)^r \subset f_1^{r_1} A + \cdots + f_n^{r_n} A \subset \alpha A.$$

• Next we show that $\mathfrak{m}$ is principal. Let $\alpha \in \mathfrak{m} \backslash \{0\}$ and $r \in \mathbf{Z}_{>0}$ *minimal* such that $\mathfrak{m}^r \subset \alpha A$. We have $\mathfrak{m}^{r-1} \not\subset \alpha A$: take $\beta \in \mathfrak{m}^{r-1} \backslash \alpha A$ and let $\pi = \frac{\alpha}{\beta} \in \mathsf{Frac}(A)$. we have

$$\pi^{-1}\mathfrak{m} = \frac{\beta}{\alpha}\mathfrak{m} \subset \alpha^{-1}\mathfrak{m}^r \subset A$$

and $\pi^{-1}\mathfrak{m}$ is an ideal of A. If this ideal was not the unit ideal, we would have $\pi^{-1}\mathfrak{m} \subset \mathfrak{m}$, implying that π^{-1} is integral over A (*cf* proposition 1.9.3 (iii) ⇒ (i)). As A is integrally closed, this would imply $\pi^{-1} \in A$ *i.e.* $\beta \in \alpha A$ which is not: we necessarily have $\pi^{-1}\mathfrak{m} = A$, so that $\mathfrak{m} = \pi A$ is principal.

• Now let $I \subset A$ be any strict nonzero ideal: we have $I \subset \mathfrak{m}$. Let $\alpha \in I \backslash \{0\}$: we have $\alpha \in \mathfrak{m} \backslash \{0\}$. By what precedes, there exists $r \in \mathbf{Z}_{>0}$ such that $\mathfrak{m}^r \subset \alpha A \subset I$. If we had $I \subset \mathfrak{m}^{r+1}$, this would imply $\pi^r \in \pi^{r+1}A$, *i.e.* $1 \in \pi A = \mathfrak{m}$ which is absurd. The set $\{n \in \mathbf{Z}_{\geqslant 0}\,;\, I \subset \mathfrak{m}^n\}$ is thus bounded above. As it is nonempty (it contains 1), it has a greatest element n_I. We have $I \subset \pi^{n_I} A$ *i.e.* $\pi^{-n_I} I \subset A$ is an ideal of A, but $\pi^{-n_I} I \not\subset \mathfrak{m}$ (otherwise $I \subset \mathfrak{m}^{n_I + 1}$), thus $\pi^{-n_I} I = A$, *i.e.* $I = \pi^{n_I} A$. □

Theorem 2.2.3. Let A be a noetherian integral domain which is not a field. Then A is a Dedekind ring if and only if for all maximal ideal $\mathfrak{m} \subset A$, the localization $A_\mathfrak{m}$ is a DVR.

Proof. If A is a Dedekind ring and $\mathfrak{m} \subset A$ a maximal ideal, the localization $A_\mathfrak{m}$ is a local Dedekind ring (by proposition 2.2.1). As A is not a field, $\mathfrak{m}$ is nonzero, and $A_\mathfrak{m}$ is not a field: this implies that $A_\mathfrak{m}$ is a DVR (lemma 2.2.2).
Conversely, assume that for all maximal ideal $\mathfrak{m} \subset A$, the localization $A_\mathfrak{m}$ is a DVR.
Let $x \in K = \mathsf{Frac}(A)$ be integral over A. Write $x = \frac{a}{b}$ with $a, b \in A$ and $b \neq 0$. For every maximal ideal $\mathfrak{m} \subset A$, the element x is *a fortiori* integral over $A_\mathfrak{m}$. As the latter is a Dedekind ring, we have $x \in A_\mathfrak{m}$, *i.e.* $aA_\mathfrak{m} \subset bA_\mathfrak{m}$. By the local-global principle (proposition 1.8.22), this implies $aA \subset bA$, *i.e.* $x \in A$, proving that A is integrally closed.
Let $\mathfrak{p} \subset A$ be a nonzero prime ideal. By Krull's theorem (theorem 1.1.7), there exists a maximal ideal $\mathfrak{m} \subset A$ such that $\mathfrak{p} \subset \mathfrak{m}$. By proposition 1.8.14, the ideal $\mathfrak{p}A_\mathfrak{m}$ is prime in $A_\mathfrak{m}$. Being nonzero by assumption, it is maximal, *i.e.* $\mathfrak{p}A_\mathfrak{m} = \mathfrak{m}A_\mathfrak{m}$, which implies that $\mathfrak{p} = \mathfrak{m}$ (thanks to proposition 1.8.22), and $\mathfrak{p}$ is maximal. □

2.3. **Factorization of ideals, class group.** Theorem 2.2.3 implies that Dedekind rings are locally PIDs, hence locally UFDs. Nevertheless, there are Dedekind rings that are not UFDs.

Example 2.3.1. Let $K = \mathbf{Q}(i\sqrt{5})$: we have $\mathcal{O}_K = \mathbf{Z}[i\sqrt{5}]$. Assume $2 = xy$ with $x, y \in \mathcal{O}_K$: write $x = a + ib\sqrt{5}$ and $y = c + id\sqrt{5}$. We have $\mathsf{N}_{K/\mathbf{Q}}(2) = \mathsf{N}_{K/\mathbf{Q}}(x)\,\mathsf{N}_{K/\mathbf{Q}}(y)$ *i.e.* $4 = (a^2+5b^2)(c^2+5d^2)$, which implies $b = d = 0$ whence $x, y \in \mathbf{Z}$, *i.e.* $x \in \{\pm 1\}$ or $y \in \{\pm 1\}$. The element 2 is thus irreducible in $\mathcal{O}_K$. On the other hand, we have $(1+i\sqrt{5})(1-i\sqrt{5}) = 6 \in 2\mathcal{O}_K$ but $1+i\sqrt{5}, 1-i\sqrt{5} \notin 2\mathcal{O}_K$, *i.e.* 2 is not prime. This implies that $\mathcal{O}_K$ (which is a Dedekind ring) is not a UFD (*cf* proposition 1.1.21).

As we will see, Dedekind rings have nevertheless a unique factorization property, not for nonzero elements into a product of prime elements, but for nonzero ideals into a product of prime ideals.

Lemma 2.3.2. Let A be a noetherian ring and $I \subset A$ a nonzero ideal.
(1) The ideal I contains a product $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ of nonzero prime ideals (non necessarily distinct).
(2) If A is a Dedekind ring, there are only finitely many maximal ideals of A that contain I.

Proof. (1) We use a noetherian induction: let $\mathscr{E}$ be the set of nonzero ideals in A that do not contain a finite product of nonzero prime ideals. Assume $\mathscr{E} \neq \varnothing$: as A is noetherian, it admits an element I which is maximal for the inclusion (*cf* proposition 1.3.1 (1)). We have of course $I \neq A$ (because A contains at least a prime ideal by Krull's theorem, *cf* theorem 1.1.7), and I itself is not prime: there exists $x, y \notin I$ such that $xy \in I$. The ideals $I + xA$ and $I + yA$ strictly contain I: by maximality of I in $\mathscr{E}$, we have $I + xA, I + yA \notin \mathscr{E}$, which implies the existence of $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ nonzero prime ideals such that $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset I + xA$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subset I + yA$. We have then

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m \subset (I + xA)(I + yA) \subset I$$

contradicting $I \in \mathscr{E}$. It follows that $\mathscr{E}$ is empty.
(2) By (1), there exists $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ nonzero prime ideals (hence maximal since A is a Dedekind ring) such that $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset I$. If $\mathfrak{m}$ is a maximal ideal in A such that $I \subset \mathfrak{m}$, we have *a fortiori* $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{m}$. If $\mathfrak{p}_i \neq \mathfrak{m}$ for all $i \in \{1, \ldots, n\}$, there exists $a_i \in \mathfrak{p}_i \backslash \mathfrak{m}$, and $a_1 \cdots a_n \in \mathfrak{p}_1 \cdots \mathfrak{p}_n \backslash \mathfrak{m}$ which is absurd: there exists $i \in \{1, \ldots, n\}$ such that $\mathfrak{p}_i = \mathfrak{m}$. □

Theorem 2.3.3. Let A a Dedekind ring and $I \subset A$ a nonzero ideal. There exist pairwise distinct nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and integers $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}_{>0}$ such that

$$I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n}$$

This decomposition is unique up to the order of factors, and the set of nonzero prime ideals containing I is precisely $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Proof. • Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ be the set of prime ideals containing I (*cf* lemma 2.3.2 (2)). For $i \in \{1, \ldots, n\}$, the ring $A_{\mathfrak{p}_i}$ is a DVR (*cf* theorem 2.2.3). The ideal $IA_{\mathfrak{p}_i} \subset A_{\mathfrak{p}_i}$ is strict: there exists $\alpha_i \in \mathbf{Z}_{>0}$ such that $IA_{\mathfrak{p}_i} = \mathfrak{p}_i^{\alpha_i} A_{\mathfrak{p}_i}$. Put $J = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n}$. By construction, we have $IA_{\mathfrak{p}_i} = JA_{\mathfrak{p}_i}$ for all $i \in \{1, \ldots, n\}$. On the other hand, if $\mathfrak{m} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ is a maximal ideal in A, we have $IA_\mathfrak{m} = A_\mathfrak{m} = JA_\mathfrak{m}$. The local-global principle (*cf* proposition 1.8.22) implies that $I = J$.
• It remains to prove unicity up to the order. Assume that $I = \mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_m^{\beta_m}$ where $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ are pairwise distinct nonzero prime ideals and $\beta_1, \ldots, \beta_m \in \mathbf{Z}_{>0}$. For $i \in \{1, \ldots, n\}$, we have $\mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_m^{\beta_m} \subset \mathfrak{p}_i$: there exists $j \in \{1, \ldots, m\}$ such that $\mathfrak{p}_i = \mathfrak{q}_j$. This implies that $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$. Exchanging the factorizations, we have the reverse inclusion, *i.e.* $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$, hence $m = n$, and after

runumbering, $\mathfrak{p}_i = \mathfrak{q}_i$ for all $i \in \{1, \ldots, n\}$. Also, we have $\mathfrak{p}_i^{\beta_i} A_{\mathfrak{p}_i} = IA_{\mathfrak{p}_i} = \mathfrak{p}_i^{\alpha_i} A_{\mathfrak{p}_i}$, which implies $\alpha_i = \beta_i$ for all $i \in \{1, \ldots, n\}$. □

Remark 2.3.4. A way to formulate unicity is to say that the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ that appear in the factorization are exactly the nonzero prime ideals that contain I (indeed its prime divisors), and that for all $i \in \{1, \ldots, n\}$, the multiplicity α_i is the valuation of the ideal $IA_{\mathfrak{p}_i}$ in the DVR $A_{\mathfrak{p}_i}$.

Example 2.3.5. With the notations of example 2.3.1, we have the isomorphism

$$\begin{aligned} \mathbf{Z}[X]/\langle X^2 + 5\rangle &\xrightarrow{\sim} \mathscr{O}_K \\ X &\mapsto i\sqrt{5} \end{aligned}$$

It induces an isomorphism $\mathbf{F}_2[X]/\langle (1+X)^2\rangle \xrightarrow{\sim} \mathscr{O}_K/2\mathscr{O}_K$: let $\mathfrak{p}$ be the ideal generated by 2 and $\theta := 1 + i\sqrt{5}$ (it is the image of the maximal ideal $\langle 1 + X\rangle$ of $\mathbf{F}_2[X]/\langle (1+X)^2\rangle$ by the preceding isomorphism). The induced isomorphism is an isomorphism $\mathscr{O}_K/\mathfrak{p} \xrightarrow{\sim} \mathbf{F}_2$, so that $\mathfrak{p}$ is maximal. On the other hand, the image of $\mathfrak{p}^2$ in $\mathscr{O}_K/2\mathscr{O}_K$ is zero: we have $\mathfrak{p}^2 \subset 2\mathscr{O}_K \subset \mathfrak{p}$. As $2\mathscr{O}_K$ is not prime, we have $2\mathscr{O}_K \neq \mathfrak{p}$, showing that $2\mathscr{O}_K = \mathfrak{p}^2$.

Definition 2.3.6. Let A an integral domain and K its fraction field.
(1) A *fractional ideal* is a sub-A-module $I \subset K$ such that there exists $d \in A\backslash\{0\}$ with $I \subset d^{-1}A$.
(2) Operations on fractional ideals. Let $I, J \subset K$ be fractional ideals: there exists $d, \delta \in A\backslash\{0\}$ such that $I \subset d^{-1}A$ and $J \subset \delta^{-1}A$. Let $I + J$ (resp. IJ) be the sub-A-module of K generated by $I \cup J$ (resp. elements of the form[24] xy with $x \in I$ and $y \in J$). Then $IJ \subset (d\delta)^{-1}A$ and $I \cap J \subset I + J \subset (d\delta)^{-1}A$ so that IJ, $I \cap J$ and $I + J$ are fractional ideals.
(3) If $I \subset K$ is a fractional ideal, we put

$$I^{-1} = \{x \in K\,;\, xI \subset A\}$$

it is a sub-A-module of K. If $I \neq \{0\}$, then I^{-1} is a fractional ideal (if $a \in I\backslash\{0\}$, we have $aI^{-1} \subset A$, so that $I^{-1} \subset a^{-1}A$).
(4) A nonzero fractional ideal $I \subset K$ is called *invertible* if the inclusion $II^{-1} \subset A$ is an equality.

Remark 2.3.7. (1) A fractional ideal is nothing but a set of the form $d^{-1}\mathfrak{a}$ where $\mathfrak{a} \subset A$ is an ideal and $d \in A\backslash\{0\}$. In particular, every ideal in A is a fractional ideal. Also, for all $x \in K^\times$, the set xA is a fractional ideal. Such a fractional ideal is called *principal*. A principal fractional ideal is invertible, and $(xA)^{-1} = x^{-1}A$.
(2) If $I \subset J \subset K$ are fractional ideals, we have $J^{-1} \subset I^{-1}$. In particular, if $I \subset A$, we have $A \subset I^{-1}$.
(3) If $I, J \subset K$ are invertible fractional ideals, so is the product IJ, and $(IJ)^{-1} = I^{-1}J^{-1}$.
(4) If $S \subset A$ is a multiplicative part and $I \subset K$ a invertible fractional ideal over A, then $S^{-1}I$ is an invertible fractional ideal over $S^{-1}A$, and $(S^{-1}I)^{-1} = S^{-1}I^{-1}$ (indeed we have $(S^{-1}I^{-1})(S^{-1}I) = S^{-1}II^{-1} = S^{-1}A$).

Corollary 2.3.8. In a Dedekind ring, every nonzero fractional ideal is invertible.

Proof. Let A a Dedekind ring, K its fraction field and $I \subset K$ a nonzero fractional ideal. Assume first that $I \subset A$ is an ideal. Let $x \in I\backslash\{0\} \subset A\backslash\{0\}$. By theorem 2.3.3, there exists nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}_{>0}$ such that $xA = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n}$. As $xA \subset I$, we have necessarily $I = \mathfrak{p}_1^{\beta_1} \cdots \mathfrak{p}_n^{\beta_n}$ with $0 \leqslant \beta_i \leqslant \alpha_i$ for all $i \in \{1, \ldots, n\}$. Put $J = \mathfrak{p}_1^{\alpha_1 - \beta_1} \cdots \mathfrak{p}_n^{\alpha_n - \beta_n} \subset A$: we have $IJ = xA$, thus $I(x^{-1}J) = A$, proving that I is invertible and $I^{-1} = x^{-1}J$. In the general case, we have $I = d^{-1}\mathfrak{a}$ with $d \in A\backslash\{0\}$ and $\mathfrak{a} \subset A$. By what precedes, the ideal $\mathfrak{a}$ is invertible: we have $\mathfrak{a}\mathfrak{a}^{-1} = A$, hence $I(d\mathfrak{a}^{-1}) = A$, so that I is invertible, with inverse $d\mathfrak{a}^{-1}$. □

Theorem 2.3.9. Let A be a Dedekind ring, $\mathscr{P}_A$ the set of its nonzero prime ideals and K its fraction field. If $I \subset K$ is a nonzero fractional ideal, there exists a unique family $\big(v_{\mathfrak{p}}(I)\big)_{\mathfrak{p} \in \mathscr{P}_A} \in \mathbf{Z}^{(\mathscr{P}_A)}$ such that

$$I = \prod_{\mathfrak{p} \in \mathscr{P}_A} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$$

(the product is finite since only finitely many $v_{\mathfrak{p}}(I)$ are nonzero).

Proof. There exists a nonzero ideal $\mathfrak{a} \subset A$ and $d \in A\backslash\{0\}$ such that $I = d^{-1}\mathfrak{a}$. By theorem 2.3.3 applied to the ideals $\mathfrak{a}, dA \subset A$, the existence of the decomposition follows. For unicity, assume that

$$\prod_{\mathfrak{p} \in \mathscr{P}_A} \mathfrak{p}^{n_{\mathfrak{p}}} = \prod_{\mathfrak{p} \in \mathscr{P}_A} \mathfrak{p}^{m_{\mathfrak{p}}}$$

[24] We have thus $IJ = \Big\{x \in K,\ (\exists n \in \mathbf{Z}_{\geqslant 0})\ (\exists x_1, \ldots, x_n \in I)\ (\exists y_1, \ldots, y_n \in J)\ x = \sum\limits_{k=1}^{n} x_k y_k\Big\}$.

with $(n_\mathfrak{p})_{\mathfrak{p}\in\mathscr{P}_A}, (m_\mathfrak{p})_{\mathfrak{p}\in\mathscr{P}_A} \in \mathbf{Z}^{(\mathscr{P}_A)}$. We have $\prod\limits_{\mathfrak{p}\in\mathscr{P}_A} \mathfrak{p}^{n_\mathfrak{p}-m_\mathfrak{p}} = A$, *i.e.*

$$\prod_{\substack{\mathfrak{p}\in\mathscr{P}_A\\ n_\mathfrak{p}-m_\mathfrak{p}\geqslant 0}} \mathfrak{p}^{n_\mathfrak{p}-m_\mathfrak{p}} = \prod_{\substack{\mathfrak{p}\in\mathscr{P}_A\\ n_\mathfrak{p}-m_\mathfrak{p}<0}} \mathfrak{p}^{-n_\mathfrak{p}+m_\mathfrak{p}} \subset A.$$

By unicity in theorem 2.3.3, this implies that $n_\mathfrak{p} - m_\mathfrak{p} = 0$ *i.e.* $n_\mathfrak{p} = m_\mathfrak{p}$ for all $\mathfrak{p} \in \mathscr{P}_A$ (note that the sets $\{\mathfrak{p} \in \mathscr{P}_A,\ n_\mathfrak{p} - m_\mathfrak{p} \geqslant 0\}$ and $\{\mathfrak{p} \in \mathscr{P}_A,\ n_\mathfrak{p} - m_\mathfrak{p} < 0\}$ are disjoint). □

Notation. If A is an integral domain, we denote by $\mathsf{Fr}(A)$ the set of its nonzero fractional ideals, and $\mathsf{Princ}(A)$ the subset of its nonzero principal fractional ideals.

Proposition 2.3.10. Let A be a Dedekind ring and $\mathscr{P}_A$ the set of its nonzero prime ideals.
(1) Endowed with the law $(I, J) \mapsto IJ$, the set $\mathsf{Fr}(A)$ is an abelian group with unit element A and with inverse map $I \mapsto I^{-1}$. Moreover, the map

$$\begin{aligned} f_A\colon \mathbf{Z}^{(\mathscr{P}_A)} &\to \mathsf{Fr}(A)\\ (n_\mathfrak{p})_{\mathfrak{p}\in\mathscr{P}_A} &\mapsto \prod_{\mathfrak{p}\in\mathscr{P}_A} \mathfrak{p}^{n_\mathfrak{p}} \end{aligned}$$

is a group isomorphism, with inverse $I \mapsto \big(v_\mathfrak{p}(I)\big)_{\mathfrak{p}\in\mathscr{P}_A}$. In particular, we have

$$\begin{aligned} v_\mathfrak{p}(IJ) &= v_\mathfrak{p}(I) + v_\mathfrak{p}(J)\\ v_\mathfrak{p}(I^{-1}) &= -v_\mathfrak{p}(I) \end{aligned}$$

for all $I, J \in \mathsf{Fr}(A)$ and $\mathfrak{p} \in \mathscr{P}_A$.
(2) If $I, J \in \mathsf{Fr}(A)$, we have $I \subset J \Leftrightarrow (\forall \mathfrak{p} \in \mathscr{P}_A)\ v_\mathfrak{p}(I) \geqslant v_\mathfrak{p}(J)$. In particular I is an ideal in A if and only if $v_\mathfrak{p}(I) \geqslant 0$ for all $\mathfrak{p} \in \mathscr{P}_A$.

Proof. (1) By definition 2.3.6, if $I, J \in \mathsf{Fr}(A)$, then $IJ \in \mathsf{Fr}(A)$ and $I^{-1} \in \mathsf{Fr}(A)$. The law $(I, J) \mapsto IJ$ is associative, commutative and admits A as unit element. Moreover, every element is invertible by corollary 2.3.8: $\mathsf{Fr}(A)$ is an abelian group. The map f_A is a group homomorphism, with inverse $I \mapsto \big(v_\mathfrak{p}(I)\big)_{\mathfrak{p}\in\mathscr{P}_A}$ (theorem 2.3.9): it is thus an isomorphism.
(2) by theorem 2.3.3, if $I \subset A$ is an ideal, we have $v_\mathfrak{p}(I) \geqslant 0$ for all $\mathfrak{p} \in \mathscr{P}_A$. The converse is obvious. If $I, J \in \mathsf{Fr}(A)$, we have thus $I \subset J \Leftrightarrow IJ^{-1} \subset A \Leftrightarrow (\forall \mathfrak{p} \in \mathscr{P}_A)\ v_\mathfrak{p}(I) - v_\mathfrak{p}(J) = v_\mathfrak{p}(IJ^{-1}) \geqslant 0$. □

Definition 2.3.11. Let A be a Dedekind ring. The set $\mathsf{Princ}(A)$ is a subgroup of $\mathsf{Fr}(A)$. We denote

$$\mathsf{Cl}(A) = \mathsf{Fr}(A)/\mathsf{Princ}(A)$$

the quotient group, that we call the *ideal class group* of A.

Example 2.3.12. Let A be a Dedekind ring.
(1) A is a PID if and only if $\mathsf{Cl}(A) = \{1\}$.
(2) Let I be a nonzero fractional ideal. The class of I in $\mathsf{Cl}(A)$ is of finite order if and only if there exists $n \in \mathbf{Z}_{>0}$ such that I^n is principal.

Definition 2.3.13. A ring is *semi-local* if it has only finitely many maximal ideals.

Remark 2.3.14. (1) A local ring is semi-local.
(2) If A is a Dedekind ring and $I \subset A$ a nonzero ideal, then A/I is semi-local: let $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$ be the decomposition of I into a product of nonzero prime ideals; the Chinese remainder theorem implies that $A/I \simeq \bigoplus_{i=1}^r A/\mathfrak{p}_i^{\alpha_i}$, and each factor $A/\mathfrak{p}_i^{\alpha_i}$ is local, with maximal ideal $\mathfrak{p}_i/\mathfrak{p}_i^{\alpha_i}$.

Proposition 2.3.15. Let A be a Dedekind ring, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subset A$ nonzero prime ideals and $I \subset A$ an ideal. There exists $a \in A$ such that $(\forall i \in \{1, \ldots, n\})\ IA_{\mathfrak{p}_i} = aA_{\mathfrak{p}_i}$. In particular, a semi-local Dedekind ring is a PID.

Proof. We have $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n} J$ with $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}_{\geqslant 0}$ and J prime to $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ (theorem 2.3.3). By lemma 2.2.2, for all $i \in \{1, \ldots, n\}$, the ring $A_{\mathfrak{p}_i}$ is a DVR: let $\pi_i \in \mathfrak{p}_i$ be such that $\mathfrak{p}_i A_{\mathfrak{p}_i} = \pi_i A_{\mathfrak{p}_i}$. We have $IA_{\mathfrak{p}_i} = \pi_i^{\alpha_i} A_{\mathfrak{p}_i}$ for all $i \in \{1, \ldots, n\}$. As $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are pairwise coprime, so are $\mathfrak{p}_1^{\alpha_1+1}, \ldots, \mathfrak{p}_n^{\alpha_n+1}$: by the chinese remainder theorem (*cf* theorem 1.1.14), the natural morphism

$$A/\mathfrak{p}_1^{\alpha_1+1} \cdots \mathfrak{p}_n^{\alpha_n+1} \to (A/\mathfrak{p}_1^{\alpha_1+1}) \times \cdots \times (A/\mathfrak{p}_n^{\alpha_n+1})$$

is an isomorphism: there exists $a \in A$ such that $a \equiv \pi_i^{\alpha_i} \mod \mathfrak{p}_i^{\alpha_i+1}$ hence $aA_{\mathfrak{p}_i} = IA_{\mathfrak{p}_i}$ for all $i \in \{1, \ldots, n\}$. If A is semi-local, take $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ the set of maximal ideals of A. By the local-global principle (proposition 1.8.22), we have $I = aA$. As A is an integral domain by definition, it is a PID. □

Corollary 2.3.16. Let A be a Dedekind ring, $I \subset A$ a nonzero ideal and $a \in I \backslash \{0\}$. There exists $b \in A$ such that $I = aA + bA$.

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subset A$ be the nonzero prime ideals containing a (lemme 2.3.2 (2)). By proposition 2.3.15, there exists $b \in A$ such that $(\forall i \in \{1, \ldots, n\})\, IA_{\mathfrak{p}_i} = bA_{\mathfrak{p}_i}$. Put $J = aA + bA \subset A$. If $\mathfrak{p}$ is a maximal ideal that does not contain a, we have $aA_{\mathfrak{p}} = A_{\mathfrak{p}}$: as $a \in I$ and $a \in J$, this implies that $IA_{\mathfrak{p}} = JA_{\mathfrak{p}} = A_{\mathfrak{p}}$. If $i \in \{1, \ldots, n\}$, we have $aA_{\mathfrak{p}_i} \subset IA_{\mathfrak{p}_i}$, hence $IA_{\mathfrak{p}_i} = bA_{\mathfrak{p}_i} \subset JA_{\mathfrak{p}_i} \subset IA_{\mathfrak{p}_i}$, so that $JA_{\mathfrak{p}_i} = IA_{\mathfrak{p}_i}$. By the local-global principle (proposition 1.8.22), we have $I = J$. □

2.4. **Factorization in an extension, ramification.** Let A be a Dedekind ring and $K = \mathsf{Frac}(A)$. The aim of this section is to explain the decomposition of the ideal generated by an ideal of A in the integral closure of A in a finite separable extension of K. If $\mathfrak{p}$ is a nonzero prime ideal in A, we denote $\kappa(\mathfrak{p}) = A/\mathfrak{p}$ the residue field of A at $\mathfrak{p}$.

Definition 2.4.1. Let A be a Dedekind ring, and L/K a finite separable field extension. Let B be the integral closure of A in L. By corollary 1.10.39 (1) and theorem 2.1.3, B is a finite A-algebra and a Dedekind ring.
(1) If $\mathfrak{p} \subset A$ and $\mathfrak{P} \subset B$ are nonzero prime ideals, we say that $\mathfrak{P}$ *divides* $\mathfrak{p}$, or that $\mathfrak{P}$ *lies above* $\mathfrak{p}$ (and we denote $\mathfrak{P} \mid \mathfrak{p}$) if $\mathfrak{P} \cap A = \mathfrak{p}$.
(2) As B is a Dedekind ring, we have

$$\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$$

with $e_{\mathfrak{P}} = v_{\mathfrak{P}}(\mathfrak{p}B) \in \mathbf{Z}_{>0}$. The integer $e_{\mathfrak{P}}$ is called the *ramification index* of $\mathfrak{p}$ en $\mathfrak{P}$.
(3) If $\mathfrak{P} \mid \mathfrak{p}$, the field $\kappa(\mathfrak{P}) = B/\mathfrak{P}$ is a finite extension of $\kappa(\mathfrak{p}) = A/\mathfrak{p}$ called the *residual extension* at $\mathfrak{P}$. We put $f_{\mathfrak{P}} = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})]$: this integer is called the residual degree of $\mathfrak{p}$ at $\mathfrak{P}$.
(4) If $e_{\mathfrak{P}} = 1$ and the field extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is separable, we say that $\mathfrak{p}$ (or even L/K) is *unramified* at $\mathfrak{P}$, and *ramified* at $\mathfrak{P}$ otherwise. If $\mathfrak{p}$ is unramified at every prime ideal dividing it, we say that $\mathfrak{p}$ is *unramified*, or that L/K is unramified at $\mathfrak{p}$.
(5) When there is only one prime ideal $\mathfrak{P}$ above $\mathfrak{p}$ and $f_{\mathfrak{P}} = 1$, we say that L/K is *totally ramified* at $\mathfrak{p}$.
(6) If the ideal $\mathfrak{p}B$ is prime in B, we say that $\mathfrak{p}$ is *inert* in L/K. If $e_{\mathfrak{P}} = f_{\mathfrak{P}} = 1$ for all $\mathfrak{P} \mid \mathfrak{p}$, we say that $\mathfrak{p}$ is *totally split* in L/K.

Theorem 2.4.2. Under the hypothesis of definition 2.4.1, we have

$$\dim_{\kappa(\mathfrak{p})}(B/\mathfrak{p}B) = [L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}$$

Proof. There are isomorphisms $A/\mathfrak{p} \xrightarrow{\sim} A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ and $B/\mathfrak{p}B \xrightarrow{\sim} S^{-1}B/\mathfrak{p}S^{-1}B$ (with $S = A \backslash \mathfrak{p}$): replacing A by $A_{\mathfrak{p}}$ (which is licit by proposition 1.9.13), we may assume that A is a DVR, with maximal ideal $\mathfrak{p}$ (*cf* lemma 2.2.2). The ring A is a PID: the A-module B is free of rank $[L : K]$ (*cf* corollary 1.10.39 (2)). This implies that $\dim_{\kappa(\mathfrak{p})}(B/\mathfrak{p}B) = [L : K]$.
For $\mathfrak{P} \mid \mathfrak{p}$, the ideals $\mathfrak{P}^{e_{\mathfrak{P}}}$ are pairwise coprime: the Chinese remainder theorem provides an isomorphism

$$B/\mathfrak{p}B = B/\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}} \xrightarrow{\sim} \bigoplus_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}$$

Consider the filtration $\mathfrak{P}^{e_{\mathfrak{P}}} \subsetneq \mathfrak{P}^{e_{\mathfrak{P}}-1} \subsetneq \cdots \subsetneq \mathfrak{P}^2 \subsetneq \mathfrak{P} \subsetneq B$. As $B_{\mathfrak{P}}$ is a DVR (lemma 2.2.2), we have isomorphisms $B_{\mathfrak{P}}/\mathfrak{P}B_{\mathfrak{P}} \xrightarrow{\sim} \mathfrak{P}^k B_{\mathfrak{P}}/\mathfrak{P}^{k+1}B_{\mathfrak{P}} \xleftarrow{\sim} \mathfrak{P}^k/\mathfrak{P}^{k+1}$ (the first isomorphism is induced by the multiplication by $\pi_{\mathfrak{P}}^k$, where $\pi_{\mathfrak{P}}$ is a uniformizer of $B_{\mathfrak{P}}$). This implies that $\mathfrak{P}^k/\mathfrak{P}^{k+1}$ is a $\kappa(\mathfrak{P})$-vector space of dimension 1, hence a $\kappa(\mathfrak{p})$-vector space of dimension $f_{\mathfrak{P}}$. This shows that

$$\dim_{\kappa(\mathfrak{p})}(B/\mathfrak{P}^{e_{\mathfrak{P}}}) = \sum_{k=0}^{e_{\mathfrak{P}}-1} \dim_{\kappa(\mathfrak{p})}(\mathfrak{P}^k/\mathfrak{P}^{k+1}) = e_{\mathfrak{P}} f_{\mathfrak{P}}$$

hence $\dim_{\kappa(\mathfrak{p})}(B/\mathfrak{p}B) = \sum\limits_{\mathfrak{P}|\mathfrak{p}} \dim_{\kappa(\mathfrak{p})}(B/\mathfrak{P}^{e_{\mathfrak{P}}}) = \sum\limits_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}$. □

Lemma 2.4.3. (PRIME AVOIDANCE). Let R be a ring, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subset R$ prime ideals and $I \subset \bigcup\limits_{i=1}^{n} \mathfrak{p}_i$ an ideal. There exists $i \in \{1, \ldots, n\}$ such that $I \subset \mathfrak{p}_i$.

Proof. Removing some $\mathfrak{p}_i$ if necessary, we may assume that $(\forall i \in \{1, \ldots, n\})\, \mathfrak{p}_i \not\subset \bigcup\limits_{j \neq i} \mathfrak{p}_j$: let $a_i \in \mathfrak{p}_i \backslash \bigcup\limits_{j \neq i} \mathfrak{p}_j$. Assume moreover that for all $i \in \{1, \ldots, n\}$, we have $I \not\subset \mathfrak{p}_i$: let $x_i \in I \backslash \mathfrak{p}_i$. Put $x = \sum\limits_{i=1}^{n} x_i \prod\limits_{j \neq i} a_j \in I$. If

$i \in \{1, \ldots, n\}$, we have $a_i \in \mathfrak{p}_i$ hence $x \equiv x_i \prod\limits_{j \neq i} a_j \mod \mathfrak{p}_i$. As $x_i \notin \mathfrak{p}_i$ and $a_j \notin \mathfrak{p}_i$ for $j \neq i$, we have $x_i \prod\limits_{j \neq i} a_j \notin \mathfrak{p}_i$ whence $x \notin \mathfrak{p}_i$, so that $x \in I \backslash \bigcup\limits_{i=1}^{n} \mathfrak{p}_i$, contradicting the hypothesis. □

Remark 2.4.4. The terminology comes from the contrapositive.

Theorem 2.4.5. Under the hypothesis of theorem 2.4.2, assume moreover that the field extension L/K is Galois. The group $\mathsf{Gal}(L/K)$ acts transitively on the set of prime ideals that divide $\mathfrak{p}$. The integers $e_{\mathfrak{P}}$ and $f_{\mathfrak{P}}$ only depend of $\mathfrak{p}$ and not of $\mathfrak{P}$: we denote them $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ respectively. If $\mathsf{Gal}(L/K)_{\mathfrak{P}}$ denotes the stabilizer of $\mathfrak{P}$, then $\mathsf{Gal}(L/K)_{\sigma(\mathfrak{P})} = \sigma \, \mathsf{Gal}(L/K)_{\mathfrak{P}} \sigma^{-1}$ for all $\sigma \in \mathsf{Gal}(L/K)$: the integer $g_{\mathfrak{p}} = \big[\mathsf{Gal}(L/K) : \mathsf{Gal}(L/K)_{\mathfrak{P}}\big]$ only depends of $\mathfrak{p}$ and not of $\mathfrak{P}$. We have $[L : K] = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$.

Proof. Let $\mathfrak{P}$ and $\mathfrak{P}'$ be prime ideals above $\mathfrak{p}$ such that $\mathfrak{P}' \neq \sigma(\mathfrak{P})$ for all $\sigma \in \mathsf{Gal}(L/K)$. As the ideals $\mathfrak{P}'$ and $\sigma(\mathfrak{P})$ are maximal, we have $\mathfrak{P}' \not\subset \sigma(\mathfrak{P})$ for all $\sigma \in \mathsf{Gal}(L/K)$: there exists $x \in \mathfrak{P}'$ such that $x \notin \sigma(\mathfrak{P})$ for all $\sigma \in \mathsf{Gal}(L/K)$ (*cf* lemma 2.4.3). This implies that $y = \mathsf{N}_{L/K}(x) = \prod\limits_{\sigma \in \mathsf{Gal}(L/K)} \sigma(x) \notin \mathfrak{P}$, contradicting the fact that $y \in A \cap \mathfrak{P}' = \mathfrak{p} \subset \mathfrak{P}$. The action of $\mathsf{Gal}(L/K)$ on the set of prime ideals that divide $\mathfrak{p}$ is thus transitive, and the integers $e_{\mathfrak{P}}$ and $f_{\mathfrak{P}}$ thus only depend of $\mathfrak{p}$ and not of $\mathfrak{P}$. We also have $\mathsf{Gal}(L/K)_{\sigma(\mathfrak{P})} = \sigma \, \mathsf{Gal}(L/K)_{\mathfrak{P}} \sigma^{-1}$ for all $\sigma \in \mathsf{Gal}(L/K)$. Moreover, we have $\#\{\mathfrak{P} \in \mathsf{Spec}(B) \, ; \mathfrak{P} \mid \mathfrak{p}\} = \big[\mathsf{Gal}(L/K) : \mathsf{Gal}(L/K)_{\mathfrak{P}}\big] = g_{\mathfrak{p}}$: this shows that

$$[L : K] = \sum_{\mathfrak{P} | \mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}} = \#\{\mathfrak{P} \in \mathsf{Spec}(B) \, ; \mathfrak{P} \mid \mathfrak{p}\} e_{\mathfrak{p}} f_{\mathfrak{p}} = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$$

thanks to proposition 2.4.2. □

Proposition 2.4.6. Under the hypothesis of theorem 2.4.2, assume that $B = A[\theta]$. Let $F \in A[X]$ be the minimal polynomial of θ over K. For a nonzero prime ideal $\mathfrak{p} \subset A$, the factorization of the reduction $\overline{F}$ of F in $\kappa(\mathfrak{p})[X]$ has the form $\overline{F}(X) = \prod\limits_{i=1}^{s} f_i(X)^{r_i}$ with $f_1, \ldots, f_s$ irreducible and pairwise coprime. The decomposition of $\mathfrak{p}B$ is then

$$\mathfrak{p}B = \prod_{i=1}^{s} \mathfrak{P}_i^{r_i}$$

with $\mathfrak{P}_i = \mathfrak{p}B + F_i(\theta)B$ (where $F_i \in A[X]$ is any lifting of f_i). Moreover, we have $B/\mathfrak{P}_i \simeq \kappa(\mathfrak{p})[X]/\langle f_i(X)\rangle$.

Proof. By hypothesis, there is an isomorphism

$$\begin{aligned} A[X]/\langle F(X)\rangle &\xrightarrow{\sim} B \\ X &\mapsto \theta \end{aligned}$$

It induces isomorphisms $\kappa(\mathfrak{p})[X]/\langle \overline{F}(X)\rangle \xrightarrow{\sim} B/\mathfrak{p}B$ thus $\kappa(\mathfrak{p})[X]/\langle f_i(X)\rangle \xrightarrow{\sim} B/\mathfrak{P}_i$ for all $i \in \{1, \ldots, s\}$. This shows that $\mathfrak{P}_i$ is maximal in B, divides $\mathfrak{p}$, and that $f_{\mathfrak{P}_i} = [\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{p})] = \deg(f_i)$.

On the other hand, if $i \neq j$, we have $\kappa(\mathfrak{p})[X] = f_i(X)\kappa(\mathfrak{p})[X] + f_j(X)\kappa(\mathfrak{p})[X]$ (because f_i and f_j are coprime), hence $A[X] = F_i(X)A[X] + F_j(X)A[X] + \mathfrak{p}[X]$, which implies that $\mathfrak{P}_i + \mathfrak{P}_j = B$: the ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ are pairwise coprime.

Conversely, let $\mathfrak{P} \subset B$ be a maximal maximal ideal such that $\mathfrak{P} \mid \mathfrak{p}$. As $F(X) \equiv \prod\limits_{i=1}^{s} F_i(X) \mod \mathfrak{p}[X]$, we have $\prod\limits_{i=1}^{s} F_i(\theta) \in \mathfrak{P}$: there exists $i \in \{1, \ldots, s\}$ such that $F_i(\theta) \in \mathfrak{P}$, hence $\mathfrak{P}_i \subset \mathfrak{P}$, *i.e.* $\mathfrak{P}_i = \mathfrak{P}$ by maximality of $\mathfrak{P}_i$. The set of prime ideals of B that divide $\mathfrak{p}$ is thus precisely $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_s\}$.

It remains to show that for all $i \in \{1, \ldots, s\}$, the ramification index $e_{\mathfrak{P}_i}$ is r_i. By the Chinese remainder theorem, there is an isomorphism

$$B/\mathfrak{p}B \simeq \kappa(\mathfrak{p})[X]/\langle \overline{F}(X)\rangle \xrightarrow{\sim} \prod_{i=1}^{s} \kappa(\mathfrak{p})[X]/\langle f_i(X)^{r_i}\rangle$$

For $j \neq i$, we have $F_j(\theta) \notin \mathfrak{P}_i$ by what precedes: the localization of the factor $\kappa(\mathfrak{p})[X]/\langle f_j(X)^{r_j}\rangle$ at $\mathfrak{P}_i$ is zero. This shows that

$$B_{\mathfrak{P}_i}/\mathfrak{p}B_{\mathfrak{P}_i} \simeq \kappa(\mathfrak{p})[X]/\langle f_i(X)^{r_i}\rangle$$

hence $e_{\mathfrak{P}_i} f_{\mathfrak{P}_i} = \dim_{\mathfrak{p}}(B_{\mathfrak{P}_i}/\mathfrak{p}B_{\mathfrak{P}_i}) = \dim_{\mathfrak{p}}(\kappa(\mathfrak{p})[X]/\langle f_i(X)^{r_i}\rangle) = r_i \deg(f_i) = r_i f_{\mathfrak{P}_i}$, *i.e.* $e_{\mathfrak{P}_i} = r_i$. □

2.4.7. *Relative norm.* If $I \subset K$ is a nonzero nonzero fractional ideal, then IB is a nonzero fractional ideal: this provides a group homomorphism $\mathsf{Fr}(A) \to \mathsf{Fr}(B)$. If $I = xA$ is principal, so $IB = xB$: this homomorphism induces a group homomorphism

$$i_{B/A} \colon \mathsf{Cl}(A) \to \mathsf{Cl}(B)$$

We want to built an homomorphism in the reverse direction. Recall that we denote by $\mathscr{P}_A$ (resp. $\mathscr{P}_B$) the set of nonzero prime ideals of A (resp. B). If $\mathfrak{P} \in \mathscr{P}_B$, we have $\mathfrak{p} := \mathfrak{P} \cap A \in \mathscr{P}_A$, and we have $f_{\mathfrak{P}} := [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})]$. We put

$$\mathsf{N}_{B/A}(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}}}$$

As valuations induce group isomorphisms $\mathsf{Fr}(A) \xrightarrow{\sim} \mathbf{Z}^{(\mathscr{P}_A)}$ and $\mathsf{Fr}(B) \xrightarrow{\sim} \mathbf{Z}^{(\mathscr{P}_B)}$ (proposition 2.3.10), this defines a unique group homomorphism

$$\mathsf{N}_{B/A} \colon \mathsf{Fr}(B) \to \mathsf{Fr}(A)$$

Proposition 2.4.8. (1) (Transitivity) Let M/L be a finite separable field extension and C the integral closure of A in M (or of B, this is the same). We have $\mathsf{N}_{B/A}(\mathsf{N}_{C/B}(J)) = \mathsf{N}_{C/A}(J)$ for all nonzero fractional ideal $J \subset M$.
(2) If $I \subset K$ is a nonzero fractional ideal, we have $\mathsf{N}_{B/A}(i_{B/A}(I)) = I^n$ (where $n = [L/K]$).
(3) If $x \in L^\times$, we have $\mathsf{N}_{B/A}(xB) = \mathsf{N}_{L/K}(x)A$.

Proof. (1) We may assume that J is a nonzero prime ideal. Put $\mathfrak{P} = B \cap J$ and $\mathfrak{p} = A \cap J = A \cap \mathfrak{P}$. We have extensions $\kappa(J)/\kappa(\mathfrak{P})$ and $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$, so that $[\kappa(J) : \kappa(\mathfrak{P})][\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = [\kappa(J) : \kappa(\mathfrak{p})]$. As $\mathsf{N}_{C/B}(J) = \mathfrak{P}^{[\kappa(J):\kappa(\mathfrak{P})]}$ and $\mathsf{N}_{B/A}(\mathfrak{P}) = \mathfrak{p}^{[k(\mathfrak{P}):\kappa(\mathfrak{p})]}$, we get

$$\begin{aligned}\mathsf{N}_{B/A}(\mathsf{N}_{C/B}(J)) &= \mathsf{N}_{B/A}(\mathfrak{P}^{[\kappa(J):\kappa(\mathfrak{P})]}) = \mathsf{N}_{B/A}(\mathfrak{P})^{[\kappa(J):\kappa(\mathfrak{P})]}\\ &= \mathfrak{p}^{[\kappa(\mathfrak{P}):\kappa(\mathfrak{p})][\kappa(J):\kappa(\mathfrak{P})]} = \mathfrak{p}^{[\kappa(J):\kappa(\mathfrak{p})]} = \mathsf{N}_{C/A}(J)\end{aligned}$$

(2) We may assume that $I = \mathfrak{p}$ is a nonzero prime ideal: we have $i_{B/A}(I) = \mathfrak{p}B = \prod\limits_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$ hence

$$\mathsf{N}_{B/A}(i_{B/A}(I)) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathsf{N}_{B/A}(\mathfrak{P})^{e_{\mathfrak{P}}} = \mathfrak{p}^{\sum\limits_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}} = I^n$$

by theorem 2.4.2.
(3) • Assume that L/K is Galois with group Γ. We first show that $i_{B/A}(\mathsf{N}_{B/A}(J)) = \mathsf{N}_{B/A}(J)B = \prod\limits_{\gamma\in\Gamma} \gamma(J)$ for all nonzero fractional ideal $J \subset L$. As above, we may assume that $J = \mathfrak{P}$ is a nonzero prime ideal. Put $\mathfrak{p} = A \cap \mathfrak{P}$: by theorem 2.4.5, the group Γ acts transitively on the set of prime ideals of B above $\mathfrak{p}$, and the integers $e_{\mathfrak{P}}$ and $f_{\mathfrak{P}}$ only depend of $\mathfrak{p}$ and not of $\mathfrak{P}$ (they are denoted $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ respectively). Let $\Gamma_{\mathfrak{P}}$ be the stabilizer of $\mathfrak{P}$: we have $\#\Gamma = [L : K] = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$ with $g_{\mathfrak{p}} = \big[\Gamma : \Gamma_{\mathfrak{P}}\big]$, so $\#\Gamma_{\mathfrak{P}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$. Moreover, we have $\mathfrak{p}B = \prod\limits_{\gamma\in\Gamma/\Gamma_{\mathfrak{P}}} \gamma(\mathfrak{P})^{e_{\mathfrak{p}}}$, which implies

$$\mathsf{N}_{B/A}(J)B = \mathfrak{p}^{f_{\mathfrak{p}}} B = \prod_{\gamma\in\Gamma/\Gamma_{\mathfrak{P}}} \gamma(\mathfrak{P})^{e_{\mathfrak{p}} f_{\mathfrak{p}}} = \prod_{\gamma\in\Gamma/\Gamma_{\mathfrak{P}}} \gamma(\mathfrak{P})^{\#\Gamma_{\mathfrak{P}}} = \prod_{\gamma\in\Gamma} \gamma(\mathfrak{P})$$

as wanted. Applied to $J = xB$ with $x \in L^\times$, this formula gives $\mathsf{N}_{B/A}(xB)B = \prod\limits_{\gamma\in\Gamma} \gamma(x)B = \mathsf{N}_{L/K}(x)B$. This shows that the valuations of the fractional ideals $\mathsf{N}_{B/A}(xB)$ and $\mathsf{N}_{L/K}(x)A$ are the same at every nonzero prime ideal of A: they are equal.
• In the general case, let M be a normal closure of L/K and C the integral closure of A in M. The field extensions M/L and M/K are Galois: by what we have seen above, if $x \in L$ we have

$$\mathsf{N}_{M/K}(x)A = \mathsf{N}_{C/A}(xC) = \mathsf{N}_{B/A}(\mathsf{N}_{C/B}(xC)) = \mathsf{N}_{B/A}(\mathsf{N}_{M/L}(x)B) = \mathsf{N}_{B/A}(x^d B) = \mathsf{N}_{B/A}(xB)^d$$

(where $d = [M : L]$). On the other hand, we have $\mathsf{N}_{M/K}(x) = \mathsf{N}_{L/K}(\mathsf{N}_{M/L}(x)) = \mathsf{N}_{L/K}(x^d) = \mathsf{N}_{L/K}(x)^d$ by proposition 1.10.9: we have $\mathsf{N}_{L/K}(x)^d A = \mathsf{N}_{B/A}(xB)^d$, which implies $\mathsf{N}_{L/K}(x)A = \mathsf{N}_{B/A}(xB)$ (looking at $\mathfrak{p}$-adic valuations). □

Corollary 2.4.9. The group homomorphism $\mathsf{N}_{B/A} \colon \mathsf{Fr}(B) \to \mathsf{Fr}(A)$ induces a group homomorphism

$$\mathsf{N}_{B/A} \colon \mathsf{Cl}(B) \to \mathsf{Cl}(A)$$

Proof. Follows from proposition 2.4.8 (3), which implies that $\mathsf{N}_{B/A}(\mathsf{Princ}(B)) \subset \mathsf{Princ}(A)$. □

Remark 2.4.10. (1) By proposition 2.4.8 (2), the morphism $i_{B/A}\colon \mathsf{Fr}(A)\to\mathsf{Fr}(B)$ is injective. The induced morphism $i_{B/A}\colon \mathsf{Cl}(A)\to\mathsf{Cl}(B)$ is not injective in general (non principal ideals may "become" principal in an extension). Similarly, the map $\mathsf{N}_{B/A}$ is not injective in general.
(2) If $S\subset A$ is a multiplicative part and $J\subset L$ a nonzero fractional ideal, we have

$$\mathsf{N}_{S^{-1}B/S^{-1}A}(S^{-1}J)=S^{-1}\,\mathsf{N}_{B/A}(J).$$

2.5. **Different and discriminant.** Let A be a Dedekind ring, K its fraction field, L/K a finite separable extension, and B the integral closure of A in L. By corollary 1.10.39 (1) and theorem 2.1.3, B is a finite A-algebra and a Dedekind ring. Let

$$B^*=\{y\in L\,;\,(\forall x\in B)\ \mathsf{Tr}_{L/K}(xy)\in A\}$$

By definition, it is a sub-B-module of L.

Lemma 2.5.1. B^* is a fractional ideal of L that contains B.

Proof. Put $n=[L:K]$. Let $(e_1,\ldots,e_n)$ be a basis of L made of elements in B, and $(x_1,\ldots,x_n)$ in L the dual basis. Let $x\in B^*$: we can write $x=\sum\limits_{j=1}^{n}\lambda_jx_j$ with $\lambda_1,\ldots,\lambda_n\in K$. For $i\in\{1,\ldots,n\}$, we have $\lambda_i=\mathsf{Tr}_{L/K}(e_ix)\in A$. This implies that $B^*\subset Ax_1\oplus\cdots\oplus Ax_n\subset d^{-1}B$ for any element $d\in B\backslash\{0\}$ such that $dx_i\in B$ for all $i\in\{1,\ldots,n\}$ (we can in fact take d in $A\backslash\{0\}$). This shows that B^* is a fractional ideal of L. We have obviously $B\subset B^*$ because $\mathsf{Tr}_{L/K}(B)\subset A$ by corollary 1.10.7. □

Remark 2.5.2. Of course, the proof is very close to that of proposition 1.10.37.

Definition 2.5.3. The *different* of B/A is the inverse of the fractional ideal B^* (the latter is called the *inverse different*). It is an ideal of B denoted $\mathfrak{D}_{B/A}$.

Remark 2.5.4. When there is no ambiguity on A, the different is often simply denoted $\mathfrak{D}_{L/K}$. Similarly, the discriminant is often denoted $\mathfrak{d}_{L/K}$.

Proposition 2.5.5. Let $\mathfrak{a}$ (resp. $\mathfrak{b}$) be a fractional ideal in K (resp. L). The following are equivalent:
(i) $\mathsf{Tr}_{L/K}(\mathfrak{b})\subset\mathfrak{a}$;
(ii) $\mathfrak{b}\subset\mathfrak{a}\mathfrak{D}_{B/A}^{-1}$.

Proof. This is obvious if $\mathfrak{a}=\{0\}$: assume $\mathfrak{a}\neq\{0\}$. Then we have the equivalences

$$\mathsf{Tr}_{L/K}(\mathfrak{b})\subset\mathfrak{a}\Leftrightarrow\mathfrak{a}^{-1}\,\mathsf{Tr}_{L/K}(\mathfrak{b})\subset A\Leftrightarrow\mathsf{Tr}_{L/K}(\mathfrak{a}^{-1}\mathfrak{b})\subset A\Leftrightarrow\mathfrak{a}^{-1}\mathfrak{b}\subset\mathfrak{D}_{B/A}^{-1}\Leftrightarrow\mathfrak{b}\subset\mathfrak{a}\mathfrak{D}_{B/A}^{-1}.$$

□

Remark 2.5.6. The previous proposition is a characterization of the different.

Proposition 2.5.7. Let A be a Dedekind ring, $K=\mathsf{Frac}(A)$ and L/K a finite separable field extension of degree n. Denote B the integral closure of A in L. Fix $x\in B$ such that $L=K(x)$, put $C=A[x]\subset B$ and let $P\in A[X]$ the minimal polynomial of x over K.
(1) We have $\mathsf{Tr}_{L/K}\big(\frac{x^k}{P'(x)}\big)=\begin{cases}0 & \text{if } 0\leqslant k\leqslant n-2\\ 1 & \text{if } k=n-1\end{cases}$.
(2) The A-module C^* is free with basis $\big(\frac{x^k}{P'(x)}\big)_{0\leqslant k<n}$.
(3) For all $c\in C$, we have $cB\subset C\Leftrightarrow c\in P'(x)\mathfrak{D}_{B/A}^{-1}$ (so that $\mathfrak{D}_{B/A}$ divides $P'(x)B$).
(4) We have $B=C\Leftrightarrow\mathfrak{D}_{B/A}=P'(x)B$, in which case $\Omega^1_{B/A}\simeq B/\mathfrak{D}_{B/A}$.

Proof. (1) • Let $\overline{K}$ be an algebraic closure of K, and $x_1,\ldots,x_n\in\overline{K}$ are the conjugates of x over K: as $L=K(x)$, we have $[L:K]=n$. As L/K is separable, the polynomial P is separable: we have $P(T)=\prod\limits_{i=1}^{n}(T-x_i)$ where the roots $x_1,\ldots,x_n$ are pairwise distinct. We have thus $\frac{1}{P(T)}=\sum\limits_{i=1}^{n}\frac{\lambda_i}{T-x_i}$, so that $1=\sum\limits_{i=1}^{n}\lambda_i\frac{P(T)}{T-x_i}$. Evaluation at x_i gives $1=\lambda_iP'(x_i)$ whence $\frac{1}{P(T)}=\sum\limits_{i=1}^{n}\frac{1}{P'(x_i)(T-x_i)}$.
• For all $i\in\{1,\ldots,n\}$, we have $\frac{1}{T-x_i}=\frac{1}{T}\big(1-\frac{x_i}{T}\big)^{-1}=\sum\limits_{k=0}^{\infty}\frac{x_i^k}{T^{k+1}}\in\overline{K}[[\frac{1}{T}]]$. What precedes implies that $\frac{1}{P(T)}=\sum\limits_{k=0}^{\infty}\frac{1}{T^{k+1}}\sum\limits_{i=1}^{n}\frac{x_i^k}{P'(x_i)}=\sum\limits_{k=0}^{\infty}\mathsf{Tr}_{L/K}\big(\frac{x^k}{P'(x)}\big)\frac{1}{T^{k+1}}$. On the other hand, $P(T)=T^n+a_1T^{n-1}+\cdots+a_n$, so that $P(T)=T^n\big(1+\frac{a_1}{T}+\cdots+\frac{1}{T^n}\big)$, which implies that $\frac{1}{P(T)}\in\frac{1}{T^n}+\frac{1}{T^{n+1}}\overline{K}[[\frac{1}{T}]]$. Identifying coefficients gives the required formulas.

(2) It is enough to show that $M := \big(\mathsf{Tr}_{L/K}\big(x^i\frac{x^j}{P'(x)}\big)\big)_{0\leqslant i,j<n} \in \mathsf{GL}_n(A)$. By (1), we have $\mathsf{Tr}_{L/K}\big(x^i\frac{x^j}{P'(x)}\big) = 0$ if $i+j<n-1$ and $\mathsf{Tr}_{L/K}\big(x^i\frac{x^j}{P'(x)}\big) = 1$ if $i+j=n-1$. Moreover, if $n\leqslant i+j<2n-1$, then we have $\mathsf{Tr}_{L/K}\big(x^i\frac{x^j}{P'(x)}\big) = \mathsf{Tr}_{L/K}\big(x^n\frac{x^{i+j-n}}{P'(x)}\big) \in A$ since x^n is an A-linear combination of $1, x, \ldots, x^n-1$. This shows that

$$M = \left(\begin{smallmatrix} & & 1\\ & \cdot^{\cdot^{\cdot}} & *\\ 1 & * & * \end{smallmatrix}\right) \in \mathsf{M}_n(A)$$

so that $\det(M) = (-1)^{n(n-1)/2}$.

(3) Note that (2) means that $C^* = \frac{1}{P(x)}C$ (since $C = A[x] = \bigoplus\limits_{k=0}^{n-1} Ax^k$). If $c\in C$, we have thus

$$cB\subset C \Leftrightarrow P'(x)^{-1}cB\subset C^* \Leftrightarrow \mathsf{Tr}_{L/K}(P'(x)^{-1}cB)\subset A \Leftrightarrow P'(x)^{-1}c\in\mathfrak{D}_{B/A}^{-1} \Leftrightarrow c\in P'(x)\mathfrak{D}_{B/A}^{-1}$$

(because $P'(x)^{-1}cB$ is a sub-C-module of L). The set of such c is a sub-B-module of B *i.e.* an ideal in B by its very definition, so is $P'(x)\mathfrak{D}_{B/A}^{-1}$: we have $P'(x)B\subset\mathfrak{D}_{B/A}$, *i.e.* $\mathfrak{D}_{B/A}$ divides $P'(x)B$.

(4) • We have $C\subset B$, so that $B = C \Leftrightarrow 1\in\{c\in C\,;\, cB\subset C\}$. By (3), this is equivalent to $1\in P'(x)\mathfrak{D}_{B/A}^{-1}$, *i.e.* $B\subset P'(x)\mathfrak{D}_{B/A}^{-1}$ that is $\mathfrak{D}_{B/A}\subset P'(x)B$. As the reverse inclusion always holds, this is equivalent to the equality $\mathfrak{D}_{B/A} = P'(x)B$.

• If $B = C$, we have $A[X]/\langle P\rangle \xrightarrow{\sim} A[x] = B$, which implies that $\Omega^1_{B/A}$ is the B-module generated by $\mathrm{d}x$, and that the annihilator of $\mathrm{d}x$ is $P'(x)B$: we have $\Omega^1_{B/A}\simeq B/\langle P'(x)\rangle \simeq B/\mathfrak{D}_{B/A}$. □

Proposition 2.5.8. Let $S\subset A$ be a multiplicative part. Then $\mathfrak{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{D}_{B/A}$.

Proof. Recall that the integral closure commutes with localization: the integral closure of $S^{-1}A$ in L is $S^{-1}B$ (*cf* proposition 1.9.13). As $S^{-1}\mathfrak{D}_{B/A}^{-1} = (S^{-1}\mathfrak{D}_{B/A})^{-1}$ (*cf* remark 2.3.7 (4)), it is enough to show that $\mathfrak{D}^{-1}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{D}^{-1}_{B/A}$.

If $x\in B$, $y\in\mathfrak{D}^{-1}_{B/A}$ and $s,t\in S$, we have $\mathsf{Tr}_{L/K}(s^{-1}xt^{-1}y) = (st)^{-1}\,\mathsf{Tr}_{L/K}(xy)\in S^{-1}A$: as this holds for all $x\in B$ and $s\in S$, this shows that $t^{-1}y\in\mathfrak{D}^{-1}_{S^{-1}B/S^{-1}A}$, showing that $S^{-1}\mathfrak{D}^{-1}_{B/A}\subset\mathfrak{D}^{-1}_{S^{-1}B/S^{-1}A}$.

Conversely, let $\{b_1,\ldots,b_r\}$ be a generating family of B as an A-module, and let $\beta\in\mathfrak{D}^{-1}_{S^{-1}B/S^{-1}A}$: for all $i\in\{1,\ldots,r\}$, we have $\mathsf{Tr}_{L/K}(b_i\beta)\in S^{-1}A$. Taking a common denominator, there exists $s\in S$ such that $s\,\mathsf{Tr}_{L/K}(b_i\beta)\in A$ for all $i\in\{1,\ldots,r\}$, which implies that $s\beta\in\mathfrak{D}_{B/A}$, hence $\beta\in S^{-1}\mathfrak{D}_{B/A}$. □

Proposition 2.5.9. Assume[25] that B is free over A. Then $\mathfrak{d}_{B/A} = \mathsf{N}_{B/A}(\mathfrak{D}_{B/A})$.

Proof. As integral closure, discriminant, different and relative norm commute with localization (*cf* propositions 1.9.13, 1.10.17, 2.5.8 and remark 2.4.10 (2)), this can be checked after localizing at nonzero prime ideals of A. We thus may assume that A is a DVR, with maximal ideal $\mathfrak{p}$.

• Let $(e_1,\ldots,e_n)$ be a basis of B over A, and denote by $\mathfrak{B} = (e_1^*,\ldots,e_n^*)$ the dual basis for the trace map. Then we have $B^* := \mathfrak{D}^{-1}_{B/A} = Ae_1^*\oplus\cdots\oplus Ae_n^*$. For all $i\in\{1,\ldots,n\}$, we have $e_i = \sum\limits_{j=1}^n x_{i,j}e_j^*$ where $M = (x_{i,j})_{1\leqslant i,j\leqslant n}\in\mathsf{M}_n(A)$. Then $e_ie_j = \sum\limits_{k=1}^n x_{i,k}e_k^*e_j$ so that $\mathsf{Tr}_{L/K}(e_ie_j) = x_{i,j}$ for all $i,j\in\{1,\ldots,n\}$. This implies that $\mathfrak{d}_{B/A}$ is the ideal generated by $\det(M)$. On the other hand, M is the matrix, in the basis $\mathfrak{B}$ of an A-linear endomorphism u of B^*, whose image is B. By theorem 1.4.7, there exist $P,Q\in\mathsf{SL}_n(A)$ such that $M = P^{-1}\,\mathsf{diag}(a_1,\ldots,a_n)Q$ where $a_1,\ldots,a_n\in A$ are such that $a_1A\supset\cdots\supset a_nA$. Changing the basis $\mathfrak{B}$, we may assume that $P = \mathrm{I}_n$: this implies that $\mathsf{Coker}(u)\simeq\bigoplus\limits_{i=1}^n A/a_iA$. Writing $a_iA = \mathfrak{p}^{\ell_i}$, we have $\mathfrak{d}_{B/A} = \det(M)A = a_1\cdots a_nA = \mathfrak{p}^\ell$, where $\ell = \sum\limits_{i=1}^n \ell_i$ is the length of $\mathsf{Coker}(u)\simeq B^*/B$.

On the other hand, write $\mathfrak{D}_{B/A} = \prod\limits_{\mathfrak{P}|\mathfrak{p}}\mathfrak{P}^{\alpha_\mathfrak{P}}$: we have $\mathsf{N}_{B/A}(\mathfrak{D}_{B/A}) = \mathfrak{p}^\delta$ with $\delta = \sum\limits_{\mathfrak{P}|\mathfrak{p}} f_\mathfrak{P}\alpha_\mathfrak{P}$. Moreover, we have $B^*/B = \mathfrak{D}^{-1}_{B/A}/B\simeq B/\mathfrak{D}_{B/A}\simeq\bigoplus\limits_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{\alpha_\mathfrak{P}}$: as the length of $B/\mathfrak{P}^{\alpha_\mathfrak{P}}$ as an A-module is $f_\mathfrak{P}\alpha_\mathfrak{P}$ (*cf* proof of theorem 2.4.2), that of B^*/B is $\ell = \delta$, proving the equality. □

Proposition 2.5.10. (Transitivity of the different). Let M/L be a finite separable field extensions, and C the integral closure of B in M. Then $\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B}\mathfrak{D}_{B/A}$.

[25] As observed earlier, this condition is not really necessary.

Proof. Let $\mathfrak{c} \subset M$ be a nonzero fractional ideal. We have

$$\begin{aligned}\mathfrak{c} \subset \mathfrak{D}_{C/B}^{-1} \Leftrightarrow \mathsf{Tr}_{M/L}(\mathfrak{c}) \subset B \Leftrightarrow \mathfrak{D}_{B/A}^{-1} \mathsf{Tr}_{M/L}(\mathfrak{c}) \subset \mathfrak{D}_{B/A}^{-1} \Leftrightarrow \mathsf{Tr}_{L/K}(\mathfrak{D}_{B/A}^{-1} \mathsf{Tr}_{M/L}(\mathfrak{c})) \subset A \\ \Leftrightarrow \mathsf{Tr}_{L/K}(\mathsf{Tr}_{M/L}(\mathfrak{D}_{B/A}^{-1}\mathfrak{c})) \subset A \Leftrightarrow \mathsf{Tr}_{M/K}(\mathfrak{D}_{B/A}^{-1}\mathfrak{c}) \subset A \Leftrightarrow \mathfrak{D}_{B/A}^{-1}\mathfrak{c} \subset \mathfrak{D}_{C/A}^{-1} \Leftrightarrow \mathfrak{c} \subset \mathfrak{D}_{B/A}\mathfrak{D}_{C/A}^{-1}\end{aligned}$$

(here we used the transitvity of the trace, *cf* proposition 1.10.9) which shows that $\mathfrak{D}_{C/B}^{-1} = \mathfrak{D}_{B/A}\mathfrak{D}_{C/A}^{-1}$, *i.e.* $\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B}\mathfrak{D}_{B/A}$. □

This allows to recover 1.10.24 in a special case.

Corollary 2.5.11. Under the assumtions of proposition 2.5.10, assume that C is free over B and B is free over A. Then $\mathfrak{d}_{C/A} = \mathsf{N}_{B/A}(\mathfrak{d}_{C/B})\mathfrak{d}_{B/A}^{[M:L]}$.

Proof. We apply $\mathsf{N}_{C/A}$ to the equality $\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B}\mathfrak{D}_{B/A}$ (*cf* proposition 2.5.10). By proposition 2.5.9, this shows that $\mathfrak{d}_{C/A} = \mathsf{N}_{C/A}(\mathfrak{D}_{C/B})\,\mathsf{N}_{C/A}(\mathfrak{D}_{B/A})$. The equality the follows from $\mathsf{N}_{C/A} = \mathsf{N}_{B/A} \circ \mathsf{N}_{C/B}$, which implies $\mathsf{N}_{C/A}(\mathfrak{D}_{C/B}) = \mathsf{N}_{B/A}(\mathfrak{d}_{C/B})$ and $\mathsf{N}_{C/A}(\mathfrak{D}_{B/A}) = \mathsf{N}_{B/A}(\mathfrak{D}_{B/A}^{[M:L]}) = \mathfrak{d}_{B/A}^{[M:L]}$. □

2.6. **Rings of integers of number fields.** In what follows, $\overline{\mathbf{Q}}$ denotes the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$. Recall that a number field is a finite extension of $\mathbf{Q}$, and that if K is a number field, we denote by $\mathcal{O}_K$ the ring of integers of K, *i.e.* the integral closure of $\mathbf{Z}$ in K.

Proposition 2.6.1. Let K be a number field and $n = [K : \mathbf{Q}]$. The ring of integers $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank n.

Proof. Follows from the fact that $\mathbf{Z}$ is PID and from corollary 1.10.39 (2). □

Example 2.6.2. (1) Let $d \in \mathbf{Z}\backslash\{0,1\}$ be a square free integer, and $K = \mathbf{Q}(\sqrt{d})$. Then

$$\mathcal{O}_K = \begin{cases}\mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \mod 4\,\mathbf{Z} \\ \mathbf{Z}[\sqrt{d}] & \text{otherwise}\end{cases}$$

(2) If p is an odd prime integer, $\zeta \in \mathbf{C}$ a primitive p-th root of unity and $K = \mathbf{Q}(\zeta)$, then $\mathcal{O}_K = \mathbf{Z}[\zeta]$.

Proposition 2.6.3. Let $(x_1, \dots, x_n)$ be a basis of $\mathcal{O}_K$ over $\mathbf{Z}$ and $M = (m_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(\mathbf{Z})$ such that $\det(M) \neq 0$. For $i \in \{1, \dots, n\}$, put $y_i = \sum\limits_{j=1}^{n} m_{i,j}x_j$. If $R = \sum\limits_{i=1}^{n} \mathbf{Z}\,y_i \subset \mathcal{O}_K$, then $[\mathcal{O}_K : R] = \#(\mathcal{O}_K/R)$ is finite and $\mathrm{D}(y_1, \dots, y_n) = [\mathcal{O}_K : R]^2\,\mathrm{D}(x_1, \dots, x_n)$.

Proof. The hypothesis $\det(M) \neq 0$ implies that R is a free $\mathbf{Z}$-module of rank n. It is a sub-module of $\mathcal{O}_K$ which is also of rank n (proposition 2.6.1), it is of finite index (this follows from the adapted basis theorem, *cf* 1.4.11), *i.e.* $[\mathcal{O}_K : R] = \#(\mathcal{O}_K/R) < +\infty$. We have $\mathrm{D}(y_1, \dots, y_n) = \det(M)^2\,\mathrm{D}(x_1, \dots, x_n)$: it is enough to show that $|\det(M)| = [\mathcal{O}_K : R]$, which follows from theorem 1.4.7. □

Definition 2.6.4. Let $(x_1, \dots, x_n)$ and $(y_1, \dots, y_n)$ be $\mathbf{Z}$-bases of $\mathcal{O}_K$. Let $M = (m_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{GL}_n(\mathbf{Z})$ be the change of basis matrix, *i.e.* such that $y_i = \sum\limits_{j=1}^{n} m_{i,j}x_j$ for all $i \in \{1, \dots, n\}$. Proposition 2.6.3 implies that

$$\mathrm{D}(y_1, \dots, y_n) = \det(M)^2\,\mathrm{D}(x_1, \dots, x_n) = \mathrm{D}(x_1, \dots, x_n)$$

(because $\det(M) \in \{\pm 1\} = \mathbf{Z}^\times$). The integer

$$d_K = \mathrm{D}(x_1, \dots, x_n)$$

does not depend on the choice of the basis $(x_1, \dots, x_n)$. It is called the ***absolute discriminant*** of K.

Corollary 2.6.5. If $(x_1, \dots, x_n)$ is a basis de K over $\mathbf{Q}$, made of elements in $\mathcal{O}_K$, and $R = \bigoplus\limits_{i=1}^{n} \mathbf{Z}\,x_i \subset \mathcal{O}_K$, then

$$\mathrm{D}(x_1, \dots, x_n) = [\mathcal{O}_K : R]^2 d_K.$$

Corollary 2.6.6. A prime p ramifies in K if and only if $p \mid d_K$.

Proof. This is a special case of theorem 3.5.24. □

Example 2.6.7. (1) Let $d \in \mathbf{Z}\backslash\{0,1\}$ be squarefree and $K = \mathbf{Q}(\sqrt{d})$. If $d \equiv 1 \mod 4\mathbf{Z}$, then $\mathcal{O}_K = \mathbf{Z}[\alpha]$ with $\alpha = \frac{1+\sqrt{d}}{2}$: the family $(1,\alpha)$ is a basis of $\mathcal{O}_K$ over $\mathbf{Z}$ (*cf* example 2.6.2 (1)). The minimal polynomial of α over $\mathbf{Q}$ is $P(X) = X^2 - X - \frac{d-1}{4}$: we have thus $d_K = \mathrm{D}(1,\alpha) = \mathsf{disc}(P) = d$ (can be checked by direct computation). If $d \not\equiv 1 \mod 4\mathbf{Z}$, we have $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$: the family $(1,\sqrt{d})$ is a basis of $\mathcal{O}_K$ over $\mathbf{Z}$. The minimal polynomial of $\sqrt{d}$ over $\mathbf{Q}$ is $P(X) = X^2 - d$: we have thus $d_K = \mathrm{D}(1,\sqrt{d}) = \mathsf{disc}(P) = 4d$. At the end, we have

$$d_K = \begin{cases} d & \text{if } d \equiv 1 \mod 4\mathbf{Z} \\ 4d & \text{if } d \not\equiv 1 \mod 4\mathbf{Z} \end{cases}$$

(2) If p is an odd prime integer, $\zeta \in \mathbf{C}$ a primitive p-th root of unity and $K = \mathbf{Q}(\zeta)$, we have $\mathcal{O}_K = \mathbf{Z}[\zeta]$ (*cf* example 2.6.2 (2)) and thus $d_K = (-1)^{\frac{p-1}{2}} p^{p-2}$. By corollary 2.6.6, p is the unique prime which is ramified in K.

Proposition 2.6.8. Let K be a number field and $n = [K : \mathbf{Q}]$.
(1) A family $x_1, \ldots, x_n \in \mathcal{O}_K$ is a basis of $\mathcal{O}_K$ over $\mathbf{Z}$ if and only if $\mathrm{D}(x_1, \ldots, x_n) = d_K$.
(2) If $x_1, \ldots, x_n \in \mathcal{O}_K$ is such that $\mathrm{D}(x_1, \ldots, x_n) \neq 0$ is squarefree, then $(x_1, \ldots, x_n)$ is a $\mathbf{Z}$-basis of $\mathcal{O}_K$.

Proof. Follows from proposition 1.10.19 and corollary 1.10.20. □

It is usually difficult to compute the ring of integers of a number field K. Using the primitive element theorem, we can start from an element α such that $K = \mathbf{Q}(\alpha)$. After multiplying α by an appropriate integer (as small as possible), we may assume that $\alpha \in \mathcal{O}_K$, so that $\mathbf{Z}[\alpha] \subset \mathcal{O}_K$. In general, the inclusion is strict, but $\mathbf{Z}[\alpha]$ is of finite index in $\mathcal{O}_K$. More precisely, by proposition 1.10.38, we have $\mathbf{Z}[\alpha] \subset \mathcal{O}_K \subset \frac{1}{d}\mathbf{Z}[\alpha]$ with $d = \mathrm{D}(1, \alpha, \ldots, \alpha^{n-1})$ (where $n = [K : \mathbf{Q}]$), which is easily computed using the minimal polynomial of α over $\mathbf{Q}$ and proposition 1.10.31. This reduces a lot the number of possibilities for $\mathcal{O}_K$. From this, on can search conditions on coordinates in the basis $(1, \alpha, \ldots, \alpha^{n-1})$ for an element $x \in K$ to belong to $\mathcal{O}_K$. To find such conditions, one uses the trace and the norme. For instance, if $x \in K$ is integral over $\mathbf{Z}$, so is $\alpha^i x$, hence $\mathsf{Tr}_{K/\mathbf{Q}}(\alpha^i x) \in \mathbf{Z}$ for all $i \in \{0, \ldots, n-1\}$.

Remark 2.6.9. Unlike number fields, rings of integers of number fields are not monogen in general: if K is a number field, in general, there is no $\alpha \in K$ such that $\mathcal{O}_K = \mathbf{Z}[\alpha]$.

Example 2.6.10. Let p be an odd prime integer, $\zeta \in \mathbf{C}$ a primitive p-th root of unity and $K = \mathbf{Q}(\zeta)$. We have of course $\mathbf{Z}[\zeta] \subset \mathcal{O}_K$. The minimal polynomial of ζ over $\mathbf{Q}$ is

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 = \frac{X^p - 1}{X - 1}$$

We have $(X-1)\Phi_p'(X) + \Phi_p(X) = pX^{p-1}$, thus $\Phi_p'(\zeta) = \frac{p\zeta^{p-1}}{\zeta - 1}$: by exemple 1.10.8 (2), we have thus $\mathsf{N}_{K/\mathbf{Q}}(\Phi_p'(\zeta)) = \frac{\mathsf{N}_{K/\mathbf{Q}}(p)\,\mathsf{N}_{K/\mathbf{Q}}(\zeta)^{p-1}}{\mathsf{N}_{K/\mathbf{Q}}(\zeta-1)} = \frac{p^{p-1}}{p} = p^{p-2}$ (we have $\mathsf{N}_{K/\mathbf{Q}}(\zeta) = 1$ and $\mathsf{N}_{K/\mathbf{Q}}(\zeta - 1) = p$), which implies that

$$\mathrm{D}(1, \zeta, \zeta^2, \cdots, \zeta^{p-2}) = \mathsf{disc}(\Phi_p) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2} = (-1)^{\frac{p-1}{2}} p^{p-2}$$

(proposition 1.10.31). We thus have

$$\mathbf{Z}[\zeta] \subset \mathcal{O}_K \subset \tfrac{1}{p^{p-2}}\mathbf{Z}[\zeta].$$

Let's prove that $\mathcal{O}_K = \mathbf{Z}[\zeta]$.
First observe $(1-\zeta)\mathcal{O}_K \cap \mathbf{Z} = p\mathbf{Z}$. Indeed we have $p \in (1-\zeta)\mathcal{O}_K$ because $1 - \zeta \mid \mathsf{N}_{K/\mathbf{Q}}(\zeta - 1) = p$. If the inclusion $p\mathbf{Z} \subset (1-\zeta)\mathcal{O}_K \cap \mathbf{Z}$ was strict, we would have $(1-\zeta)\mathcal{O}_K \cap \mathbf{Z} = \mathbf{Z}$, thus $1 \in (1-\zeta)\mathcal{O}_K$: there would exist $z \in \mathcal{O}_K$ such that $1 = (1-\zeta)z$, whence $1 = p\,\mathsf{N}_{K/\mathbf{Q}}(z)$ in $\mathbf{Z}$, which is absurd.
If $x = x_0 + x_1\zeta + \cdots + x_{p-2}\zeta^{p-2} \in \mathcal{O}_K$ (with $x_0, \ldots, x_{p-2} \in \mathbf{Q}$), we have

$$(1-\zeta)x = x_0(1-\zeta) + x_1(\zeta - \zeta^2) + \cdots + x_{p-2}(\zeta^{p-2} - \zeta^{p-1})$$

As $\mathsf{Tr}_{K/\mathbf{Q}}(1-\zeta) = p$ and $\mathsf{Tr}_{K/\mathbf{Q}}(\zeta^k - \zeta^{k+1}) = 0$ for $1 \leqslant k < p-1$, we have

$$\mathsf{Tr}_{K/\mathbf{Q}}((1-\zeta)x) = px_0$$

As conjugates of $(1-\zeta)x$ are of the form $(1-\zeta^k)y$ with $k \in \mathbf{Z}$ and $y \in \mathcal{O}_K$, hence dividible by $1-\zeta$, we have $\mathsf{Tr}_{K/\mathbf{Q}}((1-\zeta)x) \in (1-\zeta)\mathcal{O}_K \cap \mathbf{Z} = p\mathbf{Z}$. This implies that $x_0 \in \mathbf{Z}$.
If we have $x_0, \ldots, x_{k-1} \in \mathbf{Z}$ with $k < p-2$, then

$$\zeta^{-k}\big(x - (x_0 + x_1\zeta + \cdots + x_{k-1}\zeta^{k-1})\big) = x_k + x_{k+1}\zeta + \cdots + x_{p-2}\zeta^{p-2-k} \in \mathcal{O}_K$$

which implies that $x_k \in \mathbf{Z}$ from what precedes. At the end, we have $x_0, \ldots, x_{p-2} \in \mathbf{Z}$ and $x \in \mathbf{Z}[\zeta]$.

Proposition 2.6.11. (Stickelberger). Let K be a number field. We have $d_K \equiv 0 \mod 4\mathbf{Z}$ or $d_K \equiv 1 \mod 4\mathbf{Z}$.

Proof. Write $\mathsf{Hom}_{\mathbf{Q}\text{-alg}}(K, \overline{\mathbf{Q}}) = \{\sigma_1, \dots, \sigma_n\}$: if $\{\alpha_1, \dots, \alpha_n\}$ is a basis of $\mathcal{O}_K$ over $\mathbf{Z}$, we have $d_K = \det(M)^2$ with $M = (\sigma_i(\alpha_j))_{1 \leqslant i,j \leqslant n}$ (proposition 1.10.22). We have $\det(M) = S - A$ where $S = \sum\limits_{\substack{\tau \in \mathfrak{S}_n \\ \varepsilon(\tau)=1}} \prod\limits_{i=1}^{n} \sigma_i(\alpha_{\tau(i)})$ and $A = \sum\limits_{\substack{\tau \in \mathfrak{S}_n \\ \varepsilon(\tau)=-1}} \prod\limits_{i=1}^{n} \sigma_i(\alpha_{\tau(i)})$. We thus have $d_K = (S+A)^2 - 4SA$: we have to see that $S + A, SA \in \mathbf{Z}$. As S and A are polynomials in $\sigma_i(\alpha_j) \in \mathcal{O}_K$, we have $S, A \in \mathcal{O}_K$: it is enough to show that $S + A, SA \in \mathbf{Q}$. Let $L \subset \overline{\mathbf{Q}}$ be the Galois closure of K. If $g \in \mathsf{Gal}(L/\mathbf{Q})$, the map

$$\begin{aligned} \mathsf{Hom}_{\mathbf{Q}\text{-alg}}(K, \overline{\mathbf{Q}}) &\to \mathsf{Hom}_{\mathbf{Q}\text{-alg}}(K, \overline{\mathbf{Q}}) \\ \sigma &\mapsto g \circ \sigma \end{aligned}$$

is a permutation. If the latter is even, we have $g(S) = S$ and $g(A) = A$, if it is odd, we have $g(S) = A$ and $g(A) = S$: in all cases we have $g(S + A) = S + A$ and $g(SA) = SA$, hence $S + A, SA \in L^{\mathsf{Gal}(L/\mathbf{Q})} = \mathbf{Q}$. □

Corollary 2.6.12. (Refinement of proposition 2.6.8 (2)). If K is a number field of degree n and $\{x_1, \dots, x_n\}$ a family whose discriminant is $4a$ with $a \equiv 2, 3 \mod 4\mathbf{Z}$ and squarefree, then $(x_1, \dots, x_n)$ is a basis of $\mathcal{O}_K$ over $\mathbf{Z}$.

Proof. Let $\mathfrak{B}$ be a basis of $\mathcal{O}_K$ over $\mathbf{Z}$ and $M \in \mathsf{M}_n(\mathbf{Z})$ the matrix whose columns are the coordinates of $(x_1, \dots, x_n)$ in the basis $\mathfrak{B}$. By proposition 1.10.13, we have $4a = \mathrm{D}(x_1, \dots, x_n) = \det(M)^2 d_K$. If $(x_1, \dots, x_n)$ was not a basis, we would have $\det(M) > 1$ thus $\det(M) = 2$ since a is squarefree. This would imply $d_K = a \equiv 2, 3 \mod 4\mathbf{Z}$, contradicting proposition 2.6.11. □

2.7. Exercises.

Exercise 2.7.1. Let L/K be an extension of number fields. Denote by n its degree and fix $\mathfrak{p} \subset \mathcal{O}_K$ a maximal ideal: we know that $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a $k(\mathfrak{p})$-vector space of dimension n (where $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ is the residue field of $\mathfrak{p}$). A family of elements in $\mathcal{O}_L$ is called *independent modulo* $\mathfrak{p}$ if its image in $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is linearly independent over $k(\mathfrak{p})$. Let $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ be the nonzero prime ideals of $\mathcal{O}_L$ above $\mathfrak{p}$. For each $i \in \{1, \dots, r\}$, fix $\mathfrak{B}_i \subset \mathcal{O}_L$ whose image modulo $\mathfrak{P}_i$ is a basis of $\mathcal{O}_L/\mathfrak{P}_i$ (so that $\mathfrak{B}_i$ has f_i elements, where $f_i := f_{\mathfrak{P}_i/\mathfrak{p}}$ is the residul degree at $\mathfrak{P}_i$). Let $e_i = e_{\mathfrak{P}_i/\mathfrak{p}}$ be the ramification index at $\mathfrak{P}_i$.
(1) Let $N \geqslant \max\{e_1, \dots, e_r\}$. For $i \in \{1, \dots, r\}$ and $j \in \{1, \dots, e_i\}$, show there exist $\alpha_{i,j} \in \mathfrak{P}_i^{j-1} \cap \bigcap\limits_{k \neq i} \mathfrak{P}_k^N$ such that $\alpha_{i,j} \notin \mathfrak{P}_i^j$.
(2) Put $\mathfrak{L} = \big\{\alpha_{i,j}\beta\,;\, i \in \{1, \dots, r\},\ j \in \{1, \dots, e_i\}, \beta \in \mathfrak{B}_i\big\}$. Show that $\#\mathfrak{L} = n$.
(3) Assume $\sum\limits_{\ell \in \mathfrak{L}} \lambda_\ell \ell \in \mathfrak{p}\mathcal{O}_L$ with $\lambda_\ell \in \mathcal{O}_K$ for all $\ell \in \mathfrak{L}$. Looking modulo $\mathfrak{P}_i$ for all $i \in \{1, \dots, r\}$, then modulo $\mathfrak{P}_i^2$ for all $i \in \{1, \dots, r\}$, *etc*, show that $(\forall \ell \in \mathfrak{L})\ \lambda_\ell \in \mathfrak{p}$, and deduce that $\mathfrak{L}$ is independent modulo $\mathfrak{p}$.
We assume henceforth that $K = \mathbf{Q}$, so that $\mathfrak{p} = p\mathbf{Z}$ where p is a prime number.
(4) Let $\{\alpha_1, \dots, \alpha_n\} \subset \mathcal{O}_L$ be an independent family modulo $\mathfrak{p}$. Show that it is a basis of L over $\mathbf{Q}$.
(5) Let A be the sub-$\mathbf{Z}$-module of $\mathcal{O}_L$ generated by $\{\alpha_1, \dots, \alpha_n\}$. Show that $\mathcal{O}_L/A$ is finite, then that $p \nmid [\mathcal{O}_L : A]$ [hint: reductio ad absurdum].
(6) Deduce that $\mathsf{disc}(\alpha_1, \dots, \alpha_n) = md_L$ with $p \nmid m$.
(7) Assume now that $\{\alpha_1, \dots, \alpha_n\}$ is the family constructed in question (3). Show that $p^s \mid \mathsf{disc}(\alpha_1, \dots, \alpha_n)$, then that $p^s \mid d_L$, with $s = \sum\limits_{i=1}^{r} (e_i - 1) f_i = n - \sum\limits_{i=1}^{r} f_i$.

Exercise 2.7.2. Let $f(X) = X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n \in \mathbf{Z}[X]$ and p a prime number dividing a_n. Write $a_n = p^d b_n$ with $p \nmid b_n$. Assume that $p^d \mid a_i$ for all $i \in \{1, \dots, n\}$ and that $f(X)$ is irreducible[26] in $\mathbf{Z}[X]$. Let $\alpha \in \mathbf{C}$ be a root of $f(X)$ and $L = \mathbf{Q}[\alpha]$.
(1) Show that $\alpha^n = p^d\beta$ with $\beta \in \mathcal{O}_L$ prime to p.
(2) Deduce that $p^d\mathcal{O}_L$ is the n-th power of an ideal of $\mathcal{O}_L$.
(3) Show that if d is prime to n, then $p\mathcal{O}_L$ is the n-th power of an ideal of $\mathcal{O}_L$, and conclude that p is totally ramified in L in that case.
(4) Show that if d is prime to n, then $p^{n-1} \mid d_L$ [hint: use exercise 2.7.1].
(5) What can be said when $\mathsf{gcd}(d, n) > 1$?

[26] By Eisenstein's criterion, this is automatic when $d = 1$.

Exercise 2.7.3. Let A be a commutative ring. Show that A is a DVR if and only if A is local, noetherian, and its maximal ideal is principal, generated by a non nilpotent ideal.

Exercise 2.7.4. A Dedekind ring which is a UFD is a PID.

Exercise 2.7.5. Show that the ring of integers of $\mathbf{Q}(\sqrt{10})$ (*i.e.* the integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\sqrt{10})$) is a Dedekind ring but not a PID [hint: show that the ideal generated by 3 and $\sqrt{10}-1$ is not principal].

Exercise 2.7.6. Show that a module over a Dedekid ring is flat if and only if it is torsion-free.

Exercise 2.7.7. Let R be a Dedekind ring and $I \subset R$ a nonzero ideal. Show that R/I contains only finitely many ideals.

Exercise 2.7.8. Let R be a Dedekind ring, and I, J nonzero ideals of R. Show that there exists an integral ideal $I_1 \subset R$ which is prime to both I and J and such that $II_1 = \langle a\rangle$ is principal in R [hint: use the Chinese remainder theorem]. Prove also that there exists a nonzero element $\alpha \in \mathsf{Frac}(R)$ such that αI and J are coprime integral ideals in R.

Exercise 2.7.9. Let A be a Dedekind ring, K its fraction field, and $I, J \subset K$ nonzero fractional ideals.
(1) Let X be a finite set of nonzero prime ideals of A, and $(n_{\mathfrak{p}})_{\mathfrak{p}\in X}$ a sequence of integers. Show that there exists $x \in K$ such that $v_{\mathfrak{p}}(x) = n_{\mathfrak{p}}$ for all $\mathfrak{p} \in X$ and $v_{\mathfrak{p}}(x) \geqslant 0$ if $\mathfrak{p} \notin X$.
(2) Show that there are $x, y \in K^\times$ such that xI and yJ are coprime ideals of A.
(3) Deduce that $I \oplus J \simeq A \oplus IJ$.
(4) Let $I, J \subset K$ be nonzero fractional ideals in K, and $n, m \in \mathbf{Z}_{\geqslant 0}$. Show that $A^n \oplus I \simeq A^m \oplus J$ if and only if $n = m$ and $[I] = [J]$ in $\mathsf{Cl}(A)$ (*i.e.* if and only if there exists $z \in K^\times$ such that $J = zI$).

Exercise 2.7.10. Let A be a Dedekind ring, and M an A-module of finite type.
(1) Show that if M is torsion-free, then it is projective.
(2) Show that if M is torsion-free, then M is isomorphic to a direct sum of ideals [hint: induction on the rank of a free A-module containing M].
(3) In general, show that $M \simeq A^k \oplus \mathfrak{a} \oplus T$ where $k \in \mathbf{Z}_{\geqslant 0}$, $\mathfrak{a} \subset A$ is an ideal and T is the torsion of M.
(4) Show that T, k and $[\mathfrak{a}] \in \mathsf{Cl}(A)$ are uniquely determined.

Exercise 2.7.11. Let A be a Dedekind ring, and M a nonzero finitely generated torsion A-module.
(1) Put $I = \mathsf{ann}_A(M) = \{a \in A\,;\, (\forall m \in M)\, am = 0\}$. Show that I is a nonzero ideal in A. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be nonzero the prime ideals of A that divide I.
(2) Show that $S := A \backslash \bigcup\limits_{i=1}^{r} \mathfrak{p}_i$ is a multiplicative part in A, and that $S^{-1}A$ is a PID.
(3) Let N be an A-module such that $IN = 0$. Show that $N \simeq (A/I) \otimes_A S^{-1}N$.
(4) Show that there are uniquely determined ideals $I_1 \supset I_2 \supset \cdots \supset I_m \neq 0$ such that
$$M \simeq \bigoplus_{k=1}^{m} A/I_k.$$

Exercise 2.7.12. Let $A = \mathbf{Z}\left[\sqrt{-5}\right]$ and $K = \mathsf{Frac}(A) = \mathbf{Q}(\sqrt{-5})$. Explain why $I = 3A + (1+\sqrt{-5})A \subset K$ is a projective A-module. Show it explicitely as a direct factor of A^2. Show that it is not free.

Exercise 2.7.13. Let A be an integral domain which is not a field and such that for each ideal $I \subset A$ and each $a \in I\backslash\{0\}$, there exists $b \in I$ such that $I = \langle a, b\rangle$. Show that A is a Dedekind ring [hint: show that for each nonzero prime ideal $\mathfrak{p}$, the ring $A_{\mathfrak{p}}$ is a DVR].

Exercise 2.7.14. Let A be a ring. Show that A is a Dedekind ring if and only if A is a noetherian integrally closed domain such that A/I is artinian[(27)] for every non-zero ideal $I \subset A$.

Exercise 2.7.15. Let K be a field, $A = K[X, Y]$ and $I = XA + YA$. Show that $I^{-1} = A$, hence I is not invertible.

[(27)] *I.e.* satisfies the descending chain condition on ideals; that is, there is no infinite descending sequence of ideals.

Exercise 2.7.16. Let $A = \mathbf{Z}\left[\sqrt{-3}\right] \subset K = \mathbf{Q}(\sqrt{-3})$ and $I = A + Aj \subset K$ the fractional ideal generated by 1 and $j = \frac{-1+\sqrt{-3}}{2}$. Is I invertible?

Exercise 2.7.17. Let A be an integral domain in which every nonzero ideal is invertible. Show that A is a field or a Dedekind ring [hint: start by showing that A is noetherian, then that every nonzero ideal has a unique (up to the order) factorization as a product of maximal ideals].

Exercise 2.7.18. Let A be a noetherian integral domain in which every maximal ideal is invertible. Show that A is a field or a Dedekind ring.

Exercise 2.7.19. Let $B = \mathbf{C}[X, Y]/\langle Y^2 - (X^3 - X)\rangle$. The aim of this exercise is to show that B is a Dedekind ring. Put $A = \mathbf{C}[X]$ and $K = \mathbf{C}(X) = \mathsf{Frac}(A)$. Let $y \in \overline{K}$ be a root of $Y^2 - (X^3 - X) \in A[Y]$, $L = K[y]$ and $\mathcal{O}_L$ the ring of elements in L that are integral over A.
(1) Show that B is isomorphic to $A[y]$.
(2) What is $\dim_K(L)$? Show that $\mathsf{Frac}(A[y]) = L$ and that $A[y] \subseteq \mathcal{O}_L$.
(3) Let $z = a(X) + b(X)y \in \mathcal{O}_L$. Using the trace, show that $a(X) \in A$ and that there exists $P \in A$ such that $b(x) = \frac{P(X)}{X^3-X}$.
(4) Using the norm, show that $X^3 - X$ divides P^2. Deduce that $b(X) \in A$.
(5) Show that B is a Dedekind ring.

Exercise 2.7.20. Let A be a Dedekind ring, K its fraction field and X an indeterminate.
(1) The *content* of a polynomial $P \in A[X]$ is the ideal $\mathfrak{c}(P)$ generated by the coefficients of P. Show that $\mathfrak{c}(PQ) = \mathfrak{c}(P)\mathfrak{c}(Q)$ for all $P, Q \in A[X]$.
(2) Let $S = \{P \in A[X]\,;\, \mathfrak{c}(P) = A\}$. Show that S is a multiplicative part in $A[X]$: let

$$B = S^{-1}(A[X]) \subset \mathsf{Frac}(A[X])$$

be the associated localization. Show that if $P, Q \in A[X]$ and $Q \neq 0$, then $\frac{P}{Q} \in B$ if and only if $\mathfrak{c}(P) \subset \mathfrak{c}(Q)$.
(3) Show that $K \cap B = A$. Let $J \subset B$ be an ideal: show that $J = IB$ where $I = J \cap A$, and that the map $I \mapsto IB$ is a bijection between the set of ideals of A onto the set of ideals of B.
(4) Prove that B is a PID.

Exercise 2.7.21. (1) Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field κ. Show that $\mathfrak{m}/\mathfrak{m}^2$ is a κ-vector space of finite dimension, and that $d = \dim_\kappa(\mathfrak{m}/\mathfrak{m}^2)$ is the minimal number of generators of the ideal $\mathfrak{m}$.
(2) Let A be a noetherian integral domain which is not a field. Show that A is a Dedekind ring if and only if for every maximal ideal $\mathfrak{p}$ of A, there are no ideals $I \subset R$ such that $\mathfrak{p}^2 \subsetneq I \subsetneq \mathfrak{p}$.

Exercise 2.7.22. Let $m, n \in \mathbf{Z}\backslash\{0, 1\}$ be coprime squarefree integers. Assume that $m, n \equiv 1 \mod 4\,\mathbf{Z}$ and put $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$ where $\alpha = \frac{1+\sqrt{m}}{2}$ and $\beta = \frac{1+\sqrt{n}}{2}$.
(1) Show that $[K : \mathbf{Q}] = 4$.
(2) Compute $\mathsf{Tr}_{\mathbf{Q}(\sqrt{m})/\mathbf{Q}}(\sqrt{m})$, and deduce $\mathsf{Tr}_{K/\mathbf{Q}}(\sqrt{m})$. Likewise, compute $\mathsf{Tr}_{K/\mathbf{Q}}(\sqrt{n})$ and $\mathsf{Tr}_{K/\mathbf{Q}}(\sqrt{mn})$.
(3) Show that $\mathrm{D}(1, \alpha, \beta, \alpha\beta) = m^2n^2$.
(4) What are the rings of integers of $\mathbf{Q}(\sqrt{m})$, $\mathbf{Q}(\sqrt{n})$ and $\mathbf{Q}(\sqrt{mn})$?
(5) Let $x = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{mn} \in K$ (with $a, b, c, d \in \mathbf{Q}$). Compute $\mathsf{Tr}_{K/\mathbf{Q}(\sqrt{m})}(x)$, $\mathsf{Tr}_{K/\mathbf{Q}(\sqrt{n})}(x)$ and $\mathsf{Tr}_{K/\mathbf{Q}(\sqrt{mn})}(x)$.
(6) Show that $4\mathcal{O}_K \subset \mathbf{Z}[\alpha, \beta]$, and that $\mathcal{O}_K = \mathbf{Z}[\alpha, \beta]$.
We assume henceforth that $m, n \equiv 1 \mod 8\,\mathbf{Z}$.
(7) What is the minimal polynomial of α (resp. β) over $\mathbf{Q}$ (resp. over $\mathbf{Q}(\sqrt{m})$)?
(8) Deduce an isomorphism

$$A := (\mathbf{Z}/2\,\mathbf{Z})[X, Y]/\langle X^2 - X, Y^2 - Y\rangle \xrightarrow{\sim} \mathcal{O}_K/2\mathcal{O}_K$$

(9) Show that there are exactly four ring homomorphisms $A \to \mathbf{Z}/2\,\mathbf{Z}$.
(10) Deduce that A is not isomorphic to $(\mathbf{Z}/2\,\mathbf{Z})[X]/\langle P(X)\rangle$ with $P(X) \in (\mathbf{Z}/2\,\mathbf{Z})[X]$ of degree 4 [hint: the ring homomorphisms $(\mathbf{Z}/2\,\mathbf{Z})[X]/\langle P\rangle \to \mathbf{Z}/2\,\mathbf{Z}$ are in bijection with the set of roots of P in $\mathbf{Z}/2\,\mathbf{Z}$].
(11) Deduce that there is no $x \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbf{Z}[x]$.
(12) What is the decomposition of $2\mathcal{O}_K$ as a product of nonzero prime ideals of $\mathcal{O}_K$? Same question for $p\mathcal{O}_K$ where p is a prime number dividing m.

Exercise 2.7.23. Let A be a Dedekind ring, $K = \mathsf{Frac}(A)$ and L/K a finite separable field extension of degree n. Denote B the integral closure of A in L. Fix $x \in B$ such that $L = K(x)$, put $C = A[x] \subset B$ and let $P \in A[X]$ the minimal polynomial of x over K.

(1) Show that $\frac{1}{P(T)} = \sum\limits_{i=1}^{n} \frac{1}{P'(x_i)(T-x_i)}$ where $x_1, \ldots, x_n \in \overline{K}$ are the conjugates of x over K.

(2) Show that $\mathsf{Tr}_{L/K}\left(\frac{x^k}{P'(x)}\right) = \begin{cases} 0 & \text{if } 0 \leqslant k \leqslant n-2 \\ 1 & \text{si } k = n-1 \end{cases}$.

(3) Show that the A-module C^* is free with basis $\left(\frac{x^k}{P'(x)}\right)_{0 \leqslant k < n}$.

(4) Show that for all $c \in C$, we have $cB \subset C \Leftrightarrow c \in P'(x)\mathfrak{D}_{B/A}^{-1}$ (so that $\mathfrak{D}_{B/A}$ divides $P'(x)B$).

(5) Deduce that $B = C \Leftrightarrow \mathfrak{D}_{B/A} = P'(x)B$.

(6) Assuming that $B = C$, show that $\Omega^1_{B/A} \simeq B/\mathfrak{D}_{B/A}$.

Exercise 2.7.24. Let A be a Dedekind ring, $K = \mathsf{Frac}(A)$ and L/K a finite separable field extension of degree n. Denote B the integral closure of A in L. If $\mathfrak{P}$ is a nonzero prime ideal in B above $\mathfrak{p} \subset A$ is such that $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is separable, show that $v_{\mathfrak{P}}(\mathfrak{D}_{B/A}) \geqslant e_{\mathfrak{P}} - 1$, with equality if and only if $e_{\mathfrak{P}}$ is prime to $\mathsf{char}(\kappa(p))$ [hint: localize an complete to reduce to the case where A and B are complete DVRs, and use previous exercises].

Exercise 2.7.25. Let $A \subset B$ be DVRs with fraction fields $K \subset L$. Assume L/K that the residual extension κ_L/κ_K is purely inseparable of height 1 (*i.e.* such that $\kappa_L^p \subset \kappa_K$, where $p = \mathsf{char}(\kappa_K)$), and not monogenic. Show that $\Omega^1_{B/A}$ is not monogenic.

Exercise 2.7.26. Let A be a Dedekind ring, $K = \mathsf{Frac}(A)$ and L/K a finite and separable field extension. Denote by B the integral closure of A in L, and $\mathscr{P}_A$ the set of nonzero prime ideals of A. An *A-order* of L is a subring R of L such that $A \subset R$ and R is an A-module of finite type.

(1) Let R be a subring of L such that $A \subset R$. Show that R is an A-order of L if and only if $R \subset B$.

(2) Assume that R is an A-order of L.

(i) Show that for all $\mathfrak{p} \in \mathscr{P}_A$, the localization $R_{\mathfrak{p}}$ is an $A_{\mathfrak{p}}$-order of L.
(ii) Show that $R = B$ if and only if $R_{\mathfrak{p}} = B_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathscr{P}_A$.
(iii) Show that nonzero prime ideals of R are maximal.

(3) Let R be an A-order of L and $\theta \in R$ such that $L = K(\theta)$. Denote by $P(X)$ the minimal polynomial of θ over K. Let $\mathfrak{p} \in \mathscr{P}_A$ and $\overline{P}$ the image of P in $\kappa(\mathfrak{p})[X]$, where $\kappa(\mathfrak{p}) = A/\mathfrak{p}$. Show that if $\overline{P}$ is separable, then $R_{\mathfrak{p}} = B_{\mathfrak{p}}$ and the prime ideals of B above $\mathfrak{p}$ are unramified [hint: recall that $A[\theta]^* = \frac{1}{P'(\theta)}A[\theta]$].

(4) Let $R \subset R'$ be an extension of rings, the *conductor* of R'/R is $\mathfrak{c}_{R'/R} = \{r \in R\,;\, rR' \subset R\}$.

(i) Show that $\mathfrak{c}_{R'/R}$ is the largest ideal of R' that is contained in R.
(ii) Let R be an A-order of L and $S \subset R$ a multiplicative part. Show that $\mathfrak{c}_{S^{-1}B/S^{-1}R} = S^{-1}\mathfrak{c}_{B/R}$ [hint: use the fact that B is finite over R].
(iii) Let R be an A-order of L. Show that $\mathfrak{c} := \mathfrak{c}_{B/R} \neq \{0\}$ if and only if $\mathsf{Frac}(R) = L$.

Assume henceforth that $\mathsf{Frac}(R) = L$.

(5) Show that $\mathfrak{c}R^* \subset \mathfrak{D}_{B/A}^{-1}$ (where $R^* = \{y \in L\,;\, (\forall x \in R)\ \mathsf{Tr}_{L/K}(xy) \in A\}$), and that this inclusion is an equality when $R = A[\theta]$ for some $\theta \in L$ such that $L = K(\theta)$.

(6) In this question we assume that $A = \mathbf{Z}$.

(i) Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_L$ and put $R = \mathbf{Z} + \mathfrak{a}$. Show that R is a $\mathbf{Z}$-order of L, with conductor $d\mathbf{Z} + \mathfrak{a}$, where $d \in \mathbf{Z}_{>0}$ is such that $\mathbf{Z} \cap \mathfrak{a} \subset d\mathbf{Z}$.
(ii) Assume that $L = \mathbf{Q}(\sqrt{5})$. Show that $R = \mathbf{Z}[\sqrt{5}]$ is a $\mathbf{Z}$-order of L. What is its conductor?

(7) Let $\mathfrak{q} \in \mathscr{P}_B$. Show that $\mathfrak{c} \subset \mathfrak{q}$ if and only if $\mathfrak{c} \subset \mathfrak{q} \cap R$. Deduce that if $\mathsf{Frac}(R) = L$, there are only finitely many prime ideals of R that contain $\mathfrak{c}$.

(8) (hard) Let $\mathfrak{p}$ be a nonzero prime ideal of R. Show that the following are equivalent:

(a) $\mathfrak{p}$ does not contain $\mathfrak{c}$;
(b) $R = \{x \in L\,; x\mathfrak{p} \subset \mathfrak{p}\}$;
(c) $\mathfrak{p}$ is invertible;
(d) $R_{\mathfrak{p}}$ is a DVR.

[hint: to show (a)⇒(b), use the fact that $\mathfrak{p} + \mathfrak{c} = R$; to show (b)⇒(c), use the fact that if $\alpha \in \mathfrak{p}\backslash\{0\}$, there exists $r \in \mathbf{Z}_{>0}$ such that $\mathfrak{p}^r R_{\mathfrak{p}} \subset \alpha R_{\mathfrak{p}}$; to show (c)⇒(d), show that nonzero ideals of $R_{\mathfrak{p}}$ are powers of $\mathfrak{p}R_{\mathfrak{p}}$, then that $R_{\mathfrak{p}}$ is integrally closed.]

(9) (hard) Show that under the equivalent conditions of question (8), $\mathfrak{p}B$ is the only maximal ideal of B that contains $\mathfrak{p}$ [hint: take $\mathfrak{q} \in \mathscr{P}_B$ such that $\mathfrak{p} \subset \mathfrak{q}$, and show that $R_\mathfrak{p} = B_\mathfrak{q}$.]

3. Valued fields

In this section, K denotes a field.

3.1. Absolute values.

Definition 3.1.1. An *absolute value* on K is a map $|.| : K \to \mathbf{R}_{\geqslant 0}$ such that:

(1) $(\forall x \in K)\,(|x| = 0 \Leftrightarrow x = 0)$;
(2) $(\forall x, y \in K)$ $|xy| = |x|\,|y|$ (multiplicativity);
(3) $(\forall x, y \in K)$ $|x + y| \leqslant |x| + |y|$ (triangle inequality).

If it satisfies the stronger requirement

(3') $(\forall x, y \in K)$ $|x + y| \leqslant \max\{|x|, |y|\}$ (strong triangle inequality),

the absolute value is called *non archimedean.* It is called *archimedean* otherwise.
The pair $(K, |.|)$ is called a *valued field.* We say that $(K, |.|)$ is archimedean (resp. non archimedean) if $|.|$ is.

Example 3.1.2. (0) The *trivial* absolute value on K is given by $|0| = 0$ and $|x| = 1$ for all $x \in K^\times$ (it is non archimedean).
(1) The "usual" absolute value $|.|_\infty$ on $K = \mathbf{R}$, and the modulus $|.|_\infty$ on $\mathbf{C}$ are archimedean.
(2) Let p be a prime number, and $v_p\colon \mathbf{Z} \to \mathbf{Z}_{\geqslant 0} \cup \{+\infty\}$ the p-adic valuation. It extends into a map $v_p\colon \mathbf{Q} \to \mathbf{Z} \cup \{+\infty\}$: if $x \in \mathbf{Q}$, put $|x|_p = p^{-v_p(x)}$. This defines a non archimedean absolute value called the p-adic absolute value.

Remark 3.1.3. (1) Let $|.|$ be an absolute value on K. By (2), we have $|1|^2 = |1|$, so $|1| = 1$ since $|1| \neq 0$ by (1). In particular, we have $\left|x^{-1}\right| = |x|^{-1}$ for all $x \in K^\times$, and $|.| : K^\times \to \mathbf{R}_{>0}$ is a group homomorphism.
(2) Assume $|.|$ is a non archimedean absolute value on K. If $x, y \in K$ are such that $|x| \neq |y|$, say $|x| < |y|$, then $|y| \leqslant \max\{|x|, |x + y|\}$ by (3), so $|y| \leqslant |x + y|$ whence $|x + y| = |y|$. This shows that (3') is an equality whenever $|x| \neq |y|$.
(3) The *group of the absolute value* $|.|$ is $|K^\times|$: this is a subgroup of $\mathbf{R}_{>0}$. There exist notions of absolute values with groups more complicated that subgroups of $\mathbf{R}_{>0}$, but we will not need these. The absolute value $|.|$ is called *discrete* if $|K^\times|$ is a discrete subgroup of $\mathbf{R}_{>0}$. Note that $|K^\times|$ is dense in $\mathbf{R}_{>0}$ otherwise.

Definition 3.1.4. Let $(K_1, |.|_1)$ and $(K_2, |.|_2)$ be valued fields. A *morphism of valuation fields* from K_1 to K_2 is a morphism of fields $f\colon K_1 \to K_2$ (so it is automatically injective) such that $|f(x)|_2 = |x|_1$ for all $x \in K_1$. It is an *isomorphism* when f is surjective.

Definition 3.1.5. An absolute value on K defines a topology on K (indeed a metric space structure): a basis of open neighborhoods of $a \in K$ is given by $\mathsf{B}(a, r) = \{x \in K\,;\, |x - a| < r\}$ for $r \in \mathbf{R}_{>0}$.
Two absolute values are *equivalent* when they define the same topology on K.

Example 3.1.6. The topology defined by the trivial absolute value is the discrete topology.

Proposition 3.1.7. *Two absolute values $|.|_1$ and $|.|_2$ on K are equivalent if and only if there exists $\gamma \in \mathbf{R}_{>0}$ such that $|.|_2 = |.|_1^\gamma$.*

Proof. Assume $|.|_1$ and $|.|_2$ are equivalent. If $|.|_1$ is trivial, then the topology defined by $|.|_2$ is discrete. If $x \in K$ and $|x|_2 < 1$, then $\lim\limits_{n\to\infty} x^n = 0$, so $x = 0$. If $x \in K^\times$, then $|x|_2 \geqslant 1$, and also $|x|_2^{-1} = |x|_2^{-1} \geqslant 1$, *i.e.* $|x|_2 \leqslant 1$, so $|x|_2 = 1$, and $|.|_2$ is discrete as well. Assume from now on that $|.|_1$ and $|.|_2$ are not trivial: there exists $x_0 \in K$ such that $0 < |x_0|_1 < 1$. If $|x|_1 < 1$, then $\lim\limits_{n\to\infty} x^n = 0$, so $|x|_2 < 1$ as well, in particular $0 < |x_0|_2 < 1$: put $\gamma = \frac{\ln(|x_0|_2)}{\ln(|x_0|_1)} \in \mathbf{R}_{>0}$.
Let $x \in K$ be such that $0 < |x|_1 < 1$ and put $\lambda = \frac{\ln(|x|_1)}{\ln(|x_0|_1)} \in \mathbf{R}_{>0}$. If $r \in \mathbf{Q} \cap]\lambda, +\infty[$, then $r = \frac{m}{n}$ with $m, n \in \mathbf{Z}_{>0}$, and the inequality $\lambda < \frac{m}{n}$ is equivalent to $|x|_1^n < |x_0|_1^m$, *i.e.* $\left|\frac{x^n}{x_0^m}\right|_1 < 1$. This implies that $\left|\frac{x^n}{x_0^m}\right|_2 < 1$ from what precedes, *i.e.* $\frac{\ln(|x|_2)}{\ln(|x_0|_2)} < \frac{m}{n} = r$. Since this holds for all $r \in \mathbf{Q} \cap]\lambda, +\infty[$, we have $\frac{\ln(|x|_2)}{\ln(|x_0|_2)} \leqslant \lambda$, *i.e.* $\frac{\ln(|x|_2)}{\ln(|x_0|_2)} \leqslant \frac{\ln(|x|_1)}{\ln(|x_0|_1)}$. As $|.|_1$ and $|.|_2$ play symmetric roles, we have in fact $\frac{\ln(|x|_2)}{\ln(|x_0|_2)} = \frac{\ln(|x|_1)}{\ln(|x_0|_1)}$, thus $\frac{\ln(|x|_2)}{\ln(|x|_1)} = \gamma$, *i.e.* $|x|_2 = |x|_1^\gamma$, whenever $x \in K^\times$ satisfies $|x|_1 < 1$. Replacing x by x^{-1} shows that it holds true also when $|x|_1 > 1$. Exchanging $|.|_1$ and $|.|_2$, we have similarly the implication $|x|_2 \neq 1 \Rightarrow |x|_1 \neq 1$, so $|x|_1 = 1 \Rightarrow |x|_2 = 1$, *i.e.* $|x|_2 = |x|_1^\gamma$ for all $x \in K$. □

Remark 3.1.8. If $|.|$ is an archimedean absolute value on K, the map $|.|^\gamma$ is *not* an absolute value for any $\gamma \in \mathbf{R}_{>0}$ in general, for the triangle inequality might not be satisfied by $|.|^\gamma$ (it is when $0 < \gamma \leqslant 1$ by convexity of the map $t \mapsto t^\gamma$).

Definition 3.1.9. Let K be a field. A *place* of K is a class of equivalence of non trivial absolute values on K. The set of place is denoted $\mathsf{V}(K)$.

Theorem 3.1.10. (Ostrowski). A non-trivial absolute value on $\mathbf{Q}$ is equivalent to either the "usual" absolute value or to a p-adic absolute value.

Proof. Let $|.| : \mathbf{Q} \to \mathbf{R}_{\geqslant 0}$ be a non trivial absolute value. Let $a, b \in \mathbf{Z}_{>1}$. For $n \in \mathbf{Z}_{\geqslant 0}$, let

$$a^n = \alpha_0 + \alpha_1 b + \cdots + \alpha_r b^r$$

be the writing of a^n in base b: we have $r = \lfloor n \log_b(a) \rfloor$ and $\alpha_i \in \{0, \ldots, b-1\}$ for $i \in \{0, \ldots, r\}$ (and $\alpha_r \neq 0$). Then $|a|^n \leqslant \sum\limits_{i=0}^{r} |\alpha_i| \, |b|^i \leqslant (r+1) M_b \max\{1, |b|^r\}$, where $M_b = \max\limits_{0 \leqslant i < b} |i|$, so that

$$|a| \leqslant \big(n \log_b(a) + 1\big)^{1/n} M_b^{1/n} \max\big\{1, |b|^{\log_b(a)}\big\}.$$

As $\lim\limits_{n \to \infty} \big(n \log_b(a) + 1\big)^{1/n} M_b^{1/n} = 1$, we get $|a| \leqslant \max\big\{1, |b|^{\log_b(a)}\big\}$.

- First case. $|a| > 1$. This implies that $|a| \leqslant |b|^{\log_b(a)}$, so in particular $|b| > 1$, and $|a|^{1/\ln(a)} \leqslant |b|^{1/\ln(b)}$. As $|b| > 1$, we have $|b|^{1/\ln(b)} \leqslant |a|^{1/\ln(a)}$ as well, so that $|x|^{1/\ln(x)}$, hence $c := \frac{\ln|x|}{\ln(x)}$ does not depend on $x \in \mathbf{Z}_{>1}$. This implies that $|x| = x^c$ for all $x \in \mathbf{Z}_{>1}$. The axioms of absolute value imply that $|x| = |x|_\infty^c$ for all $x \in \mathbf{Q}$, and $|.|$ is equivalent to the "usual" absolute value.
- Second case. For all $a \in \mathbf{Z}_{>1}$, we have $|a| \leqslant 1$ (so that $|x| \leqslant 1$ for all $x \in \mathbf{Z}$). As $|.|$ is non trivial, there exists $a \in \mathbf{Z}_{>1}$ such that $|a| < 1$. Factoring a into a product of primes, we get at least one prime p such that $|p| < 1$. If q is an other prime and $n \in \mathbf{Z}_{\geqslant 0}$, we have $\gcd(p^n, q^n) = 1$: there exist $u, v \in \mathbf{Z}$ such that $up^n + vq^n = 1$, so that $1 \leqslant |u| \, |p|^n + |v| \, |q|^n \leqslant |p|^n + |q|^n$. As $\lim\limits_{n \to \infty} |p|^n = 0$, this implies that $|q| \geqslant 1$, whence $|q| = 1$. This shows in particular that $|x| = 1$ whenever $x \in \mathbf{Z} \backslash p\mathbf{Z}$, so that $|x| = |x|_p^c$ with $c = -\frac{\ln|p|}{\ln(p)}$ for all $x \in \mathbf{Z}$, whence for all $x \in \mathbf{Q}$, so that $|.|$ is equivalent to the p-adic absolute value. □

Remark 3.1.11. We have the *product formula*

$$\prod_{v \in \mathsf{V}(\mathbf{Q})} |x|_v = 1$$

for all $x \in \mathbf{Q}^\times$.

3.1.12. *The approximation theorem.* Let K be a field.

Lemma 3.1.13. Let $|.|$ be an absolute value on K and $x \in K$. Then

$$\lim_{m \to \infty} \frac{x^m}{1 + x^m} = \begin{cases} 0 & \text{if } |x| < 1 \\ 1 & \text{if } |x| > 1 \end{cases}$$

Proof. We have $\frac{x^m}{1+x^m} - 1 = -\frac{1}{1+x^m}$. □

Lemma 3.1.14. Let $|.|_1, \ldots, |.|_n$ be pairwise non equivalent non trivial absolute values on K. There exists $a \in K$ such that $|a|_1 > 1$ and $|a|_i < 1$ for all $i \in \{2, \ldots, n\}$. For each $\varepsilon \in \mathbf{R}_{>0}$, there exists $\alpha \in K$ such that $|\alpha - 1|_1 < \varepsilon$ and $|\alpha|_i < \varepsilon$ for all $i \in \{2, \ldots, n\}$.

Proof. We use induction on $n \in \mathbf{Z}_{\geqslant 2}$.

- Assume $n = 2$ and that such an a does not exist: for all $x \in K$, we have $|x|_1 > 1 \Rightarrow |x|_2 \geqslant 1$. Applied to x^{-1} when $x \neq 0$, this implies that $|x|_1 < 1 \Rightarrow |x|_2 \leqslant 1$. Taking contrapositives, we have the same implications after exchanging $|.|_1$ and $|.|_2$. As $|.|_1$ and $|.|_2$ are non trivial, there exists $y_1, y_2 \in K^\times$ such that $|y_1|_1 < 1$ and $|y_2|_2 < 1$: this implies that $|y|_1 < 1$ and $|y|_2 < 1$ where $y = y_1 y_2$. If $x \in K$ and $n \in \mathbf{Z}_{>0}$ are such that $|x|_1 < |y|_1^n$, we have $\left|\frac{x}{y^n}\right|_1 < 1$, which implies that $\left|\frac{x}{y^n}\right|_2 \leqslant 1$ *i.e.* $|x|_2 \leqslant |y|_2^n$. This shows that for all $a \in K$, we have $\mathsf{B}_1(a, |y|^n) \subset \overline{\mathsf{B}}_2(a, |y|_2^n) \subset \mathsf{B}_2(a, |y|_2^{n-1})$. As the balls $\mathsf{B}_2(a, |y|_2^{n-1})$ for a basis for the topology on K defined by $|.|_2$, this shows that the topology defined by $|.|_1$ is finer than that defined by $|.|_2$. Symmetrically, the topology defined by $|.|_2$ is finer than that defined by $|.|_1$: they are the same, so $|.|_1$ and $|.|_2$ are equivalent, contradicting the hypothesis.
- Assume that $n > 2$. By the induction hypothesis, there exists $b \in K$ such that $|b|_1 > 1$ and $|b|_i < 1$ for all $i \in \{2, \ldots, n-1\}$. By the case $n = 2$, there exists $c \in K$ such that $|c|_1 > 1$ and $|c|_n < 1$.

Case where $|b|_n \leqslant 1$. For $m \in \mathbf{Z}_{>0}$, put $a_m = cb^m$. We have $|a_m|_1 = |c|_1 \, |b|_1^m > 1$ and $|a_m|_n = |c|_n \, |b|_n^m < 1$. If $i \in \{2, \ldots, n-1\}$, we have $|a_m|_i = |c|_i \, |b|_i^m \xrightarrow[m \to \infty]{} 0$, so we can take $a = a_m$ with m is large enough.

Case where $|b|_n > 1$. For $m \in \mathbf{Z}_{>0}$, put $a_m = \frac{cb^m}{1+cb^m}$. As $|b|_1 < 1$ and $|b|_n > 1$, lemma 3.1.13 implies that $\lim\limits_{m\to\infty} a_m = c$ for the absolute values $|.|_1$ and $|.|_n$. As $|c|_1 > 1$ and $|c|_n < 1$, this implies that $|a_m|_1 > 1$ and $|a_m|_n < 1$ whenever m is large enough. On the other hand, if $i \in \{2, \dots, n-1\}$, we have $\lim\limits_{m\to\infty} a_m = 0$ for the absolute value $|.|_i$, so that $|a_m|_i < 1$ for m large enough. Here again we can take $a = a_m$ with m is large enough.

- Using the a we constructed, we have $\lim\limits_{m\to\infty} \frac{a^m}{1+a^m} = 1$ for the absolute value $|.|_1$ and $\lim\limits_{m\to\infty} \frac{a^m}{1+a^m} = 0$ for the absolute values $|.|_i$ if $i \in \{2, \dots, n\}$: we can take $\alpha = \frac{a^m}{1+a^m}$ with m large enough. □

Theorem 3.1.15. (Approximation theorem). Let $|.|_1, \dots, |.|_n$ be pairwise non equivalent non trivial absolute values on K. Given $\varepsilon \in \mathbf{R}_{>0}$ and $y_1, \dots, y_n \in K$, there exists $x \in K$ such that $|x - y_i|_i < \varepsilon$ for all $i \in \{1, \dots, n\}$.

Proof. Let $M = \max\limits_{1\leqslant i\leqslant n} \sum\limits_{k=1}^{n} |y_k|_i$. By lemma 3.1.14, there exist $a_1, \dots, a_n \in K$ such that $|\alpha_i - 1|_i < \frac{\varepsilon}{M}$ and $|\alpha_i|_j < \frac{\varepsilon}{M}$ for all $j \in \{1, \dots, n\}\backslash\{i\}$. Put $x = \sum\limits_{k=1}^{n} \alpha_k y_k$. For $i \in \{1, \dots, n\}$, we have

$$|x - y_i|_i = \Big|(\alpha_i - 1)y_i + \sum_{k\neq i} \alpha_k y_k\Big|_i \leqslant |\alpha_i - 1|_i\, |y_i|_i + \sum_{k\neq i} |\alpha_k|_i\, |y_k|_i < \tfrac{\varepsilon}{M} \sum_{k=1}^{n} |y_k|_i \leqslant \varepsilon.$$

□

3.2. Valuations.

Definition 3.2.1. A *valuation*[28] on a field K is a map $v\colon K \to \mathbf{R} \cup \{+\infty\}$ such that:

(1) $v(x) = +\infty \Leftrightarrow x = 0$;
(2) $(\forall x, y \in K)\, v(xy) = v(x) + v(y)$;
(3) $(\forall x, y \in K)\, v(x+y) \geqslant \min\{v(x), v(y)\}$.

Remark 3.2.2. In condition (3), we have[29] $v(x+y) = \min\{v(x), v(y)\}$ as soon as $v(x) \neq v(y)$ (*cf* remark 3.1.3 (2)).

Definition 3.2.3. (1) The valuation v is *trivial* if $v(K^\times) = \{0\}$. Condition (2) in definition 3.2.1 implies that $v(K^\times)$ is a subgroup of $(\mathbf{R}, +)$. It also implies that $v(1) = 0$. The valuation v is called *discrete* when $v(K^\times)$ is a discrete subgroup of $\mathbf{R}$: it is then of the form $\lambda\mathbf{Z}$ for some $\lambda \in \mathbf{R}_{\geqslant 0}$. A discrete valuation v is called *normalized* when $v(K^\times) = \mathbf{Z}$.
(2) Let K be a field and $v\colon K \to \mathbf{R} \cup \{+\infty\}$ be a valuation. Then

$$\mathcal{O}_{K,v} = \{x \in K\,;\, v(x) \geqslant 0\}$$

is a subring of K called the *ring of integers* of v. Similarly,

$$\mathfrak{m}_{K,v} = \{x \in K\,;\, v(x) > 0\}$$

is an ideal in $\mathcal{O}_{K,v}$.

Proposition 3.2.4. An element $x \in \mathcal{O}_{K,v}$ is invertible in $\mathcal{O}_{K,v}$ if and only if $v(x) = 0$. In particular, $\mathcal{O}_{K,v}$ is a local ring with maximal ideal $\mathfrak{m}_{K,v}$. For all $x, y \in \mathcal{O}_{K,v}\backslash\{0\}$, we have $x \mid y$ in $\mathcal{O}_{K,v}$ if and only if $v(x) \leqslant v(y)$. Moreover $K = \mathcal{O}_{K,v}[\alpha^{-1}]$ for all $\alpha \in \mathfrak{m}_{K,v}\backslash\{0\}$, and $\mathcal{O}_{K,v}$ is integrally closed.

Proof. • If $x \in \mathcal{O}_{K,v}^\times$, then $x^{-1} \in \mathcal{O}_{K,v}$, *i.e.* $v(x^{-1}) \geqslant 0$. As $v(x) + v(x^{-1}) = v(1) = 0$, we must have $v(x) = 0$. Conversely, assume that $v(x) = 0$: as $v(x) + v(x^{-1}) = v(1) = 0$ we have $v(x^{-1}) = 0$, *i.e.* $x^{-1} \in \mathcal{O}_{K,v}$ and $x \in \mathcal{O}_{K,v}^\times$.

- Let $x \in \mathcal{O}_{K,v}\backslash\mathfrak{m}_{K,v}$: we have $v(x) = 0$, so that $x \in \mathcal{O}_{K,v}^\times$ by what precedes. This implies that $\mathcal{O}_{K,v}$ is a local ring with maximal ideal $\mathfrak{m}_{K,v}$.
- Let $x, y \in \mathcal{O}_{K,v}\backslash\{0\}$. If $y = xz$ with $z \in \mathcal{O}_{K,v}$, then $v(y) = v(x) + v(z) \geqslant v(x)$ since $v(z) \geqslant 0$. Conversely, assume that $v(x) \leqslant v(y)$. Put $z = x^{-1}y \in K$. We have $v(z) = v(y) - v(x) \geqslant 0$, hence $z \in \mathcal{O}_{K,v}$ *i.e.* $x \mid y$.
- Assume $\alpha \in \mathfrak{m}_{K,v}\backslash\{0\}$. We certainly have $\mathcal{O}_{K,v}[\alpha^{-1}] \subset K$: let $x \in K$. As $\lim\limits_{n\to\infty} v(x) + nv(\alpha) = +\infty$ (since $v(\alpha) > 0$), there exists $n \in \mathbf{Z}_{\geqslant 0}$ such that $v(\alpha^n x) \geqslant 0$, *i.e.* $\alpha^n x \in \mathcal{O}_{K,v}$, so that $x \in \mathcal{O}_{K,v}[\alpha^{-1}]$.
- Let $z \in K^\times$ be integral over $\mathcal{O}_{K,v}$: write $z = \frac{x}{y}$ with $x, y \in \mathcal{O}_{K,v}\backslash\{0\}$. Let $z^n + a_1 z^{n-1} + \cdots + a_{n-1}z + a_n = 0$ be an equation of integral dependence over $\mathcal{O}_{K,v}$. We have $x^n + a_1 x^{n-1} y + \cdots + a_n y^n = 0$, so that $nv(x) \geqslant$

[28] Some authors call "valuation" what we called "absolute value".

[29] The proof is the same: if $v(x) \neq v(y)$, say $v(x) < v(y)$, then $v(y) > v(x) = v(x + y - y) \geqslant \min\{v(x+y), v(y)\}$, so $v(x+y) \geqslant v(x) \geqslant v(x+y)$ *i.e.* $v(x+y) = v(x)$.

$\min\limits_{1\leqslant i\leqslant n}(v(a_i)+(n-i)v(x)+iv(y))$: there exists $i_0\in\{1,\ldots,n\}$ such that $nv(x)\geqslant v(a_{i_0})+(n-i_0)v(x)+i_0v(y)$, hence $i_0v(x)\geqslant i_0v(y)$ *i.e.* $v(x)\geqslant v(y)$, so that $v(z)\geqslant 0$ *i.e.* $z\in\mathcal{O}_{K,v}$. □

Corollary 3.2.5. The valuation v is non trivial and discrete if and only if $\mathcal{O}_{K,v}$ is a DVR[30].

Proof. • Assume v is non trivial and discrete: write $v(K^\times)=\alpha\mathbf{Z}$ with $\alpha\in\mathbf{R}_{>0}$. Let $\pi\in\mathcal{O}_{K,v}$ be such that $v(\pi)=\alpha$: if $x\in\mathcal{O}_{K,V}\backslash\{0\}$, we have $u:=x\pi^{-v(x)}\in\mathcal{O}_{K,v}^\times$ (because $v(u)=0$, *cf* proposition 3.2.4). This implies that $\mathcal{O}_{K,v}$ is a PID (its ideals are $\{0\}$ and $\langle\pi\rangle^n$ with $n\in\mathbf{Z}_{\geqslant 0}$), whose only nonzero prime ideal is $\langle\pi\rangle$, so that $\mathcal{O}_{K,v}$ is a DVR (*cf* definition 1.8.25).
• Conversely, assume that $\mathcal{O}_{K,v}$ is a DVR: let $\pi\in K$ be a uniformizer. Any non-zero element $x\in K^\times$ can be written in a unique way $x=u\pi^n$ with $u\in\mathcal{O}_{K,v}$ and $n\in\mathbf{Z}$: we have $v(x)=v(u)+nv(\pi)=nv(\pi)$, so that $v(K^\times)=v(\pi)\,\mathbf{Z}$. □

Remark 3.2.6. The map v induces a group homomorphism $K^\times\to\mathbf{R}$. By proposition 3.2.4, its kernel is $\mathcal{O}_{K,v}^\times=\{x\in K\,;\,v(x)=0\}$ (this is the *unit group* of v), so that v induces a group isomorphism

$$K^\times/\mathcal{O}_{K,v}^\times\xrightarrow{\sim}v(K^\times)\subset\mathbf{R}.$$

Definition 3.2.7. The quotient field $\kappa_{K,v}=\mathcal{O}_{K,v}/\mathfrak{m}_{K,v}$ is called the *residue field* of K at v.

Proposition 3.2.8. Let A be a UFD, $p\in A$ a irreducible element and $v_p\colon A\to\mathbf{Z}_{\geqslant 0}$ the p-adic valuation (*cf* definition 1.1.19). Then v_p extends uniquely into a normalized valuation $v_p\colon\mathsf{Frac}(A)\to\mathbf{Z}\cup\{+\infty\}$. If $x\in\mathsf{Frac}(A)$, then $x\in A$ if and only if $v_p(x)\geqslant 0$ for every irreducible element $p\in A$.

Proof. (1) If $x=\frac{a}{b}\in\mathsf{Frac}(A)$, with $a\in A$ and $b\in A\backslash\{0\}$, then $v_p(x)=v_p(a)-v_p(b)\in\mathbf{Z}\cup\{+\infty\}$, proving unicity. If $x=\frac{a'}{b'}$ is an other writing, then $ab'=a'b$ (because A is an integral domain), so $v_p(a)+v_p(b')=v_p(a')+v_p(b)$ (by proposition 1.1.20) *i.e.* $v_p(a)-v_p(b)=v_p(a')-v_p(b')$, proving the existence. The fact that this map is a valuation on $\mathsf{Frac}(A)$ follows from proposition 1.1.20.
(2) Let $x=\frac{a}{b}\in\mathsf{Frac}(A)$ with $a\in A$ and $b\in A\backslash\{0\}$. Assume that $v_p(x)\geqslant 0$ *i.e.* $v_p(a)\geqslant v_p(b)$ for every irreducible element $p\in A$. Then $b\mid a$ (*cf* proposition 1.1.20 (2)), so $x\in A$. The converse is trivial. □

Example 3.2.9. Let A be a DVR with maximal ideal $\mathfrak{m}$ and π a uniformizer. The π-adic valuation map $v\colon A\backslash\{0\}\to\mathbf{Z}_{\geqslant 0}$ extends uniquely into a normalized discrete valuation $v\colon\mathsf{Frac}(A)\to\mathbf{Z}\cup\{+\infty\}$, and we have $A=\{x\in\mathsf{Frac}(A)\,;\,v(x)\geqslant 0\}$ and $\mathfrak{m}=\{x\in\mathsf{Frac}(A)\,;\,v(x)>0\}$.

Proposition 3.2.10. Let v be a valuation on K and $\rho\in]0,1[$. Then the map

$$\begin{aligned}K&\to\mathbf{R}_{\geqslant 0}\\ x&\mapsto\rho^{v(x)}\end{aligned}$$

is a non archimedean absolute value. Conversely, if $|.|$ is a non archimedean absolute value on K, then $-\ln|.|:K\to\mathbf{R}\cup\{+\infty\}$ (with the convention that $-\ln(0)=+\infty$) is a valuation on K.

Definition 3.2.11. (1) A valuation v on K defines a topology on K for which a basis of neighborhoods of 0 is given by $\{x\in K\,;\,v(x)\geqslant r\}_{r\in\mathbf{R}}$.
(2) We say that two valuations v and v' are *equivalent* if they define the same topology. By propositions 3.2.10 and 3.1.7, this is equivalent to the existence of a constant $\gamma\in\mathbf{R}_{>0}$ such that $v'=\gamma v$.

Remark 3.2.12. (1) The topology defined by a valuation v and the absolute value ρ^v (for any $\rho\in]0,1[$) are the same.
(2) If v is a valuation on K and $\alpha\in\mathfrak{m}_{K,v}\backslash\{0\}$, the α-adic topology coincides with that defined by v on $\mathcal{O}_{K,v}$ (because $\alpha^n\mathcal{O}_{K,v}=\{x\in\mathcal{O}_{K,v}\,;\,v(x)\geqslant nv(\alpha)\}$). Note that in general, the $\mathfrak{m}_{K,v}$-topology *does not* coincide with that defined by v on $\mathcal{O}_{K,v}$: when $v(K^\times)$ is a divisible group for instance, one has $\mathfrak{m}_{K,v}^2=\mathfrak{m}_{K,v}$. Nevertheless, these topologies coincide when v is discrete.

Example 3.2.13. (1) On $\mathbf{Z}$ the p-adic valuation induces a valuation v_p on $\mathbf{Q}$ for every prime number p. The associated *p-adic absolute value* is defined by $|x|_p=p^{-v_p(x)}$ for all $x\in\mathbf{Q}$. The ring of integers of $\mathbf{Q}$ with respect to v_p is the localization $\mathbf{Z}_{(p)}$ with respect to the prime ideal $p\mathbf{Z}$. Its residue field is $\mathbf{F}_p$.
(2) Let F be a field and $K=F(X)=\mathsf{Frac}(F[X])$ the field of rational fractions with coefficients in F. The map $-\deg\colon F[X]\to\mathbf{Z}_{\geqslant 0}\cup\{\infty\}$ extends into a valuation on K (with the convention that $\deg(0)=-\infty$), so that for any $r\in\mathbf{R}_{>1}$, the map $R\mapsto r^{\deg(R)}$ defines a non archimedean absolute value.

[30] Obviously, the terminology well thought-out.

3.3. **Complete valued fields.** Assume K is endowed with an absolute value $|.|$.

Definition 3.3.1. (1) A sequence $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ with values in K is a *Cauchy sequence* if for every $\varepsilon\in\mathbf{R}_{>0}$ there exists $N\in\mathbf{Z}_{\geqslant 0}$ such that for all $m,n\geqslant N$, we have $|x_n-x_m|<\varepsilon$.
(2) A convergent sequence is a Cauchy sequence, and we say that K is *complete* (for $|.|$) when the converse holds.

Example 3.3.2. The field $\mathbf{Q}$ is not complete for the archimedean absolute value $|.|_\infty$, nor for the p-adic absolute values.

Proposition 3.3.3. There exists a complete valued field $(\widehat{K},|.|)$ and a morphism of valued fields $\iota\colon K\to\widehat{K}$ such that $\iota(K)$ is dense in $\widehat{K}$.

Proof. Let $\mathscr{C}(K)$ be the set of Cauchy sequences with values in K. This is a ring when endowed with componentwise addition and multiplication. Denote by $\mathscr{I}(K)$ the set of sequences with values in K that converge to 0. This is an ideal in $\mathscr{C}(K)$: put $\widehat{K}=\mathscr{C}(K)/\mathscr{I}(K)$, and let $\iota\colon K\to\widehat{K}$ be the map defined by $\iota(x)=\pi(x,x,x,\ldots)$ where $\pi\colon\mathscr{C}(K)\to\widehat{K}$ is the projection. The map ι is a ring homomorphism making $\widehat{K}$ into a K-algebra.

- The ring $\widehat{K}$ is a field. Let $\underline{x}=(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}\in\mathscr{C}(K)\backslash\mathscr{I}(K)$: we have to show that $\pi(\underline{x})$ is invertible. There exists $\varepsilon_0\in]0,1[$ such that for all $N\in\mathbf{Z}_{\geqslant 0}$, there exists $n\geqslant N$ such that $|x_n|\geqslant\varepsilon_0$. As $\underline{x}$ is Cauchy, there exists $N_0\in\mathbf{Z}_{\geqslant 0}$ such that $n,m\geqslant N_0\Rightarrow|x_n-x_m|<\frac{\varepsilon_0}{2}$. By what precedes, there exists $N_1\geqslant N_0$ such that $|x_{N_1}|\geqslant\varepsilon_0$. This implies that $|x_n|>\frac{\varepsilon_0}{2}$ for all $n\geqslant N_1$. Now changing finitely many terms in $\underline{x}$ does not modify $\pi(\underline{x})$: we may assume that $x_n=1$ for all $n<N_1$. This implies in particular that $|x_n|>\frac{\varepsilon_0}{2}$ hence $x_n\neq 0$ for all $n\in\mathbf{Z}_{\geqslant 0}$: we may consider the sequence $\underline{y}=(x_n^{-1})_{n\in\mathbf{Z}_{\geqslant 0}}$. Let's show it is a Cauchy sequence: fix $\varepsilon\in\mathbf{R}_{>0}$. There exists $N\in\mathbf{Z}_{\geqslant 0}$ such that $n,m\geqslant N\Rightarrow|x_n-x_m|<\frac{\varepsilon_0^2\varepsilon}{4}$. Then $\left|x_n^{-1}-x_m^{-1}\right|=\frac{|x_n-x_m|}{|x_nx_m|}<\varepsilon$ for all $n,m\geqslant N$. Thus $\underline{y}\in\mathscr{C}(K)$, and $\underline{xy}=1$.
- The field $\widehat{K}$ is valued. Let $\underline{x}=(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}\in\mathscr{C}(K)$. For all $n,m\in\mathbf{Z}_{\geqslant 0}$, we have $||x_n|-|x_m||\leqslant|x_n-x_m|$: this implies that $(|x_n|)_{n\in\mathbf{Z}_{\geqslant 0}}$ is a Cauchy sequence in $\mathbf{R}$: it converges. Its limit in $\mathbf{R}$ depends only on $\pi(\underline{x})$: this defines a map $|.|:\widehat{K}\to\mathbf{R}_{\geqslant 0}$. The absolute value axioms pass to the limit: the map $|.|:\widehat{K}\to\mathbf{R}_{\geqslant 0}$ is an absolute value. It extends $|.|$ on K, so ι is a morphism of valued fields.
- If $\underline{x}=(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}\in\mathscr{C}(K)$, the sequence $(\iota(x_n))_{n\in\mathbf{Z}_{\geqslant 0}}$ converges to $\pi(\underline{x})$ in $(\widehat{K},|.|)$. Indeed, let $\varepsilon\in\mathbf{R}_{>0}$: there exists $N\in\mathbf{Z}_{\geqslant 0}$ such that $n,m\geqslant N\Rightarrow|x_n-x_m|<\varepsilon$, so that $|\iota(x_n)-\pi(\underline{x})|=\lim\limits_{m\to\infty}|x_n-x_m|\leqslant\varepsilon$ for all $n\geqslant N$. In particular, $\iota(K)$ is dense in $\widehat{K}$.
- $(\widehat{K},|.|)$ is complete. Let $(\xi_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ be a Cauchy sequence in $\widehat{K}$. For each $n\in\mathbf{Z}_{\geqslant 0}$, choose $x_n\in K$ such that $|\xi_n-\iota(x_n)|<\frac{1}{n+1}$. Let $\varepsilon\in\mathbf{R}_{>0}$: there exists $N\in\mathbf{Z}_{\geqslant 0}$ such that $n,m\geqslant N\Rightarrow|\xi_n-\xi_m|<\frac{\varepsilon}{3}$. We can assume that $\frac{1}{N+1}<\frac{\varepsilon}{3}$: then $|x_n-x_m|=|\iota(x_n)-\iota(x_m)|\leqslant|\xi_n-\iota(x_n)|+|\xi_n-\xi_m|+|\xi_m-\iota(x_m)|<\varepsilon$: the sequence $\underline{x}:=(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ is Cauchy in K. Put $\ell=\pi(\underline{x})\in\widehat{K}$: we have $|\xi_n-\ell|\leqslant|\xi_n-\iota(x_n)|+|\iota(x_n)-\ell|\xrightarrow[n\to\infty]{}0$. □

Definition 3.3.4. The valued field $(\widehat{K},|.|)$ has the following universal property: if $(L,|.|_L)$ is a complete valued field and $f\colon K\to L$ a morphism of valued fields, there exists a unique morphism of valued fields $\widehat{f}\colon\widehat{K}\to L$ such that $f=\widehat{f}\circ\iota$. In particular, the valued field $(\widehat{K},|.|)$ is unique up to unique isomorphism. It is called the *completion* of $(K,|.|)$.

Remark 3.3.5. The completion of $\mathbf{Q}$ with respect to the "usual" absolute value $|.|_\infty$ is nothing but $\mathbf{R}$ (this is in fact the very definition of $\mathbf{R}$). Note that the proof of proposition 3.3.3 uses $\mathbf{R}$ (essentially to define the absolute value on $\widehat{K}$), so rigorously, one has to build the ordered field $\mathbf{R}$ first.

Definition 3.3.6. Let p be a prime integer. The completion of $\mathbf{Q}$ with respect to the p-adic absolute value is denoted by $\mathbf{Q}_p$. It is called the field of *p-adic numbers.*

Lemma 3.3.7. Let A be a ring, $\alpha\in A$ and $\widehat{A}=\varprojlim\limits_n A/\alpha^nA$ its α-adic completion. Then $\widehat{A}$ is separated and complete for the α-adic topology.

Proof. For all integers $0<n\leqslant m$, the sequence $0\to K_n\to A\xrightarrow{\alpha^n}\alpha^nA\to 0$ is exact: tensoring by A/α^mA gives the exact sequence $K_n\otimes_A(A/\alpha^mA)\to A/\alpha^mA\xrightarrow{\alpha^n}\alpha^nA\otimes_A(A/\alpha^mA)\to 0$. By right exactness of the tensor product, the maps $K_n\otimes_A(A/\alpha^{m+1}A)\to K_n\otimes_A(A/\alpha^mA)$ are surjective, so that the inverse system $\{K_n\otimes_A(A/\alpha^mA)\}_{m\in\mathbf{Z}_{>0}}$ has the Mittag-Leffler property. This implies that the map $\widehat{A}\xrightarrow{\alpha^n}\widehat{\alpha^nA}=\varprojlim\limits_m\alpha^nA\otimes_A(A/\alpha^mA)$ is surjective.

On the other hand, the sequence $0\to\alpha^nA/\alpha^mA\to A/\alpha^mA\to A/\alpha^nA\to 0$ is exact for all $m\geqslant n$. The inverse system $\{\alpha^nA/\alpha^mA\}_{m\geqslant n}$ has the Mittag-Leffler property: the sequence $0\to\widehat{\alpha^nA}\to\widehat{A}\to A/\alpha^nA\to 0$ is exact.

Put together, this provides an exact sequence $\widehat{A}\xrightarrow{\alpha^n}\widehat{A}\to A/\alpha^nA\to 0$, so that $A/\alpha^nA\xrightarrow{\sim}\widehat{A}/\alpha^n\widehat{A}$: passing to inverse limit gives an isomorphism $\widehat{A}\xrightarrow{\sim}\widehat{\widehat{A}}$, whence the result. □

Proposition 3.3.8. (Algebraic construction of the completion in the non archimedean case). Assume $|.|$ is a non archimedean valuation on K, and let v be an associated valuation. Let $\alpha\in\mathfrak{m}_{K,v}\backslash\{0\}$, and $\widehat{\mathcal{O}}_{K,v}$ be the α-adic completion of $\mathcal{O}_{K,v}$. Then $\mathcal{O}_{\widehat{K},v}\simeq\widehat{\mathcal{O}}_{K,v}$ and $\widehat{K}\simeq\widehat{\mathcal{O}}_{K,v}[\alpha^{-1}]$.

Proof. • Let $x=(x_n)_{n\in\mathbf{Z}_{>0}}\in\widehat{\mathcal{O}}_{K,v}=\varprojlim_n\mathcal{O}_{K,v}/\alpha^n\mathcal{O}_{K,v}$. For each $n\in\mathbf{Z}_{>0}$, let $\widetilde{x}_n\in\mathcal{O}_{K,v}$ be a lift of x_n. Assume that $x\neq 0$: there exist $N\in\mathbf{Z}_{>0}$ such that $\widetilde{x}_N\notin\alpha^N\mathcal{O}_{K,v}$. If $n\geqslant N$, we have $\widetilde{x}_n-\widetilde{x}_N\in\alpha^N\mathcal{O}_{K,v}$, so that $v(\widetilde{x}_n)=v(\widetilde{x}_N)$ (*cf* remark 3.2.2). This implies that $v(\widetilde{x}_n)$ does not depend on n large enough. Likewise, $v(\widetilde{x}_n)$ does not depend on the choice of the lifting when n is large enough. This implies that the map $v\colon\widehat{\mathcal{O}}_{K,v}\to\mathbf{R}_{\geqslant 0}\cup\{\infty\}$ defined by $x\mapsto\lim\limits_{n\to\infty}v(\widetilde{x}_n)$ is well defined. The valuation properties extend to v on $\widehat{\mathcal{O}}_{K,v}$. Condition (2) imply in particular that $\widehat{\mathcal{O}}_{K,v}$ is an integral domain.

• Let $x\in\widehat{\mathcal{O}}_{K,v}\backslash\{0\}$: we have $v(x)\in\mathbf{R}_{\geqslant 0}$. Let $m\in\mathbf{Z}_{\geqslant 0}$ large enough such that $v(x)<mv(\alpha)$. Using previous notations, we may assume that $v(\widetilde{x}_n)<mv(\alpha)$ for all $n\geqslant m$. By proposition 3.2.4, we have $\widetilde{x}_{m+1}\mid\alpha^m$ in $\mathcal{O}_{K,v}$: let $y\in\mathcal{O}_{K,v}$ be such that $\widetilde{x}_{m+1}y=\alpha^m$. This implies that $xy\in\alpha^m+\alpha^{m+1}\widehat{\mathcal{O}}_{K,v}$: there exists $z\in\widehat{\mathcal{O}}_{K,v}$ such that $xy=\alpha^m(1-\alpha z)$. As $1-\alpha z$ is invertible in $\widehat{\mathcal{O}}_{K,v}$ (the series $\sum\limits_{n=0}^{\infty}(\alpha z)^n$ converges), we deduce that $x\mid\alpha^m$ in $\widehat{\mathcal{O}}_{K,v}$, which implies that x is invertible in $\widehat{\mathcal{O}}_{K,v}[\alpha^{-1}]$, which thus is the field of fractions of $\widehat{\mathcal{O}}_{K,v}$.

• The valuation v extends uniquely to $\widehat{\mathcal{O}}_{K,v}[\alpha^{-1}]$. The natural map $\mathcal{O}_{K,v}\to\widehat{\mathcal{O}}_{K,v}$ localizes into a morphism of valued fields $K\to\widehat{\mathcal{O}}_{K,v}[\alpha^{-1}]$. If $x\in\widehat{\mathcal{O}}_{K,v}[\alpha^{-1}]$, there exists $m\in\mathbf{Z}_{\geqslant 0}$ such that $\alpha^mx\in\widehat{\mathcal{O}}_{K,v}$: if $N\in\mathbf{Z}_{\geqslant 0}$, we can choose $y\in\mathcal{O}_{K,v}$ such that $v(\alpha^mx-y)\geqslant N+m$, so that $v(x-\alpha^{-m}y)\geqslant N$. As $\alpha^{-m}y\in K$, this shows that the image of K in $\widehat{\mathcal{O}}_{K,v}[\alpha^{-1}]$ is dense.

• Let $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ be a Cauchy sequence in $\widehat{\mathcal{O}}_{K,v}[\alpha^{-1}]$. It is bounded: there exists $m\in\mathbf{Z}_{\geqslant 0}$ such that $\alpha^mx_n\in\widehat{\mathcal{O}}_{K,v}$ for all $n\in\mathbf{Z}_{\geqslant 0}$. The ring $\widehat{\mathcal{O}}_{K,v}$ is complete for the α-adic topology (*cf* lemma 3.3.7), hence for the topology defined by v (*cf* remark 3.2.12 (2)). This implies that $(\alpha^mx_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ is convergent in $\widehat{\mathcal{O}}_{K,v}$, so that $\widehat{\mathcal{O}}_{K,v}[\alpha^{-1}]$ is complete for v. By the universal property, we have $\widehat{K}\simeq\widehat{\mathcal{O}}_{K,v}[\alpha^{-1}]$. Henceforth, we identify them and write abusively $\widehat{K}=\widehat{\mathcal{O}}_{K,v}[\alpha^{-1}]$.

• We certainly have $\widehat{\mathcal{O}}_{K,v}\subset\mathcal{O}_{\widehat{K},v}$. Let $x\in\mathcal{O}_{\widehat{K},v}$. Fix $m\in\mathbf{Z}_{\geqslant 0}$ such that $y=\alpha^mx\in\widehat{\mathcal{O}}_{K,v}$: we have $v(y)=mv(\alpha)+v(x)\geqslant mv(\alpha)$. By proposition 3.2.4 applied to the valuation ring $\widehat{\mathcal{O}}_{K,v}$, we know that $\alpha^m\mid y$ in $\widehat{\mathcal{O}}_{K,v}$, which means that $x\in\widehat{\mathcal{O}}_{K,v}$, showing the equality $\mathcal{O}_{\widehat{K},v}=\widehat{\mathcal{O}}_{K,v}$. □

Example 3.3.9. Algebraic construction of $\mathbf{Q}_p$. The ring of integers of $\mathbf{Q}$ with respect to the p-adic valuation is $\mathbf{Z}_{(p)}$, the localization of $\mathbf{Z}$ at the prime ideal $p\mathbf{Z}$. Then $\mathbf{Q}_p=\mathbf{Z}_p[p^{-1}]$ where

$$\mathbf{Z}_p=\varprojlim_n\mathbf{Z}_{(p)}/p^n\mathbf{Z}_{(p)}\xleftarrow{\sim}\varprojlim_n\mathbf{Z}/p^n\mathbf{Z}$$

The ring of integers $\mathbf{Z}_p$ is called the *ring of p-adic integers*.

Theorem 3.3.10. (Newton's lemma). Assume that $(K,|.|)$ is a complete non archimedean valued field with ring of integers $\mathcal{O}_K$. Let $P\in\mathcal{O}_K[X]$ and $\alpha\in\mathcal{O}_K$. Assume that there exists $\varepsilon\in[0,1[$ such that

$$|P(\alpha)|\leqslant\varepsilon\,|P'(\alpha)|^2.$$

Then there exists a unique $\widetilde{\alpha}\in\mathcal{O}_K$ such that $P(\widetilde{\alpha})=0$ and $|\widetilde{\alpha}-\alpha|\leqslant\varepsilon\,|P'(\alpha)|$.

Proof. • If $P(\alpha)=0$, we take $\widetilde{\alpha}=\alpha$: assume that $P(\alpha)\neq 0$, the hypothesis imply that $P'(\alpha)\neq 0$. We have $P(\alpha+X)=P(\alpha)+P'(\alpha)X+P^{[2]}(\alpha)X^2+\cdots+P^{[n]}(\alpha)X^n$ where $n=\deg(P)$ (here $P^{[i]}$ is the divided i-th derivative, which formally is $\frac{1}{i!}P^{(i)}$: it is $\binom{n}{i}X^{n-i}\in\mathbf{Z}[X]$ when $P=X^n$, so $P^{[i]}\in\mathcal{O}_K[X]$). Put $x_1=-\frac{P(\alpha)}{P'(\alpha)}\in K$. We have $|x_1|=\frac{|P(\alpha)|}{|P'(\alpha)|}\leqslant\varepsilon\,|P'(\alpha)|\leqslant\varepsilon<1$ (since $P'\in\mathcal{O}_K$, whence $P'(\alpha)\in\mathcal{O}_K$). This implies that $x_1\in\mathcal{O}_K$, so $\alpha_1=\alpha+x_1\in\mathcal{O}_K$. Moreover, we have

$$P(\alpha_1)=P^{[2]}(\alpha)x_1^2+\cdots+P^{[n]}(\alpha)x_1^n$$

so that $|P(\alpha_1)| \leqslant \max\limits_{2\leqslant i\leqslant n}\{|P^{[i]}(\alpha)|\,|x_1|^i\}$. As $|P^{[i]}(\alpha)| \leqslant 1$ (because $P^{[i]}(\alpha)\in\mathcal{O}_K$) and $|x_1|\leqslant 1$, we deduce that $|P(\alpha_1)| \leqslant |x_1|^2 \leqslant \varepsilon^2\,|P'(\alpha)|^2$. Note also that

$$P'(\alpha_1) = P'(\alpha) + P^{(2)}(\alpha)x_1 + \cdots + (P')^{[n-1]}(\alpha)x_1^{n-1}$$

so that $|P'(\alpha_1) - P'(\alpha)| \leqslant |x_1| \leqslant \varepsilon\,|P'(\alpha)|$: as $\varepsilon\in[0,1[$, this implies that $|P'(\alpha_1)| = |P'(\alpha)|$.
What precedes show that we can construct inductively a sequence $(\alpha_m)_{m\in\mathbf{Z}_{\geqslant 0}}$ of elements in $\mathcal{O}_K$ such that $\alpha_0=\alpha$, $|P(\alpha_m)| \leqslant \varepsilon^{2^m}\,|P'(\alpha)|^2$, $|\alpha_{m+1}-\alpha_m| \leqslant \varepsilon^{2^m}\,|P'(\alpha)|$ (and $\alpha_{m+1}=\alpha_m$ if $P(\alpha_m)=0$) for all $m\in\mathbf{Z}$. By construction, the sequence $(\alpha_m)_{m\in\mathbf{Z}_{\geqslant 0}}$ is Cauchy, hence converges to a limit $\widetilde{\alpha}\in\mathcal{O}_K$ (since K is complete). Passing to the limit we have $P(\widetilde{\alpha})=0$ and $|\widetilde{\alpha}-\alpha| \leqslant \varepsilon\,|P'(\alpha)|$.

- The unicity of $\widetilde{\alpha}$ is obvious if $P'(\alpha)=0$ (we must have $\widetilde{\alpha}=\alpha$): assume that $P'(\alpha)\neq 0$. Let $\widetilde{\alpha}'\in\mathcal{O}_K$ be such that $P(\widetilde{\alpha}')=0$ and $|\widetilde{\alpha}'-\alpha| \leqslant \varepsilon\,|P'(\alpha)|$. What precedes shows that $|P'(\widetilde{\alpha})| = |P'(\alpha)|$. We have $0 = P(\widetilde{\alpha}')-P(\widetilde{\alpha}) = \sum\limits_{i=1}^{n} P^{[i]}(\widetilde{\alpha})(\widetilde{\alpha}'-\widetilde{\alpha})^i$. Assume that $\widetilde{\alpha}'\neq\widetilde{\alpha}$: dividing the preceding equality by $\widetilde{\alpha}'-\widetilde{\alpha}$ gives $-P'(\widetilde{\alpha}) = \sum\limits_{i=1}^{n} P^{[i]}(\widetilde{\alpha})(\widetilde{\alpha}'-\widetilde{\alpha})^{i-1}$, so that $|P'(\widetilde{\alpha})| \leqslant \max\limits_{2\leqslant i\leqslant n} |P^{[i]}(\widetilde{\alpha})|\,|\widetilde{\alpha}'-\widetilde{\alpha}|^{i-1}$. As $P\in\mathcal{O}_K[X]$ and $\widetilde{\alpha}\in\mathcal{O}_K$, we have $|P^{[i]}(\widetilde{\alpha})| \leqslant 1$, and as $\widetilde{\alpha}',\widetilde{\alpha}\in\mathcal{O}_K$, we have $|\widetilde{\alpha}'-\widetilde{\alpha}|\leqslant 1$. This implies that $|P'(\widetilde{\alpha})| \leqslant |\widetilde{\alpha}'-\widetilde{\alpha}|$, contradicting the inequalities $|\widetilde{\alpha}'-\widetilde{\alpha}| \leqslant \max\{|\widetilde{\alpha}'-\alpha|, |\widetilde{\alpha}-\alpha|\} \leqslant \varepsilon\,|P'(\widetilde{\alpha})|$ and $\varepsilon<1$. □

Remark 3.3.11. The convergence of the sequence $(\alpha_m)_{m\in\mathbf{Z}_{\geqslant 0}}$ is quadratic.

Example 3.3.12. (Roots of unity in $\mathbf{Q}_p$). Let p be a prime number. If $\alpha\in K$ is a root of unity: assume $\alpha^d=1$ with $d\in\mathbf{Z}_{>1}$. We have $|\alpha|^d=1$, so $|\alpha|=1$ *i.e.* $\alpha\in\mathbf{Z}_p^\times$. Let $\overline{\alpha}$ be the image of α in $\mathbf{F}_p=\mathbf{Z}_p/p\,\mathbf{Z}_p$.

- Assume that $d=p$. As $\overline{\alpha}^p=\overline{\alpha}$, we have $\overline{\alpha}=1$, *i.e.* $\alpha=1+x$ with $x\in p\,\mathbf{Z}_p$. Then $1=\alpha^p=(1+x)^p=1+px+\sum\limits_{i=2}^{p-1}\binom{p}{i}x^i+x^p$. If $x\neq 0$, this implies that $p+\sum\limits_{i=2}^{p-1}\binom{p}{i}x^{i-1}+x^{p-1}=0$: as $v_p\big(\binom{p}{i}x\big)\geqslant 2$ (since $p\mid\binom{p}{i}$), we have $v_p(x^{p-1})=1$, thus $p=2$ and $\alpha\in\{\pm1\}$. This shows that if $p\neq 2$, we have $\alpha=1$.
- Assume $d=4$ and $p=2$. We have $\alpha^2\in\{\pm1\}$ by what precedes. If we had $\alpha^2=-1$, this would imply that $(1+\alpha)^2=2\alpha$, hence $2v_2(1+\alpha)=1$ (because $v_2(\alpha)=0$), so that $v_2(1+\alpha)=\frac{1}{2}\notin\mathbf{Z}$, which is absurd. This shows that $\alpha^2=1$. More generally, if $\alpha^{2^r}=1$ with $r\in\mathbf{Z}_{>0}$, then $\alpha=\{\pm1\}$.
- Assume that $p\nmid d$. As $\overline{\alpha}\neq 0$, we have $\overline{\alpha}^{p-1}=1$, so that $\alpha^{p-1}=1+x$ for some $x\in p\,\mathbf{Z}_p$. Here again we have $1=\alpha^{(p-1)d}=1+dx+\sum\limits_{i=2}^{p-1}\binom{d}{i}x^i+x^d$. If $x\neq 0$, this implies that $d+\sum\limits_{i=2}^{p-1}\binom{d}{i}x^{i-1}+x^{d-1}=0$: this is a contradiction since $p\mid\sum\limits_{i=2}^{p-1}\binom{d}{i}x^{i-1}+x^{d-1}$. So we must have $x=0$, *i.e.* $\alpha^{p-1}=1$.
- What precedes imply that $\alpha^2=1$ if $p=2$ and $\alpha^{p-1}=1$ if $p\neq 2$. Conversely, let's show that roots of unity in $\mathbf{Q}_p$ are $\{\pm1\}$ if $p=2$ and μ_{p-1} if $p\neq 2$. This is trivial if $p=2$: assume that $p\neq 2$. Consider the polynomial $P=X^{p-1}-1$. It splits with simple roots in $\mathbf{F}_p$. For any $\alpha\in\mathbf{Z}_p$ lifting an element of $\mathbf{F}_p^\times$, we have $P'(\alpha)=(p-1)\alpha^{p-2}\in\mathbf{Z}_p^\times$, so that $|P'(\alpha)|_p=1$, whereas $|P(\alpha)|_p\leqslant\frac{1}{p}$. Newton's lemma applies (with $\varepsilon=\frac{1}{p}$): there exists a root $\widetilde{\alpha}\in\mathbf{Z}_p$ of P such that $|\widetilde{\alpha}-\alpha|<1$, so that $\widetilde{\alpha}$ and α have same reduction mod p. This means that the $p-1$ elements in $\mathbf{F}_p^\times$ can be lifted by $p-1$ roots of unity.

3.4. **Normed vector spaces.** Let $(K,|.|)$ be a valued field.

Definition 3.4.1. • Let V be a K-vector space. A *norm* on V is a map

$$\|.\|: V\to\mathbf{R}_{\geqslant 0}$$

such that

(1) $(\forall v\in V)\ \|v\|=0\Leftrightarrow v=0$ (separation);
(2) $(\forall\lambda\in K)\,(\forall v\in V)\ \|\lambda v\|=|\lambda|\,\|v\|$ (multiplicativity);
(3) $(\forall v_1,v_2\in V)\ \|v_1+v_2\|\leqslant\|v_1\|+\|v_2\|$ (triangle inequality).

When $(K,|.|)$ is not archimedean, we require the stronger:

(3') $(\forall v_1,v_2\in V)\ \|v_1+v_2\|\leqslant\max\{\|v_1\|,\|v_2\|\}$ (strong triangle inequality),

The pair $(V,\|.\|)$ is then called a *normed vector space.*

- A *normed K-algebra* is a K-algebra A endowed with a norm $\|.\|$ such that:

(4) $(\forall a,b\in A)\ \|ab\|\leqslant\|a\|\,\|b\|$.

Example 3.4.2. (1) If $(L,|.|)$ is a valued field and $K\subset L$ a subfield, endowed with the restriction of $|.|$, then the absolute value $|.|$ endows L with a normed vector space (even a normed K-algebra) structure.

(2) Let X be a set and $\mathscr{B}(X,K)$ the space of *bounded* maps on X with values in K. If $f \in \mathscr{B}(X,K)$, put $\|f\|_\infty = \sup\limits_{x\in X} |f(x)|$. Then $(\mathscr{B}(X,K), \|.\|_\infty)$ is a normed vector space over K.
As a special case, $\mathbf{x} = (x_1,\dots,x_n) \mapsto \|\mathbf{x}\|_\infty = \max\limits_{1\leqslant i\leqslant n} |x_i|$ is a norm on K^n.

(3) Let $\ell^1(K) = \Big\{\mathbf{x} = (x_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in K^{\mathbf{Z}_{\geqslant 0}}\,;\, \sum\limits_{n=0}^{\infty} |x_n| < +\infty\Big\}$. For $\mathbf{x} = (x_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in \ell^1(K)$, we put $\|\mathbf{x}\|_1 = \sum\limits_{n=0}^{\infty} |x_n|$. The map $\|.\|_1$ satisfies conditions (1), (2) and (3) of definition 3.4.1, but not condition (3') (even when $(K, |.|)$ is non archimedean). Thus $(\ell^1(K), \|.\|_1)$ is a normed vector space over K when K is archimedean, but not when $(K, |.|)$ is non archimedean.

Definition 3.4.3. Let $(V, \|.\|)$ be a normed K-vector space. Then the open balls $\mathsf{B}(v,r)$ (with $v \in V$ and $r \in \mathbf{R}_{>0}$) form a basis for a topology on V. In what follows, V will always be endowed with this topology. Assuming that K is complete, we say that $(V, \|.\|)$ is a *Banach* space when $(V, \|.\|)$ is complete.

Proposition 3.4.4. If $(K, |.|)$ is complete, then $(\mathscr{B}(X,K), \|.\|_\infty)$ is.

Proof. Let $(f_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ be a Cauchy sequence in $(\mathscr{B}(X,K), \|.\|_\infty)$: for $x \in X$, the sequence $(f_n(x))_{n\in\mathbf{Z}_{\geqslant 0}}$ is Cauchy in K, hence converges to a limit $f(x) \in K$. Let $\varepsilon \in \mathbf{R}_{>0}$: there exists $N \in \mathbf{Z}_{\geqslant 0}$ such that $N \leqslant n \leqslant m \Rightarrow \|f_n - f_m\|_\infty < \varepsilon$. For $x \in X$, we have $|f(x) - f_n(x)| \leqslant |f(x) - f_m(x)| + |f_m(x) - f_n(x)| < |f(x) - f_m(x)| + \varepsilon$. Passing to the limit as $m \to \infty$, we get $|f(x) - f_n(x)| \leqslant \varepsilon$. As this holds for all $x \in X$, we thus have $\|f - f_n\|_\infty \leqslant \varepsilon$ as soon as $n \geqslant N$. This shows that $f \in \mathscr{B}(X,K)$, and also that $(f_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ converges to f for $\|.\|_\infty$. □

Example 3.4.5. The space $(K^n, \|.\|_\infty)$ is complete.

Definition 3.4.6. Let V be a K-vector space. Two norms $\|.\|, \|.\|'$ on V are *equivalent* when they define the same topology on V.

Form now on, we assume that the absolute value $|.|$ is *non trivial.*

Proposition 3.4.7. Two norms $\|.\|, \|.\|'$ on V are equivalent if and only if there exist constants $c_1, c_2 \in \mathbf{R}_{>0}$ such that

$$(\forall v \in V)\; c_1 \|v\| \leqslant \|v\|' \leqslant c_2 \|v\|$$

Proof. Assume $\|.\|, \|.\|'$ are equivalent. The ball $\mathsf{B}(0,1)$ is open for the topology defined by $\|.\|'$: there exists $r \in \mathbf{R}_{>0}$ such that $\mathsf{B}(0,r)' \subset \overline{\mathsf{B}}(0,1)$. Let $\pi \in K$ be such that[31] $0 < |\pi| < 1$. If $v \in V\backslash\{0\}$ there exists $n \in \mathbf{Z}$ such that $|\pi|\, r \leqslant |\pi|^n \|v\|' < r$. Then we have $|\pi|^n \|v\| = \|\pi^n v\| \leqslant 1$, *i.e.* $\frac{|\pi| r}{\|v\|'} \|v\| \leqslant 1$, so that $c_1 \|v\| \leqslant \|v\|'$ with $c_1 = |\pi|\, r$. This also holds when $v = 0$. Similarly, there exists $c_2 \in \mathbf{R}_{>0}$ such that $\|v\|' \leqslant c_2 \|v\|$ for all $v \in V$. The converse is obvious. □

Remark 3.4.8. Assume that $|.|$ is the trivial absolute value, and let V be a K-vector space. If $\|.\|$ and $\|.\|'$ are two equivalent norms on V, there might not exist constants $c_1, c_2 \in \mathbf{R}_{>0}$ as in the previous statement. For instance, if $V = K[\![X]\!]$, and $\rho \in]0,1[$, let $\|.\|_\rho$ be the norm on V defined by $\|f\|_\rho = \rho^{\mathsf{ord}(f)}$ where $\mathsf{ord}(f) = \inf\{n \in \mathbf{Z}_{\geqslant 0}\,;\, a_n \neq 0\}$ (this corresponds to the X-adic norm, with $\|X\|_\rho = \rho$). If $r \in]0,1[$, there exists $t \in \mathbf{R}_{>0}$ such that $r = \rho^t$, so that $\|.\|_r = \|.\|_\rho^t$, so that the norms $\|.\|_r$ and $\|.\|_\rho$ define the same balls hence the same topology: they are equivalent. Assume $r > \rho$, and that we have $c \in \mathbf{R}_{>0}$ such that $\|.\|_r \leqslant c\|.\|_\rho$: applied to X^n, this gives $r^n \leqslant c\rho^n$, *i.e.* $\left(\frac{r}{\rho}\right)^n \leqslant c$: this is a contradiction.
Nevertheless, proposition 3.4.7 is still valid when $|.|$ is trivial if V has finite dimension: let $(e_1,\dots,e_d)$ be a basis of V over K and $\|.\|$ a norm on V. If $v = \sum\limits_{i=1}^{d} \lambda_i e_i \in V$, we have $\|v\| \leqslant \sum\limits_{i=1}^{d} |\lambda_i| \|e_i\| \leqslant c_2 := \sum\limits_{i=1}^{d} \|e_i\|$. On the other hand, for $n \in \mathbf{Z}_{>0}$, let V_n be the span of vectors $v \in V$ such that $\|v\| < \frac{1}{n}$. The sequence of sub-spaces $(V_n)_{n\in\mathbf{Z}_{>0}}$ is decreasing: V being finite dimensional, there exists $N \in \mathbf{Z}_{>0}$ such that $V_n = V_N$ for all $n \geqslant N$. If $v \in V_N$ and $n \geqslant N$, then v can be written as a linear combination of elements in V_n: the previous computation implies that $\|v\| \leqslant \frac{d}{n}$. As n is arbitrary, we have $\|v\| = 0$, hence $V_N = \{0\}$: this implies that if $v \neq 0$, then $c_1 := \frac{1}{N} \leqslant \|v\| \leqslant c_2$.

Proposition 3.4.9. Let $(V, \|.\|_V)$ and $(W, \|.\|_W)$ be normed vector spaces over $(K, |.|)$, and $\varphi \in \mathsf{Hom}_K(V,W)$. The following are equivalent:
(1) φ is continuous;
(2) φ is continuous at 0;
(3) there exists $c \in \mathbf{R}_{\geqslant 0}$ such that $(\forall v \in V)\ \|\varphi(v)\|_W \leqslant c\,\|v\|_V$.

[31] Recall that $|.|$ is not trivial.

Proof. (1)$\Leftrightarrow$(2) and (3)$\Rightarrow$(2) are obvious.
Assume (2): there exists $r \in \mathbf{R}_{>0}$ such that $\varphi(\mathsf{B}(0,r)_V) \subset \mathsf{B}(0,1)_W$, thus $\varphi(\mathsf{B}(0,1)_V) \subset \mathsf{B}\left(0,\frac{1}{r}\right)_W$. Let $v \in V\backslash\{0\}$. There exists $n \in \mathbf{Z}$ such that $|\pi| \leqslant |\pi|^n \|v\|_V < 1$, so that $\|\varphi(\pi^n v)\|_W < \frac{1}{r}$, *i.e.* $\|\varphi(v)\|_W \leqslant c\|v\|_V$ with $c = \frac{1}{|\pi| r}$. This also holds when $v = 0$. □

Definition 3.4.10. We denote by $\mathsf{Hom}_{K,\mathrm{cont}}(V,W)$ the set of elements in $\mathsf{Hom}_K(V,W)$ that are continuous. If $\varphi \in \mathsf{Hom}_{K,\mathrm{cont}}(V,W)$, we put

$$|\!|\!|\varphi|\!|\!| = \sup_{v \in V\backslash\{0\}} \frac{\|\varphi(v)\|_W}{\|v\|_V} \in \mathbf{R}_{\geqslant 0}\,.$$

This is the smallest constant $c \in \mathbf{R}_{\geqslant 0}$ such that $(\forall v \in V)\ \|\varphi(v)\|_W \leqslant c\|v\|_V$.

Proposition 3.4.11. If $(V,\|.\|_V)$ and $(W,\|.\|_W)$ be normed vector spaces over $(K,|.|)$, then $\mathsf{Hom}_{K,\mathrm{cont}}(V,W)$ is a sub-K-vector space of $\mathsf{Hom}_K(V,W)$. The map $|\!|\!|.|\!|\!| : \mathsf{Hom}_{K,\mathrm{cont}}(V,W) \to \mathbf{R}_{\geqslant 0}$ is a norm. Finally $(\mathsf{Hom}_{K,\mathrm{cont}}(V,W), |\!|\!|.|\!|\!|)$ is a Banach space when $(W,\|.\|_W)$ is.

Proof. The first point is obvious. We certainly have $|\!|\!|\varphi|\!|\!| = 0 \Rightarrow \varphi = 0$, and $|\!|\!|\lambda\varphi|\!|\!| = |\lambda|\,|\!|\!|\varphi|\!|\!|$ for all $\lambda \in K$. If $\varphi,\psi \in \mathsf{Hom}_{K,\mathrm{cont}}(V,W)$ and $v \in V$, we have

$$\|(\varphi+\psi)(v)\|_W \leqslant \|\varphi(v)\|_W + \|\psi(v)\|_W \leqslant |\!|\!|\varphi|\!|\!|\,\|v\|_V + |\!|\!|\psi|\!|\!|\,\|v\|_V \text{ when } (K,|.|) \text{ is archimedean,}$$
$$\|(\varphi+\psi)(v)\|_W \leqslant \max\{\|\varphi(v)\|_W, \|\psi(v)\|_W\} \leqslant \max\{|\!|\!|\varphi|\!|\!|\,\|v\|_V, |\!|\!|\psi|\!|\!|\,\|v\|_V\} \text{ otherwise,}$$

which implies that $|\!|\!|\varphi+\psi|\!|\!| \leqslant |\!|\!|\varphi|\!|\!| + |\!|\!|\psi|\!|\!|$ if $(K,|.|)$ is archimedean and $|\!|\!|\varphi+\psi|\!|\!| \leqslant \max\{|\!|\!|\varphi|\!|\!|, |\!|\!|\psi|\!|\!|\}$ otherwise.
Assume now that $(W,\|.\|_W)$ is complete, and let $(\varphi_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ be a Cauchy sequence in $(\mathsf{Hom}_{K,\mathrm{cont}}(V,W), |\!|\!|.|\!|\!|)$. If $v \in V$, then $\|\varphi_n(v) - \varphi_m(v)\|_W \leqslant |\!|\!|\varphi_n - \varphi_m|\!|\!|\,\|v\|_V$ for all $n,m \in \mathbf{Z}_{\geqslant 0}$, so that the sequence $(\varphi_n(v))_{n\in\mathbf{Z}_{\geqslant 0}}$ is Cauchy in $(V,\|.\|_W)$: it converges to a limit $\varphi(v) \in W$. The linearity of the maps φ_n imply that of φ. Moreover, a Cauchy sequence is bounded: there exists $C \in \mathbf{R}_{\geqslant 0}$ such that $(\forall n \in \mathbf{Z}_{\geqslant 0})\ |\!|\!|\varphi_n|\!|\!| \leqslant C$, so that for any $v \in V$, we have $\|\varphi_n(v)\|_W \leqslant C\|v\|_V$, thus $\|\varphi(v)\|_W \leqslant C\|v\|_V + \|\varphi(v) - \varphi_n(v)\|_W$, whence $\|\varphi(v)\|_W \leqslant C\|v\|_V$ (passing to the limit as $n \to \infty$). This shows that $\varphi \in \mathsf{Hom}_{K,\mathrm{cont}}(V,W)$.
Let $\varepsilon \in \mathbf{R}_{>0}$: there exists $N \in \mathbf{Z}_{\geqslant 0}$ such that $N \leqslant n \leqslant m \Rightarrow |\!|\!|\varphi_n - \varphi_m|\!|\!| < \varepsilon$. If $v \in V$, we have $\|\varphi(v) - \varphi_n(v)\|_W \leqslant \|\varphi(v) - \varphi_m(v)\|_W + \|\varphi_n(v) - \varphi_m(v)\|_W \leqslant \|\varphi(v) - \varphi_m(v)\|_W + \varepsilon\|v\|_V$. This implies that $\|\varphi(v) - \varphi_n(v)\|_W \leqslant \varepsilon\|v\|_V$ (passing to the limit as $m \to \infty$) for all $v \in V$, whence $|\!|\!|\varphi - \varphi_n|\!|\!| \leqslant \varepsilon$. This shows that the sequence $(\varphi_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ converges to φ in $(\mathsf{Hom}_{K,\mathrm{cont}}(V,W), |\!|\!|.|\!|\!|)$. □

Theorem 3.4.12. Assume $(K,|.|)$ is complete. Let $(V,\|.\|)$ be a normed vector space of finite dimension over K, and $\mathfrak{B} = (e_1,\ldots,e_n)$ a basis of V. Then the dual basis $\mathfrak{B}^* = (e_1^*,\ldots,e_n^*)$ is made of *continuous* linear forms. Moreover, all norms on V are equivalent, and V is a Banach space. In particular, sub-K-vector spaces are closed in V.

Proof. We proceed by induction on $n = \dim_K(V)$. This is trivial when $n \in \{0,1\}$: assume $n > 1$. Let $H = \mathsf{Vect}(e_1,\ldots,e_{n-1})$: by induction hypothesis, this is a Banach space when endowed with the restriction of $\|.\|$. Assume that e_n^* is not continuous. This implies that there exists a sequence $(v_i)_{i\in\mathbf{Z}_{\geqslant 0}}$ in V such that $\lim\limits_{i\to\infty} v_i = 0$ but $(e_n^*(v_i))_{i\in\mathbf{Z}_{\geqslant 0}}$ does to converge to 0: after extracting a sub-sequence, we may assume that there exists $\varepsilon \in \mathbf{R}_{>0}$ such that $|e_n^*(v_i)| \geqslant \varepsilon$ for all $i \in \mathbf{Z}_{\geqslant 0}$. For $i \in \mathbf{Z}_{\geqslant 0}$, put $u_i = \frac{v_i}{e_n^*(v_i)}$: we have $e_n^*(u_i) = 1$ *i.e.* $u_i - e_n \in H$, and $\|u_i\| \leqslant \frac{\|v_i\|}{\varepsilon} \xrightarrow[i\to\infty]{} 0$. This implies in particular that the sequence $(u_i - e_n)_{i\in\mathbf{Z}_{\geqslant 0}}$, which has values in H, converges to $-e_n$. But H being complete, this shows that $e_n \in H$, which is absurd. Thus we have shows that e_n^* is continuous. Permuting the elements in $\mathfrak{B}$, we deduce that $e_1^*,\ldots,e_n^*$ are all continuous.
Consider the map $\|.\|_{\mathfrak{B}} : V \to \mathbf{R}_{\geqslant 0}$ given by $\|v\|_{\mathfrak{B}} = \|f(v)\|_\infty$, where $f(v) = (e_1^*(v),\ldots,e_n^*(v)) \in K^n$ for all $v \in V$: this defines a norm $\|.\|_{\mathfrak{B}}$ on V. We have $\|v\| = \left\|\sum\limits_{i=1}^n e_i^*(v)e_i\right\| \leqslant \sum\limits_{i=1}^n |e_i^*(v)|\,\|e_i\| \leqslant c\|v\|_{\mathfrak{B}}$ where $c = \sum\limits_{i=1}^n \|e_i\| \in \mathbf{R}_{>0}$, whence $c_1\|v\| \leqslant \|v\|_{\mathfrak{B}}$ with $c_1 = c^{-1}$ for all $v \in V$. On the other hand, the linear forms $e_1^*,\ldots,e_n^*$, hence f, are continuous: there exists $c_2 \in \mathbf{R}_{\geqslant 0}$ such that $(\forall v \in V)\ \|v\|_{\mathfrak{B}} = \|f(v)\|_\infty \leqslant c_2\|v\|$. This shows that the norms $\|.\|$ and $\|.\|_{\mathfrak{B}}$ are equivalent, so all norms are equivalent to $\|.\|_{\mathfrak{B}}$.
As $f\colon V \to K^n$ is an isometry for the norms $\|.\|_{\mathfrak{B}}$ and $\|.\|_\infty$, and since $(K^n,\|.\|_\infty)$ is a Banach, so in V. □

Remark 3.4.13. Theorem 3.4.12 is not valid without the assumtion of completeness. For instance consider $\mathbf{Q}(\sqrt{2}) \subset \mathbf{R}$ as a $\mathbf{Q}$-vector space, endowed with the restriction $\|.\|$ of the "usual" absolute value $|.|_\infty$, and let $\mathfrak{B} = (1,\sqrt{2})$. Pell's equation $x^2 - 2y^2 = \pm 1$ has infinitely many solutions: one can construct a sequence

$(u_n, v_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ in $\mathbf{Z}^2_{>0}$ such that $\left|u_n - v_n\sqrt{2}\right|_\infty \leqslant \frac{1}{u_n+v_n\sqrt{2}}$ and $u_n, v_n \xrightarrow[n\to\infty]{} +\infty$. This implies that if $x_n = u_n - v_n\sqrt{2} \in \mathbf{Q}(\sqrt{2})$, the sequence $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ converges to 0 in $(\mathbf{Q}(\sqrt{2}), \|.\|)$, whereas the sequences of coordinates $(u_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ and $(v_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ do not. In particular, the norm $x + y\sqrt{2} \mapsto \max\{|x|, |y|\}$ and $\|.\|$ are not equivalent on $\mathbf{Q}(\sqrt{2})$.

3.4.14. *The Hahn-Banach theorem.* What follows is taken from [7]. Assume $(K, |.|)$ is complete and let $(V, \|.\|)$ be a normed K-vector space.

Theorem 3.4.15. Let $W \subset V$ be a closed sub-K-vector space and $x_1, \ldots, x_n \in V$. Then $W + Kx_1 + \cdots + Kx_n$ is a closed sub-K-vector space of V. In particular, every finite dimensional sub-K-vector space of V is closed.

Proof. The second statement follows from the first. By induction, it is enough to show the first statement when $n = 1$: write $x = x_1$. If $x \in W$, there is nothing to do: we may assume that $x \in V\backslash W$. Let $(w_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ and $(\lambda_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ be sequences in W and K respectively, such that $(w_n + \lambda_n x)_{n\in\mathbf{Z}_{\geqslant 0}}$ converges in V. Let $\ell \in V$ be its limit: we have to show that $\ell \in W + Kx$. As W is closed in V, it is enough to show that the sequence $(\lambda_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ converges in K (indeed, if $\lambda \in K$ is its limit, the sequence $(w_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ converges in V, hence in W since W is closed in V: let $w \in W$ be its limit; passing to the limit, we have $\ell = w + \lambda x \in W + Kx$).

- Assume $\ell = 0$, and that the sequence $(\lambda_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ does not converge to 0 in K: there exists $\varepsilon \in \mathbf{R}_{>0}$ and a strictly increasing map $\varphi\colon \mathbf{Z}_{\geqslant 0} \to \mathbf{Z}_{\geqslant 0}$ such that $\left|\lambda_{\varphi(n)}\right| \geqslant \varepsilon$ for all $n \in \mathbf{Z}_{\geqslant 0}$. We have

$$\left\|\lambda_{\varphi(n)}^{-1}(w_{\varphi(n)} + \lambda_{\varphi(n)}x)\right\| = \left|\lambda_{\varphi(n)}\right|^{-1}\left\|w_{\varphi(n)} + \lambda_{\varphi(n)}x\right\| \leqslant \varepsilon^{-1}\left\|w_{\varphi(n)} + \lambda_{\varphi(n)}x\right\|$$

which converges to 0. This implies that $\lim\limits_{n\to\infty} \lambda_{\varphi(n)}^{-1} w_{\varphi(n)} = -x$: as W is closed, this shows that $x \in W$, contradicting the hypothesis. We thus have shown that if $\ell = 0$, then $\lim\limits_{n\to\infty} \lambda_n = 0$.

- General case. For $n \in \mathbf{Z}_{\geqslant 0}$, put $w'_n = w_{n+1} - w_n$ and $\lambda'_n = \lambda_{n+1} - \lambda_n$. As $\lim\limits_{n\to\infty}(w_n + \lambda_n x) = \ell$, we have $\lim\limits_{n\to\infty}(w'_n + \lambda'_n x) = 0$: by the special case treated above, we have $\lim\limits_{n\to\infty} \lambda'_n = 0$. This implies that the sequence $(\lambda_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ is Cauchy, hence converges (since $(K, |.|)$ is complete). □

Theorem 3.4.16. (Hahn-Banach). Assume that $|.|$ is non archimedean and discrete. Let $W \subset V$ be a sub-K-vector space and $\varphi\colon W \to K$ a continuous linear form. Then there exists a continuous linear form $\widetilde{\varphi}\colon V \to K$ such that $\varphi = \widetilde{\varphi}_{|W}$ and $|||\widetilde{\varphi}||| = |||\varphi|||$.

Proof. We of course may assume that $\varphi \neq 0$, so that $M := |||\varphi||| > 0$.

- Case where $|.|$ is trivial. Let $E = \{x \in V\,;\, \|x\| < M^{-1}\}$: as $|.|$ is trivial, this is a sub-K-vector space of V. If $x \in E \cap W$, we have $|\varphi(x)| \leqslant M\|x\| < 1$, hence $\varphi(x) = 0$: the map φ factors through a linear form $\overline{\varphi}\colon W/(W \cap E) \to K$. We can extend $\overline{\varphi}$ into a linear form $\widetilde{\overline{\varphi}}\colon V/E \to K$ (by the axiom of choice). Let $\pi\colon V \to V/E$ be the projection and $\widetilde{\varphi} = \widetilde{\overline{\varphi}} \circ \pi\colon V \to K$: this is a linear form such that $\varphi = \widetilde{\varphi}_{|W}$. If $x \in V\backslash \mathsf{Ker}(\widetilde{\varphi})$, we have $x \notin E$, whence $\|x\| \geqslant M^{-1}$, *i.e.* $|\widetilde{\varphi}(x)| = 1 \leqslant M\|x\|$. As this obviously holds for $x = 0$, we have $|||\widetilde{\varphi}||| = |||\varphi|||$.
- Case where $|.|$ is not trivial. Using Zorn's lemma as usual, we reduce to the case where $V = W + Kx$ with $x \in V\backslash W$. As $(K, |.|)$ is complete, we can extend φ by continuity to the closure of W: we may assume that W is closed. Put $\rho = \inf\left(|K| \cap]1, +\infty[\right)$: as $|.|$ is discrete and non trivial, we have $\rho > 1$, and there exists $\lambda \in K$ such that $|\lambda| = \rho$. Let $d = \inf\limits_{w\in W}\|x - w\|$ be the distance form x to W: as W is closed and $x \notin W$, we have $d > 0$. Let $k \in \mathbf{Z}$ be such that $\rho^{k-1} \leqslant dM < \rho^k$, *i.e.* $M^{-1}\rho^{k-1} \leqslant d < M^{-1}\rho^k$: there exists $w_0 \in W$ such that $\|x - w_0\| < M^{-1}\rho^k$. Replacing x by $x - w_0$, we may assume that $\|x\| < M^{-1}\rho^k$ (and $d \leqslant \|x - w\|$ for all $w \in W$ as before). If $v \in V$, we can write uniquely $v = w + \lambda x$ with $w \in W$ and $\lambda \in K$. Put $\widetilde{\varphi}(v) = \varphi(w)$. This defines a linear form $\widetilde{\varphi}\colon V \to K$ such that $\varphi = \widetilde{\varphi}_{|W}$. Moreover, we have

$$|\widetilde{\varphi}(v)| = |\varphi(w)| \leqslant M\|w\|$$

so that $|\widetilde{\varphi}(v)| \leqslant M\|v\|$ as soon as $\|w\| \leqslant \|v\|$. Assume now that $\|w + \lambda x\| = \|v\| < \|w\|$: this implies that $\lambda \neq 0$ and $\|w\| = \|\lambda x\|$, whence $\left\|\lambda^{-1}w\right\| = \|x\| < M^{-1}\rho^k$, so that $\left|\lambda^{-1}\varphi(w)\right| < \rho^k$. As the absolute value is discrete, this implies that $\left|\lambda^{-1}\varphi(w)\right| \leqslant \rho^{k-1} \leqslant Md$, *i.e.* $|\widetilde{\varphi}(v)| = |\varphi(w)| \leqslant Md|\lambda|$. Now $\lambda^{-1}w \in W$, so $d \leqslant \left\|x + \lambda^{-1}w\right\|$, so $d|\lambda| \leqslant \|\lambda x + w\| = \|v\|$, so we get $|\widetilde{\varphi}(v)| \leqslant M\|v\|$, as required. □

Remark 3.4.17. A counterexample when the absolute value is not discrete. Let V be the set of all power series $v = a_1t^{\alpha_1} + a_2t^{\alpha_2} + \cdots$ where $\alpha_1 < \alpha_2 \cdots$ is a strictly increasing sequence of rational numbers and $a_1, a_2, \ldots \in \mathbf{Q}_p$. Put $\|v\| = e^{-\alpha_1}$. Defining addition and multiplication in the obvious way, V is a field, and $\|.\|$ is an absolute value on V. Let K be the subfield consisting of all elements $a_1t^{\alpha_1} + a_2t^{\alpha_2} + \cdots$ such that $\lim\limits_{i\to\infty}\alpha_i = +\infty$, and denote by $|.|$ the restriction of $\|.\|$ to K. Consider V as a normed K-vector space. K is itself a subspace of V, and $\varphi(\lambda) = \lambda$ (for $\lambda \in K$) defines a linear form on K such that $|||\varphi||| = 1$.

Assume there exists a linear form $\widetilde{\varphi}\colon V \to K$ such that $\|\!|\widetilde{\varphi}|\!\| = 1$. Consider $v = a_1 t^{\alpha_1} + a_2 t^{\alpha_2} + \cdots \in V$ such that $\lim\limits_{i\to\infty} \alpha_i = \alpha$. Write

$$\widetilde{\varphi}(v) = c_1 t^{\gamma_1} + c_2 t^{\gamma_2} + \cdots \in K.$$

As $|\widetilde{\varphi}(v)| \leqslant \|v\|$, we have $\alpha_1 \leqslant \gamma_1$. If we had $\alpha_1 < \gamma_1$, we could write

$$\widetilde{\varphi}(a_2 t^{\alpha_2} + \cdots) = -a_1 t^{\alpha_1} + c_1 t^{\gamma_1} + c_2 t^{\gamma_2} + \cdots$$

so that $|\widetilde{\varphi}(a_2 t^{\alpha_2} + \cdots)| = e^{-\alpha_1} > e^{-\alpha_2} = \|a_2 t^{\alpha_2} + \cdots\|$ (since $\alpha_1 < \alpha_2$), contradicting $\|\!|\widetilde{\varphi}|\!\| = 1$. We thus have $\alpha_1 = \gamma_1$, and

$$\widetilde{\varphi}(a_2 t^{\alpha_2} + \cdots) = (c_1 - a_1) t^{\alpha_1} + c_2 t^{\gamma_2} + \cdots$$

which again implies that $c_1 = a_1$. By induction, one thus shows that $\alpha_i = \gamma_i$ and $a_i = c_i$ for all $i \in \mathbf{Z}_{>0}$, which is impossible since $\lim\limits_{i\to\infty} \alpha_i = \alpha$ and $\lim\limits_{i\to\infty} \gamma_i = +\infty$.

3.5. **Extensions of absolute values.** Let $(K, |.|)$ be a *non archimedean* valued field, and L/K an extension.

Lemma 3.5.1. For $P(X) = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$, put

$$\|P\| = \max_{0 \leqslant i \leqslant n} |a_i| .$$

Then $\|PQ\| = \|P\| \, \|Q\|$ for all $P, Q \in K[X]$. In particular, $\|.\|$ extends into an absolute value on $K(X)$ that extends $|.|$.

Proof. Write $P(X) = \sum\limits_{i=0}^{\infty} a_i X^i$ and $Q(X) = \sum\limits_{j=0}^{\infty} b_j X^j$ with $(a_i)_{i \in \mathbf{Z}_{\geqslant 0}}, (b_j)_{j \in \mathbf{Z}_{\geqslant 0}} \in K^{(\mathbf{Z}_{\geqslant 0})}$. Then we have $P(X)Q(X) = \sum\limits_{n=0}^{\infty} c_n X^n$ with $c_n = \sum\limits_{i=0}^{n} a_i b_{n-i}$, so $|c_n| \leqslant \max\limits_{0 \leqslant i \leqslant n} |a_i b_{n-i}| \leqslant \|P\| \, \|Q\|$: as this holds for all $n \in \mathbf{Z}_{\geqslant 0}$, we get $\|PQ\| \leqslant \|P\| \, \|Q\|$.
Assume now that $PQ \neq 0$, and let $i_0 = \min\{i \in \mathbf{Z}_{\geqslant 0} \, ; |a_i| = \|P\|\}$ and $j_0 = \min\{j \in \mathbf{Z}_{\geqslant 0} \, ; |b_j| = \|Q\|\}$ so that $|a_i| < \|P\|$ if $i < i_0$ and $|b_j| < \|Q\|$ if $j < j_0$. Then $c_{i_0+j_0} = \sum\limits_{\substack{i,j \in \mathbf{Z}_{\geqslant 0} \\ i+j = i_0+j_0}} a_i b_j$. If $i, j \in \mathbf{Z}_{\geqslant 0}$ are such that $i + j = i_0 + j_0$ and $i < i_0$ or $j < j_0$, we have $|a_i b_j| < \|P\| \, \|Q\|$. As $|a_{i_0} b_{j_0}| = \|P\| \, \|Q\|$, we have $|c_{i_0+j_0}| = \|P\| \, \|Q\|$ (because $|.|$ in non archimedean, *cf* remark 3.1.3 (2)). Thus we have $\|PQ\| = \|P\| \, \|Q\|$.
We certainly have $\|P\| = 0 \Rightarrow P = 0$, and $\|P_1 + P_2\| \leqslant \max\{\|P_1\|, \|P_2\|\}$ for all $P_1, P_2 \in K[X]$. Extend $\|.\|$ to $K(X) = \mathsf{Frac}(K[X])$ by putting

$$\left\| \frac{P}{Q} \right\| = \frac{\|P\|}{\|Q\|}$$

for all $P, Q \in K[X]$ with $Q \neq 0$. The multiplicativity proved above implies that $\|.\|$ is multiplicative on $K(X)$. Moreover, if $R \in K(X)$, we have $\|R\| = 0 \Rightarrow R = 0$, and if $R_1, R_2 \in K(X)$, there exists $Q \in K[X] \backslash \{0\}$ such that $P_1 = QR_1, P_2 = QR_2 \in K[X]$: as $\|P_1 + P_2\| \leqslant \max\{\|P_1\|, \|P_2\|\}$, we deduce $\|R_1 + R_2\| \leqslant \max\{\|R_1\|, \|R_2\|\}$, so that $\|.\|$ is an absolute value on $K(X)$, that obviously extends $|.|$. □

Definition 3.5.2. The norm $\|.\|$ on $K[X]$ defined in lemma 3.5.1 is called the *Gauss norm*, and we will henceforth denote by $|.|_{\mathrm{Gauss}}$ the absolute value it induces on $K(X)$.

Theorem 3.5.3. (Krull's existence theorem, *cf* [18, Theorem 14.1][32]). There exists an absolute value on L that extends $|.|$.

Remark 3.5.4. Of course, any extension of $|.|$ to L is non archimedean.

Proof of theorem 3.5.3. This is obvious if $|.|$ is trivial: assume from now on that it is non trivial.
- Case where L/K is finite. Consider the set Σ of maps $\nu\colon L \to \mathbf{R}_{\geqslant 0}$ having the following properties:
  (1) $(\forall \lambda \in K)\, (\forall x \in L)\, \nu(\lambda x) = |\lambda| \, \nu(x)$;
  (2) $(\forall x, y \in L)\, \nu(xy) \leqslant \nu(x)\nu(y)$;
  (3) $\nu(1) = 1$;
  (4) $(\forall x \in L)\, (\forall k \in \mathbf{Z}_{\geqslant 0})\, \nu(x^k) = \nu(x)^k$;
  (5) $(\forall x, y \in L)\, \nu(x + y) \leqslant \max\{\nu(x), \nu(y)\}$.

[32] The sentence "Obviously ρ satisfies properties (2)-(7)" on the last line of [18, p.38] is fishy, because of property (7), which explains why we modified the latter.

Observe that if $\nu \in \Sigma$ and $x \in L^\times$, then $1 = \nu(xx^{-1}) \leqslant \nu(x)\nu(x^{-1})$, so $\nu(x) > 0$, whence $\nu(x) = 0 \Leftrightarrow x = 0$.
⊛ We first show that Σ is non empty. Let $(e_1, \ldots, e_d)$ be a basis of L over K. If $x = \sum\limits_{i=1}^{d} \lambda_i e_i \in L$, put $\|x\|_1 = \max\limits_{1 \leqslant i \leqslant d} |\lambda_i|$. This defines a norm $\|.\|_1 : L \to \mathbf{R}_{\geqslant 0}$. If $x = \sum\limits_{i=1}^{d} \lambda_i e_i \in L$ and $y = \sum\limits_{i=1}^{d} \mu_i e_i \in L$, we have $xy = \sum\limits_{1 \leqslant i,j \leqslant d} \lambda_i \mu_j e_i e_j$, so $\|xy\| \leqslant \max\limits_{1 \leqslant i,j \leqslant d} |\lambda_i \mu_j| \, \|e_i e_j\|$, *i.e.* $\|xy\| \leqslant C \|x\| \, \|y\|$ where $C = \max\limits_{1 \leqslant i,j \leqslant d} \|e_i e_j\| \in \mathbf{R}_{>0}$. If $\|.\|_2 = C \|.\|_1$, then $\|.\|_2$ is a norm on L such that $\|xy\|_2 \leqslant \|x\|_2 \|y\|_2$ for all $x, y \in L$. Now put

$$\nu_0(x) = \limsup_{k \to \infty} \sqrt[k]{\|x^k\|_2}$$

for all $x \in L$. As $\|x^k\|_2 \leqslant \|x\|_2^k$ for all $k \in \mathbf{Z}_{\geqslant 0}$, this definition makes sense, and $0 \leqslant \nu_0(x) \leqslant \|x\|_2$ for all $x \in L$.
Let $x \in L$ and $a = \inf\limits_{k \in \mathbf{Z}_{>0}} \sqrt[k]{\|x^k\|_2}$. If $\varepsilon \in \mathbf{R}_{>0}$, there exists $d \in \mathbf{Z}_{>0}$ such that $\|x^d\|_2 \leqslant (a+\varepsilon)^d$. If $k \in \mathbf{Z}_{>0}$, let $k = q(k)d + r(k)$ with $q(k) \in \mathbf{Z}_{\geqslant 0}$ and $0 \leqslant r(k) < d$ be the euclidean division of k by d: we have $\|x^k\|_2 \leqslant \|x^d\|_2^{q(k)} \|x^{r(k)}\|_2 \leqslant (a+\varepsilon)^{q(k)d} \|x^{r(k)}\|_2$, which implies that $a \leqslant \sqrt[k]{\|x^k\|_2} \leqslant (a+\varepsilon)^{q(k)d/k} b^{1/k}$ where $b = \max\limits_{0 \leqslant r < d} \|x^r\|_2$. As $\lim\limits_{k \to \infty} \frac{q(k)d}{k} = 1$ and $\lim\limits_{k \to \infty} b^{1/k} = 1$, this implies that $\lim\limits_{k \to \infty} \sqrt[k]{\|x^k\|_2} = a$, so that in fact

$$\nu_0(x) = \lim_{k \to \infty} \sqrt[k]{\|x^k\|_2} = \inf_{k \in \mathbf{Z}_{>0}} \sqrt[k]{\|x^k\|_2}.$$

As $\|\lambda x\|_2 = |\lambda| \, \|x\|_2$ for all $\lambda \in K$ and $x \in L$, the map ν_0 satisfies (1). As $\|xy\|_2 \leqslant \|x\|_2 \|y\|_2$ for all $x, y \in L$, it satisfies (2). Moreover $\nu_0(1) = \lim\limits_{k \to \infty} \sqrt[k]{\|1\|_2} = 1$ so ν_0 satisfies (3). Also, $\nu_0(x^k) = \lim\limits_{m \to \infty} \sqrt[m]{\|x^{km}\|_2} = \nu_0(x)^k$ so ν_0 satisfies (4). To prove it satisfies (5), let $x, y \in L^\times$. By symmetry, we may assume that $\nu_0(x) \leqslant \nu_0(y)$. After scaling x and y by some appropriate $\lambda \in K$, we may further assume that $\nu_0(y) > 1$ (recall that $|.|$ is non trivial). Let $\varepsilon \in \mathbf{R}_{>0}$: there exists $N \in \mathbf{Z}_{\geqslant 2}$ such that $i \geqslant N \Rightarrow \|x^i\|_2 \leqslant (\nu_0(x)+\varepsilon)^i \leqslant (\nu_0(y)+\varepsilon)^i$. As $\nu_0(y) > 1$, we may also assume that N is large enough so that $k \geqslant N \Rightarrow 1 \leqslant \|y^k\|_2 \leqslant (\nu_0(y)+\varepsilon)^k$. If $n \in \mathbf{Z}_{\geqslant 0}$, we have

$$\|(x+y)^n\|_2 = \left\| \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \right\|_2 \leqslant \max_{0 \leqslant k \leqslant n} \|x^{n-k}\|_2 \|y^k\|_2$$

Assume $n > N^2 \geqslant 4$, so that $n > 2\sqrt{n}$. If $0 < k \leqslant \sqrt{n}$, we have $0 < k \leqslant \sqrt{n} \Rightarrow n - k > \sqrt{n} \geqslant N$, which implies that $\|x^{n-k}\|_2 \|y^k\|_2 \leqslant (\nu_0(y)+\varepsilon)^{n-k} \|y\|_2^k \leqslant (\nu_0(y)+\varepsilon)^n \max\{1, \|y\|_2^{\sqrt{n}}\}$. If $\sqrt{n} < k \leqslant n$, then $k > N$, so $\|y^k\|_2 \leqslant (\nu_0(y)+\varepsilon)^k$. If $N \leqslant n-k$, then $\|x^{n-k}\|_2 \leqslant (\nu_0(y)+\varepsilon)^{n-k}$, whence $\|x^{n-k}\|_2 \|y^k\|_2 \leqslant (\nu_0(y)+\varepsilon)^n$. If $n - k < N$, we have $\|x^{n-k}\|_2 \leqslant \max\{1, \|x\|^N\}$, so that $\|x^{n-k}\|_2 \|y^k\|_2 \leqslant \max\{1, \|x\|^N\}(\nu_0(y)+\varepsilon)^n$. All together, we get $\|(x+y)^n\|_2 \leqslant (\nu_0(y)+\varepsilon)^n \max\{1, \|y\|_2^{\sqrt{n}}, \|x\|_2^N\}$, thus

$$\sqrt[n]{\|(x+y)^n\|_2} \leqslant (\nu_0(y)+\varepsilon) \max\left\{1, \|y\|_2^{1/\sqrt{n}}, \|x\|_2^{N/n}\right\}.$$

Passing to the limit as $n \to \infty$, we get $\nu_0(x+y) \leqslant \nu_0(y) + \varepsilon$. As this holds for all $\varepsilon \in \mathbf{R}_{>0}$, we have $\nu_0(x+y) \leqslant \nu_0(y)$: we have proved that ν_0 satisfies (5), *i.e.* $\nu_0 \in \Sigma$.
⊛ If $\nu_1, \nu_2 \in \sigma$, we write $\nu_1 \leqslant \nu_2$ if $\nu_1(x) \leqslant \nu_2(x)$ for all $x \in L$. This endows Σ with a partial order. If $(\nu_\lambda)_{\lambda \in \Lambda}$ is a chain in Σ, then $\nu \colon x \mapsto \inf\limits_{\lambda \in \Lambda} \nu_\lambda(x)$ defines an element in Σ. Indeed, properties (1), (3) and (4) are obvious. Property (2) follows from the fact that $(\nu_\lambda)_{\lambda \in \Lambda}$ is a chain. Assume $x, y \in L$ are such that $\nu(x) \leqslant \nu(y)$: if $\varepsilon \in \mathbf{R}_{>0}$, there exists $\lambda_0 \in \Lambda$ such that $\nu_{\lambda_0}(x) \leqslant \nu(x) + \varepsilon$. If $\lambda \in \Lambda$ is such that $\nu_\lambda \leqslant \nu_{\lambda_0}$, we have $\nu(x+y) \leqslant \nu_\lambda(x+y) \leqslant \max\{\nu_\lambda(x), \nu_\lambda(y)\} \leqslant \max\{\nu(x)+\varepsilon, \nu_\lambda(y)\} \leqslant \max\{\nu(y)+\varepsilon, \nu_\lambda(y)\}$, which implies that $\nu(x+y) \leqslant \nu(y) + \varepsilon$ by taking the infimum on λ. As this holds for all $\varepsilon \in \mathbf{R}_{>0}$, we have $\nu(x+y) \leqslant \nu(y) = \max\{\nu(x), \nu(y)\}$, showing that ν has property (5). Thus ν is a lower bound for $(\nu_\lambda)_{\lambda \in \Lambda}$ in Σ: by Zorn's lemma (*cf* theorem 9.1.1), Σ contains a minimal element ν.
⊛ Fix $a \in L^\times$ (so $\nu(a) > 0$) and let $x \in L^\times$: for all $k \in \mathbf{Z}_{>0}$ we have $\nu(xa^k) \leqslant \nu(xa^{k-1})\nu(a)$, hence $\nu(xa^k)\nu(a)^{-k} \leqslant \nu(xa^{k-1})\nu(a)^{-(k-1)}$: the sequence $(\nu(xa^k)\nu(a)^{-k})_{k \in \mathbf{Z}_{\geqslant 0}}$ is decreasing in $\mathbf{R}_{>0}$: it converges to a limit $\tau(x) \in \mathbf{R}_{\geqslant 0}$, and $\tau(x) \leqslant \nu(x)$.
The map τ obviously satisfies (1). As $\nu(xya^{2k})\nu(a)^{-2k} \leqslant \nu(xa^k)\nu(ya^k)\nu(a)^{-2k}$ for all $k \in \mathbf{Z}_{\geqslant 0}$, we have $\tau(xy) \leqslant \tau(x)\tau(y)$ for all $x, y \in L$, so τ satisfies (2). As ν satisfies (4), τ satisfies (3). If $x \in L$ and $k, n \in \mathbf{Z}_{>0}$, we have $\nu(x^k a^{kn})\nu(a)^{-kn} = (\nu(xa^n)\nu(a)^{-n})^k$ so $\tau(x^k) = \tau(x)^k$ by passing to the limit as $n \to \infty$, showing that τ satisfies (4). Finally, if $x, y \in L$, we have

$$\nu((x+y)a^k)\nu(a)^{-k} = \nu(xa^k + ya^k)\nu(a)^{-k} \leqslant \max\{\nu(xa^k)\nu(a)^{-k}, \nu(ya^k)\nu(a)^{-k}\}$$

(since ν has property (5)). Passing to the limit as $k \to \infty$ gives $\tau(x+y) \leqslant \max\{\tau(x), \tau(y)\}$.
This implies that $\tau \in \Sigma$. As $\tau \leqslant \nu$, we have $\tau = \nu$ by minimality of ν. This shows that the inequalities $\tau(x) \leqslant \nu(xa)\nu(a)^{-1} \leqslant \nu(x)$ are equalities, so that $\nu(xa) = \nu(x)\nu(a)$, which implies that $\nu \colon L \to \mathbf{R}_{\geqslant 0}$ is an absolute value. As it has properties (1) and (3), it extends $|.|$.
- General case. Let S be the set of pairs $(F, |.|_F)$ where F is a subfield of L containing K, and $|.|_F$ an absolute value extending $|.|$. We endow S with the partial order given by $(F_1, |.|_1) \leqslant (F_2, |.|_2)$ if and only if $F_1 \subset F_2$ and $|.|_{2|F_1} = |.|_1$. If $(F_\lambda, |.|_\lambda)_{\lambda\in\Lambda}$ is a chain in S, then $F = \bigcup\limits_{\lambda\in\Lambda} F_\lambda$ is a subfield of L, contains K, and the map $|.|_F : F \to \mathbf{R}_{\geqslant 0}$ given by $|x|_F = |x|_\lambda$ whenever $x \in F_\lambda$ is well defined, and is an absolute value on F. The pair $(F, |.|_F)$ is an upper bound for $(F_\lambda, |.|_\lambda)_{\lambda\in\Lambda}$. We may apply Zorn's lemma (*cf* theorem 9.1.1): there exists an maximal element $(F, |.|_F)$ in S. If $F \neq L$, choose $\alpha \in L \backslash F$. If α is algebraic (resp. transcendant) over F, the absolute value $|.|_F$ extends to $F(\alpha)$ by what precedes (resp. by lemma 3.5.1), contradicting the maximality of $(F, |.|_F)$. This means that $F = L$. □

Remark 3.5.5. The situation is completely different for archimedean valued fields. If $L/\mathbf{C}$ is a complete valued extension of $\mathbf{C}$, then $L = \mathbf{C}$ (this is a consequence of a theorem of Gel'fand-Mazur). As a consequence, a complete archimedean field is topologically isomorphic to $\mathbf{R}$ or $\mathbf{C}$.

Theorem 3.5.6. Assume $(K, |.|)$ is complete and L/K is algebraic. Then there is a unique absolute value extending $|.|$ on L.

Proof. We already know the existence of such an absolute value $|.|_L$.
- Assume that $|.|$ is trivial. If $x \in L^\times$, then $x^n + a_1x^{n-1} + \cdots + a_n = 0$ for some $n \in \mathbf{Z}_{\geqslant 0}$ and $a_1, \ldots, a_n \in K$. This implies the existence of $0 \leqslant i < j \leqslant n$ such that $\left|a_i x^{n-i}\right|_L = \left|a_j x^{n-j}\right|_L > 0$ (with the convention $a_0 = 1$), so that $|x|_L^{n-i} = |x|_L^{n-j}$, *i.e.* $|x|_L^{j-i} = 1$, whence $|x|_L = 1$, and $|.|_L$ is the trivial absolute value.
- Assume that $|.|$ is non trivial. Let $|.|_L'$ be a other absolute value extending $|.|$ on L. As L is a finite dimensional K-vector space and $(K, |.|)$ is complete, the norms $|.|_L$ and $|.|_L'$ are equivalent (*cf* theorem 3.4.12): they define the same topology. This implies that the absolute values $|.|_L$ and $|.|_L'$ are equivalent: there exists $\gamma \in \mathbf{R}_{>0}$ such that $|.|_L' = |.|_L^\gamma$ (*cf* proposition 3.1.7). As $|\lambda|_L = |\lambda|_L' = |\lambda|$, we have $|\lambda| = |\lambda|^\gamma$ for all $\lambda \in K$. As $|.|$ is non trivial, this implies that $\gamma = 1$, whence $|.|_L' = |.|_L$. □

Corollary 3.5.7. Assume $(K, |.|)$ is complete and let $\overline{K}$ an algebraic closure of K. Then $|.|$ extends uniquely to $\overline{K}$.

Corollary 3.5.8. Assume $(K, |.|)$ is complete and let L/K and L'/K be finite extensions. Denote by $|.|_L$ (resp. $|.|_{L'}$) the unique absolute value on L (resp. L') extending $|.|$. Then $|\sigma(x)|_{L'} = |x|_L$ for all $x \in L$ and all K-morphism $\sigma \colon L \to L'$.

Proposition 3.5.9. Under the hypothesis of theorem 3.5.6, assume L/K is finite. Then the unique absolute value $|.|_L$ extending $|.|$ is given by:

$$|x|_L = \sqrt[[L:K]]{\left|\mathsf{N}_{L/K}(x)\right|}$$

for all $x \in L$.

Proof. Let N be a normal closure of L/K. Denote by $x_1, \ldots, x_d \in N$ the conjugates of x over K (*i.e.* the roots of the minimal polynomial of x over K), counted with multiplicities, so that $d = [K(x) : K]$. For each $i \in \{1, \ldots, n\}$, there exists a unique K-morphism $\sigma_i \colon K(x) \to N$ such that $\sigma_i(x) = x_i$: by corollary 3.5.8, we have $|x_i|_N = |x|_L$, where $|.|_N$ is the unique absolute value on N extending $|.|$. Then $\left|\mathsf{N}_{K(x)/K}(x)\right| = \left|\prod\limits_{i=1}^{d} x_i\right|_N = |x|_L^d$. As $\mathsf{N}_{L/K}(x) = \mathsf{N}_{K(x)/K}(\mathsf{N}_{L/K(x)}(x)) = \mathsf{N}_{K(x)/K}(x)^{[L:K(x)]}$, we deduce $\left|\mathsf{N}_{L/K}(x)\right| = |x|_L^{d[L:K(x)]} = |x|_L^{[L:K]}$.

□

Corollary 3.5.10. Assume $(K, |.|)$ is complete, let L/K be a finite extension and denote by $|.|$ the unique absolute value on L extending $|.|$. Then $(L, |.|)$ is complete, and the ring of integers $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.

Proof. • As $(K, |.|)$ is complete and $(L, |.|)$ is a finite dimensional normed vector space over K, it is complete by theorem 3.4.12.
- Let $x \in L$ be integral over $\mathcal{O}_K$. Its conjugates over K are integral over $\mathcal{O}_K$ (apply an automorphism to an equation of integral dependence for x over $\mathcal{O}_K$): their product $\mathsf{N}_{L/K}(x) \in K$ is integral over $\mathcal{O}_K$. As

the latter is integrally closed (*cf* proposition 3.2.4), we have $\mathsf{N}_{L/K}(x) \in \mathcal{O}_K$, so $\left|\mathsf{N}_{L/K}(x)\right| \leqslant 1$, whence $|x| = \sqrt[n]{\left|\mathsf{N}_{L/K}(x)\right|} \leqslant 1$, *i.e.* $x \in \mathcal{O}_L$.

- Conversely, let $x \in \mathcal{O}_L$. The coefficients of its minimal polynomial P are (up to a sign) elementary symmetric polynomials in the conjugates of x (replacing L by its normal closure, we may assume that L/K is normal). As each of these belongs to the ring $\mathcal{O}_L$, so do the coefficients of P, which thus belong to $K \cap \mathcal{O}_L = \mathcal{O}_K$, and x is integral over $\mathcal{O}_K$. □

Remark 3.5.11. The ring of integers of a valuation thus deserves its name.

Until the end of this section, we drop the assumption on $|.|$ (*i.e.* we allow it to be archimedean).

Proposition 3.5.12. Assume $|.|$ is not trivial, and that L/K is finite. There are finitely many absolute values $|.|_1, \ldots, |.|_n$ extending $|.|$ on L. The map

$$\delta\colon \widehat{K} \otimes_K L \to \bigoplus_{i=1}^n \widehat{L_i}$$

induced by the diagonal map (where $\widehat{L_i}$ denotes the completion of L with respect to $|.|_i$) is surjective. In particular, we have $\sum_{i=1}^n [\widehat{L_i} : \widehat{K}] \leqslant [L : K]$ and there are at most $[L : K]$ absolute values extending $|.|$ on L. When $|.|$ is non archimedean, $\mathsf{Ker}(\delta)$ is the radical of $\widehat{K} \otimes_K L$.

Proof. • Let $|.|_1, \ldots, |.|_n$ be distinct absolute values extending $|.|$ on L. The composite $L \xrightarrow{\Delta} \bigoplus_{i=1}^n L \to \bigoplus_{i=1}^n \widehat{L_i}$ (where Δ is the diagonal map) is K-linear: as $\widehat{L_i}$ is a $\widehat{K}$-vector space for all $i \in \{1, \ldots, n\}$, it extends into the $\widehat{K}$-linear map δ. Note that the absolute values $|.|_1, \ldots, |.|_n$ are pairwise nonequivalent, otherwise there would exist integers $0 < i < j \leqslant n$ and $\gamma \in \mathbf{R}_{>0}$ such that $|.|_j = |.|_i^\gamma$, and we would have $\gamma = 1$ (because $|.| = |.|^\gamma$ and $|.|$ is not trivial), contradicting the hypothesis.

- Let $(z_1, \ldots, z_n) \in \bigoplus_{i=1}^n \widehat{L_i}$: for $\varepsilon \in \mathbf{R}_{>0}$, there exists $(y_1, \ldots, y_n) \in L^n$ such that $|z_i - y_i|_i < \varepsilon$ for all $i \in \{1, \ldots, n\}$. By theorem 3.1.15, there exists $x \in L$ such that $|x - y_i|_i < \varepsilon$, whence $|x - z_i|_i < 2\varepsilon$ for all $i \in \{1, \ldots, n\}$. This shows that the image of δ is dense in $\bigoplus_{i=1}^n \widehat{L_i}$. As $\dim_{\widehat{K}}(\widehat{K} \otimes_K L) = [L : K] < \infty$, this image is also a finite dimensional sub-$\widehat{K}$-vector space: by theorem 3.4.12, it is closed in the finite dimensional $\widehat{K}$-vector space $\bigoplus_{i=1}^n \widehat{L_i}$ (since $[\widehat{L_i} : \widehat{K}] < \infty$ for all $i \in \{1, \ldots, n\}$), so δ is surjective.
- As δ is $\widehat{K}$-linear and surjective, we have $\dim_{\widehat{K}}\left(\bigoplus_{i=1}^n \widehat{L_i}\right) \leqslant \dim_{\widehat{K}}(\widehat{K} \otimes_K L)$, *i.e.* $\sum_{i=1}^n [\widehat{L_i} : \widehat{K}] \leqslant [L : K]$. this shows that there are finitely many absolute values extending $|.|$ on L.
- Assume that $|.|$ is non archimedean. Take n maximal, *i.e.* so that $|.|_1, \ldots, |.|_n$ are exactly the absolute values extending $|.|$ on L. The $\widehat{K}$-algebra $\widehat{K} \otimes_K L$ has finite dimension: its prime ideals are maximal, and there are only finitely many of them, that we denote $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$. This implies that $\mathsf{rad}(\widehat{K} \otimes_K L) = \bigcap_{i=1}^r \mathfrak{m}_i$ is the nilradical of $\widehat{K} \otimes_K L$. If $x \in \mathsf{rad}(\widehat{K} \otimes_K L)$, there exists $m \in \mathbf{Z}_{>0}$ such that $x^m = 0$: if $\delta(x) = (x_1, \ldots, x_n)$, we have $x_i^m = 0$ in $\widehat{L_i}$, hence $x_i = 0$ for all $i \in \{1, \ldots, n\}$, so that $x \in \mathsf{Ker}(\delta)$. Conversely, let $i \in \{1, \ldots, r\}$. Put $\widetilde{L}_i := (\widehat{K} \otimes_K L)/\mathfrak{m}_i$: this is a finite field extension of $\widehat{K}$: by theorem 3.5.6, there exists a unique absolute value $\|.\|_i$ on $\widetilde{L}_i$ that extends $|.|$: there exists a unique $\sigma(i) \in \{1, \ldots, n\}$ such that $\|.\|_{i|L} = |.|_{\sigma(i)}$. Moreover, $\widetilde{L}_i$ is complete (by theorem 3.5.6 again) and L is dense in $\widetilde{L}_i$: we have $\widetilde{L}_i = \widehat{L_{\sigma(i)}}$. This implies in particular that if $x \notin \mathfrak{m}_i$, then the image of $x \in \widehat{L_{\sigma(i)}}$ is nonzero, so that $x \notin \mathsf{Ker}(\delta)$. We thus have $\mathsf{Ker}(\delta) = \bigcap_{i=1}^r \mathfrak{m}_i = \mathsf{rad}(\widehat{K} \otimes_K L)$. □

Corollary 3.5.13. Under the hypothesis of proposition 3.5.12, the following are equivalent:

(i) $\widehat{K} \otimes_K L$ is reduced;
(ii) δ is an isomorphism;
(iii) $\sum_{i=1}^n [\widehat{L_i} : \widehat{K}] = [L : K]$.

If these conditions are satisfied, then $\chi_{x,L/K}(X)=\prod\limits_{i=1}^{n}\chi_{x,\widehat{L_i}/\widehat{K}}(X)$ so in particular $\mathsf{Tr}_{L/K}(x)=\sum\limits_{i=1}^{n}\mathsf{Tr}_{\widehat{L_i}/\widehat{K}}(x)$ and $\mathsf{N}_{L/K}(x)=\prod\limits_{i=1}^{n}\mathsf{N}_{\widehat{L_i}/\widehat{K}}(x)$ for all $x\in L$. Moreover, we have $\left|\mathsf{N}_{L/K}(x)\right|=\prod\limits_{i=1}^{n}|x|_i^{[\widehat{L_i}:\widehat{K}]}$ for all $x\in L$.

Proof. The equivalence between the three statements is obvious, as is the equality of characteristic polynomials, that imply the equalities of traces and norms. Taking the absolute value of $\mathsf{N}_{L/K}(x)=\prod\limits_{i=1}^{n}\mathsf{N}_{\widehat{L_i}/\widehat{K}}(x)$ provides the last equality, noting that $\left|\mathsf{N}_{\widehat{L_i}/\widehat{K}}(x)\right|=|x|_i^{[\widehat{L_i}:\widehat{K}]}$ by proposition 3.5.9. □

Corollary 3.5.14. Under the hypothesis of proposition 3.5.12, if L/K is separable, the conditions of corollary 3.5.13 are satisfied.

Proof. If L/K is separable, there exists $\alpha\in L$ such that $L=K(\alpha)$ (primitive element theorem). Let $P\in K[X]$ be the minimal polynomial of α over K: we have $L\simeq K[X]/\langle P\rangle$, so that $\widehat{K}\otimes_K L\simeq\widehat{K}[X]/\langle P\rangle$. As P is separable, the ring $\widehat{K}[X]/\langle P\rangle$ is a product of finite extensions of $\widehat{K}$ (corresponding to the irreducible factors of P in $\widehat{K}[X]$): it is reduced. □

Proposition 3.5.15. Under the hypothesis of proposition 3.5.12, assume that L/K is Galois. Then the extensions $\widehat{L}_i/\widehat{K}$ are Galois, and

$$\mathsf{Gal}(\widehat{L}_i/\widehat{K})\simeq\{\sigma\in\mathsf{Gal}(L/K)\,;\,(\forall x\in L)\ |\sigma(x)|_i=|x|_i\}$$

(the RHS is the *decomposition subgroup* of L/K relative to $|.|_i$).

Proof. • By hypothesis, L is the decomposition field of a separable polynomial $P(X)\in K[X]\subset\widehat{K}[X]$. As $L\subset\widehat{L}_i$, the polynomial P is split in $\widehat{L}_i$. Let $\widetilde{L}_i$ be the subextension of $\widehat{L}_i/\widehat{K}$ generated by the roots of P: we have $L\subset\widetilde{L}_i$. As $\widetilde{L}_i$ is closed in $\widehat{L}_i$ with respect to $|.|_i$ (since $\widetilde{L}_i$ is finite dimensional) and L is dense in $\widehat{L}_i$, we have $\widetilde{L}_i=\widehat{L}_i$, implying that $\widehat{L}_i/\widehat{K}$ is Galois.
• Put $D_i:=\{\sigma\in\mathsf{Gal}(L/K)\,;\,(\forall x\in L)\ |\sigma(x)|_i=|x|_i\}$: any $\sigma\in D_i$ extends by continuity into an automorphism of $\widehat{L}_i$, so we have an injective group homomorphism $D_i\to\mathsf{Gal}(\widehat{L}_i/\widehat{K})$. If $\sigma\in\mathsf{Gal}(\widehat{L}_i/\widehat{K})$, we have $\sigma_{|K}=\mathsf{Id}_K$ and $\sigma(L)=L$ (since L/K is Galois), so the restriction $\sigma_{|L}$ belongs to $\mathsf{Gal}(L/K)$. As $(\widehat{K},|.|)$ is complete, corollary 3.5.8 implies that $|\sigma(x)|_i=|x|_i$ for all $x\in\widehat{L}_i$, so *a fortiori* for all $x\in L$, so that $\sigma_{|L}\in D_i$, and showing that $D_i\to\mathsf{Gal}(\widehat{L}_i/\widehat{K})$ is an isomorphism. □

3.5.16. *Completion of Dedekind rings.* Let L/K be a finite separable field extension, $|.|$ a non archimedean discrete absolute value on K and $A=\mathcal{O}_{K,|.|}$ its ring of integers (this is a DVR). We have $\widehat{K}=\mathsf{Frac}(\widehat{A})$ (*cf* proposition 3.3.8). Let B be the integral closure of A in L: this is a Dedekind ring by theorem 2.1.3. Denote by $\mathfrak{p}$ the maximal ideal of A and let $\mathfrak{p}B=\prod\limits_{i=1}^{r}\mathfrak{P}_i^{e_i}$ if factorization in B (so that the nonzero prime ideals of B are $\{\mathfrak{P}_1,\ldots,\mathfrak{P}_r\}$). In particular, B is semi-local: by proposition 2.3.15, it is in fact a PID.

Proposition 3.5.17. There are exactly r absolute values $|.|_1,\ldots,|.|_r$ extending $|.|$ to L. If $\widehat{L_i}$ denotes the completion of L with respect to $|.|_i$, there is an isomorphism

$$\delta\colon\widehat{K}\otimes_K L\xrightarrow{\sim}\bigoplus_{i=1}^{r}\widehat{L_i}$$

inducing an isomorphism

$$\widehat{A}\otimes_A B\xrightarrow{\sim}\bigoplus_{i=1}^{r}\widehat{B_i}$$

where $\widehat{B_i}$ is the ring of integers of $\widehat{L_i}$ for all $i\in\{1,\ldots,r\}$. Moreover, we have $[\widehat{L_i}:\widehat{K}]=e_if_i$ where $f_i=[\kappa(\mathfrak{P}_i):\kappa(\mathfrak{p})]$.

Proof. • Let $i\in\{1,\ldots,r\}$. The localization $B_{\mathfrak{P}_i}$ is a DVR: let $\pi_i\in B$ be a uniformizer. As $\mathfrak{P}_jB_{\mathfrak{P}_i}=B_{\mathfrak{P}_i}$ if $j\neq i$, we have $\mathfrak{p}B_{\mathfrak{P}_i}=\mathfrak{P}_i^{e_i}B_{\mathfrak{P}_i}=\pi_i^{e_i}B_{\mathfrak{P}_i}$: there exists $u_i\in B_{\mathfrak{P}_i}^{\times}$ such that $u_i\pi_i^{e_i}$ is a uniformizer of A. Denote $|.|_i$ the unique absolute value on $L=\mathsf{Frac}(B_{\mathfrak{P}_i})$ whose ring of integers is $B_{\mathfrak{P}_i}$ and such that $|\pi_i|_i^{e_i}=|u_i\pi_i^{e_i}|$: this normalization implies that $|.|_i$ extends $|,|$ on L. We have $\mathfrak{P}_i=B\cap\mathfrak{m}_{L,|.|_i}$, showing that the absolute values $|.|_1,\ldots,|.|_r$ are pairwise distinct.
• Let $\|.\|$ be an absolute value extending $|.|$ on L. As $\mathcal{O}_{L,\|.\|}$ is integrally closed (*cf* proposition 3.2.4) and contains A, it contains B, and $B\cap\mathfrak{m}_{L,\|.\|}$ is a nonzero prime ideal of B: there exists $i\in\{1,\ldots,r\}$ such that $B\cap\mathfrak{m}_{L,\|.\|}=\mathfrak{P}_i$. This implies that $B\backslash\mathfrak{P}_i\subset\mathcal{O}_{L,\|.\|}^{\times}$, so that $B_{\mathfrak{P}_i}\subset\mathcal{O}_{L,\|.\|}$. As $\|.\|$ extends $|.|$, we must

have $\|\pi_i\|^{e_i} = |u_i\pi_i^{e_i}|$, so that $\|.\|$ and $|.|_i$ coincide on $B_{\mathfrak{P}_i}$ hence on L. This shows that the absolute values extending $|.|$ on L are exactly $|.|_1, \dots, |.|_r$.

- We have $\mathfrak{p}^nB = \prod\limits_{i=1}^{r} \mathfrak{P}_i^{ne_i}$: by the Chinese remainder theorem, the natural map $B/\mathfrak{p}^nB \to \bigoplus\limits_{i=1}^{r} B/\mathfrak{P}_i^{ne_i}$ is an isomorphism. As A is a DVR, it is a PID, so B is a free A-module of finite rank, so $\varprojlim\limits_n B/\mathfrak{p}^nB \simeq \widehat{A}\otimes_A B$: passing to the limit provides a natural isomorphism $\widehat{A}\otimes_A B \xrightarrow{\sim} \bigoplus\limits_{i=1}^{r} \widehat{B_i}$, where $\widehat{B_i} = \varprojlim\limits_m B/\mathfrak{P}_i^m$. Note that for all $i \in \{1,\dots,r\}$, we have $B/\mathfrak{P}_i^m \xrightarrow{\sim} B_{\mathfrak{P}_i}/\mathfrak{P}_i^m B_{\mathfrak{P}_i}$, so that $\widehat{B_i}$ coincides with the completion of the DVR $B_{\mathfrak{P}_i}$. Moreover, $\widehat{K}\otimes_A B = \widehat{K}\otimes_K L$ (because $L = KB$) and similarly $\widehat{K}\otimes_A \widehat{B_i}$ is a field: this is the completion $\widehat{L_i}$ of L with respect to $|.|_i$. The preceding isomorphism thus induces a $\widehat{K}$-linear isomorphism $\widehat{K}\otimes_K L \xrightarrow{\sim} \bigoplus\limits_{i=1}^{r} \widehat{L_i}$.
- The statement on rings of integers follows, noting that $\widehat{B_i} = \varprojlim\limits_m B_{\mathfrak{P}_i}/\mathfrak{P}_i^m B_{\mathfrak{P}_i}$ is the ring of integers of $\widehat{L_i}$ since $B_{\mathfrak{P}_i}$ is that of L for the absolute value $|.|_i$.
- We have seen that $\mathfrak{p}B_{\mathfrak{P}_i} = \mathfrak{P}_i^{e_i}B_{\mathfrak{P}_i}$: this implies that $e_{\widehat{L_i}/\widehat{K}} = e_i$. Similarly, we have $\kappa_{\widehat{L_i}} =_{\mathfrak{P}_i} /\mathfrak{P}_i = \kappa(\mathfrak{P}_i)$ and $\kappa_{\widehat{K}} = A/\mathfrak{p} = \kappa(\mathfrak{p})$, so that $f_{\widehat{L_i}/\widehat{K}} = [\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{p})]$: the equality $[\widehat{L_i} : \widehat{K}] = e_if_i$ follows from theorem 3.8.4. □

Remark 3.5.18. (1) Taking dimensions, the isomorphism δ implies the equality of theorem 2.4.2.
(2) As A is noetherian and B is of finite type, $\widehat{A}\otimes_A B$ is nothing but the $\mathfrak{p}$-adic completion of B (*cf* corollary 1.11.38).
(3) The previous proposition is a special case of proposition 3.5.12 and its corollaries.

Corollary 3.5.19. If $x \in L$, we have $\mathsf{Tr}_{L/K}(x) = \sum\limits_{i=1}^{r} \mathsf{Tr}_{\widehat{L_i}/\widehat{K}}(x)$ and $\mathsf{N}_{L/K}(x) = \prod\limits_{i=1}^{r} \mathsf{N}_{\widehat{L_i}/\widehat{K}}(x)$.

Corollary 3.5.20. If L/K is Galois, so is $\widehat{L_i}/\widehat{K}$, and $\mathsf{Gal}(\widehat{L_i}/\widehat{K})$ identifies with the decomposition subgroup $D_i = \{\sigma \in \mathsf{Gal}(L/K)\,;\, \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}$.

Proof. Any $\sigma \in D_i$ extends by continuity into an element in $\mathsf{Aut}_{\widehat{K}}(\widehat{L_i})$: the statement follows from the equalities $\#D_i = e_if_i = [\widehat{L_i} : \widehat{K}]$ (*cf* theorem 2.4.5). □

Proposition 3.5.21. Let $\mathfrak{P}$ be a nonzero prime ideal in B and $\mathfrak{p} = A \cap \mathfrak{P}$. Denote by $\widehat{B}$ (resp. $\widehat{A}$) the $\mathfrak{P}$-adic (resp. $\mathfrak{p}$-adic) completion of B (resp. A). Then $\mathfrak{D}_{\widehat{B}/\widehat{A}} = \widehat{B}\otimes_B \mathfrak{D}_{B/A}$ (*i.e.* "the different of the completion is the completion of the different").

Proof. As $\widehat{A}$ coincides with the $\mathfrak{p}$-adic completion of $A_{\mathfrak{p}}$ (and similarly for B) by lemma 1.11.29, and as taking integal closure commutes with localization (*cf* proposition 1.9.13), we may replace A by $A_{\mathfrak{p}}$, and assume that A is a DVR. We use the notation of section 3.5.16.
By proposition 3.5.17, the isomorphism $\delta\colon \widehat{K}\otimes_K L \xrightarrow{\sim} \bigoplus\limits_{i=1}^{r} \widehat{L_i}$ induces an isomorphism $\widehat{A}\otimes_A B \xrightarrow{\sim} \bigoplus\limits_{i=1}^{r} \widehat{B_i}$, where $\widehat{B_i}$ is the ring of integers of $\widehat{L_i}$. The K-bilinear form $L \times L \to K$ defined by the trace $\mathsf{Tr}_{L/K}$ induces a $\widehat{K}$-bilinear map $\psi\colon (\widehat{K}\otimes_K L)\times(\widehat{K}\otimes_K L) \to \widehat{K}$ by extension of scalars. Then we have $(\widehat{A}\otimes_A B)^* = \widehat{A}\otimes_A B^*$ (this can be seen using dual bases of B and B^*). Moreover, ψ induces the bilinear map attached to $\mathsf{Tr}_{\widehat{L_i}/\widehat{K}}$ on $\widehat{L_i}\times\widehat{L_i}$ for all $i \in \{1,\dots,r\}$. With obvious notations, this implies that $\bigoplus\limits_{i=1}^{r}(\widehat{A}\otimes_A B_i^*) = \widehat{A}\otimes_A B^* = \Big(\bigoplus\limits_{i=1}^{r}\widehat{B_i}\Big)^* = \bigoplus\limits_{i=1}^{r}\widehat{B_i}^*$, hence $\widehat{A}\otimes_A B_i^* = \widehat{B_i}^*$ for all $i \in \{1,\dots,r\}$ (since the factors $\widehat{L_i}$ are pairwise orthogonal for ψ). Taking inverses, this gives $\mathfrak{D}_{\widehat{B_i}/\widehat{A}} = \widehat{A}\otimes_A \mathfrak{D}_{B_{\mathfrak{P}_i}/A} = \widehat{B_i}\otimes_B \mathfrak{D}_{B/A}$. □

Corollary 3.5.22. Let $\mathfrak{p}$ be a nonzero prime ideal in A, and $\widehat{\mathfrak{d}}_{B/A}$ the ideal of $\widehat{A} = \varprojlim\limits_n A/\mathfrak{p}^n$ generated by $\mathfrak{d}_{B/A}$. Then $\widehat{\mathfrak{d}}_{B/A} = \prod\limits_{\mathfrak{P}|\mathfrak{p}} \mathfrak{d}_{\widehat{B_{\mathfrak{P}}}/\widehat{A}}$ (where $\widehat{B_{\mathfrak{P}}} = \varprojlim\limits_n B/\mathfrak{P}^n$).

Proof. Follows from proposition 3.5.21 by taking the norm (*cf* proposition 2.5.9). □

Theorem 3.5.23. Let $\mathfrak{P}$ be a nonzero ideal of B and $\mathfrak{p} = A \cap \mathfrak{P}$. The extension L/K is unramified at $\mathfrak{P}$ if and only if $\mathfrak{P}$ does not divide the different $\mathfrak{D}_{B/A}$.

Proof. Normalization and the different ideal are compatible with localization (*cf* propositions 1.9.13 and 2.5.8): we may replace A by $A_{\mathfrak{p}}$ and assume that A is a DVR with maximal ideal $\mathfrak{p}$. By proposition 3.5.21, we may also replace A (resp. B) by its $\mathfrak{p}$-adic (resp. $\mathfrak{P}$-adic) completion, and assume that B is a DVR with maximal ideal $\mathfrak{P}$. In that case, L/K is unramified (at $\mathfrak{P}$) if and only if $B/\mathfrak{p}B$ is a separable field extension of $\kappa(\mathfrak{p}) = A/\mathfrak{p}$: we have to prove this is equivalent to $\mathfrak{D}_{B/A} = B$, *i.e.* to $\mathfrak{d}_{B/A} = A$ (*cf* proposition 2.5.9). Let $(x_1, \ldots, x_d)$ a basis de B over A (so that $\mathfrak{d}_{B/A} = \mathrm{D}(x_1, \ldots, x_d)A$). As $\mathfrak{d}_{(B/\mathfrak{p}B)/\kappa(\mathfrak{p})} = \mathrm{D}(x_1, \ldots, x_d)A/\mathfrak{p}$ (because $(x_1, \ldots, x_d)$ is a basis de $B/\mathfrak{p}B$ over $\kappa(\mathfrak{p})$), it is enough to show that $B/\mathfrak{p}B$ is a separable extension of $\kappa(\mathfrak{p})$ if and only if $\mathfrak{d}_{(B/\mathfrak{p}B)/\kappa(\mathfrak{p})} \neq \{0\}$. If $B/\mathfrak{p}B$ is a separable extension of $\kappa(\mathfrak{p})$, then $\mathfrak{d}_{(B/\mathfrak{p}B)/\kappa(\mathfrak{p})} \neq \{0\}$ by proposition 1.10.22. Conversely, assume that $\mathfrak{d}_{(B/\mathfrak{p}B)/\kappa(\mathfrak{p})} \neq 0$. We have $\mathfrak{p}B = \mathfrak{P}^e$: assume that $e > 1$. We may assume that some elements in the basis $(\overline{x}_1, \ldots, \overline{x}_d)$ belong to $\mathfrak{P}/\mathfrak{p}B$. By definition, this implies that $\mathfrak{d}_{(B/\mathfrak{p}B)/\kappa(\mathfrak{p})} \in \mathfrak{P}/\mathfrak{p}B$ hence $\mathfrak{d}_{(B/\mathfrak{p}B)/\kappa(\mathfrak{p})} = \{0\}$, which is not: we have necessarily $e = 1$, so that $B/\mathfrak{p}B = \kappa(\mathfrak{P})$ is a field, and a finite extension of $\kappa(\mathfrak{p})$. If it was not separable, we would have $\mathsf{Tr}_{\kappa(\mathfrak{P})/\kappa(\mathfrak{p})} = 0$ (*cf* corollary 1.10.5), so that $\mathfrak{d}_{\kappa(\mathfrak{P})/\kappa(\mathfrak{p})} = 0$, which is not: $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is separable. □

Theorem 3.5.24. Assume[33] that B is a free A-module. Nonzero prime ideals of A that are ramified in the extension L/K are precisely the divisors of the discriminant ideal $\mathfrak{d}_{B/A}$. In particular, there are only finitely many such ideals.

Proof. Follows from theorem 3.5.23 since $\mathfrak{d}_{B/A} = \mathsf{N}_{B/A}(\mathfrak{D}_{B/A})$ (*cf* proposition 2.5.9). □

3.6. **Hensel's lemma.** Let $(K, |.|)$ be a complete non archimedean valued field. Recall that $K(X)$ is endowed with the Gauss absolute value $|.|_{\mathrm{Gauss}}$ defined by

$$|P|_{\mathrm{Gauss}} = \max_{0 \leqslant i \leqslant n} |a_i|$$

for $P = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$ (*cf* lemma 3.5.1 and definition 3.5.2)
For $n \in \mathbf{Z}_{\geqslant 0}$, we put $W_n = \{P \in K[X]\,;\, \deg(P) < n\}$. If $F, G \in K[X]$ are such $\deg(F) = n$ and $\deg(G) = m$, the determinant of the K-linear map

$$\begin{aligned} \Theta\colon W_n \oplus W_m &\to W_{n+m} \\ (f, g) &\mapsto fG + gF \end{aligned}$$

is, up to a sign, the Sylvester resultant $\mathsf{Res}(F, G)$ of F and G (in the canonical bases of W_n, W_m and W_{n+m}).

Theorem 3.6.1. (Hensel's lemma). Assume $P, F, G \in \mathcal{O}_K[X]$ and $\varepsilon \in [0, 1[$ are such that:

(i) $\deg(F) = n$, $\deg(G) = m$ and $\deg(P) = n + m$;
(ii) $|P - FG|_{\mathrm{Gauss}} \leqslant \varepsilon\, |\mathsf{Res}(F, G)|^2$;
(iii) $P - FG \in W_{n+m}$, *i.e.* $\deg(P - FG) < n + m$.

Then there exist $\widetilde{F}, \widetilde{G} \in \mathcal{O}_K[X]$ such that:

- $P = \widetilde{F}\widetilde{G}$;
- $\widetilde{F} - F \in W_n$ and $\widetilde{G} - G \in W_m$;
- $|\widetilde{F} - F|_{\mathrm{Gauss}} \leqslant \varepsilon\, |\mathsf{Res}(F, G)|$ and $|\widetilde{G} - G|_{\mathrm{Gauss}} \leqslant \varepsilon\, |\mathsf{Res}(F, G)|$.

Proof. • We can of course assume that $|\mathsf{Res}(F, G)| > 0$. Put $V_n = \{f \in W_n\,;\, |f|_{\mathrm{Gauss}} \leqslant \varepsilon\, |\mathsf{Res}(F, G)|\}$ and $V_m = \{g \in W_m\,;\, |g|_{\mathrm{Gauss}} \leqslant \varepsilon\, |\mathsf{Res}(F, G)|\}$ and $\|(f, g)\| := \max\{|f|_{\mathrm{Gauss}}, |g|_{\mathrm{Gauss}}\}$ for all $(f, g) \in V_n \oplus V_m$. Property (iii) implies that the map

$$\begin{aligned} \Phi\colon V_n \oplus V_m &\to W_{n+m} \\ (f, g) &\mapsto P - FG - fg \end{aligned}$$

is well defined, so we can consider the map $\Theta^{-1} \circ \Phi\colon V_n \oplus V_m \to W_n \oplus W_m$. By condition (ii), we have

$$\begin{aligned} |P - FG - fg|_{\mathrm{Gauss}} &\leqslant \max\{|P - FG|_{\mathrm{Gauss}}, |fg|_{\mathrm{Gauss}}\} \\ &\leqslant \max\{\varepsilon\, |\mathsf{Res}(F, G)|, \varepsilon^2\, |\mathsf{Res}(F, G)|^2\} = \varepsilon\, |\mathsf{Res}(F, G)|^2 . \end{aligned}$$

As $F, G \in \mathcal{O}_K[X]$, the matrix of Θ in the canonical bases has coefficients in $\mathcal{O}_K$. By Cramer's formulae, we have $|||\Theta^{-1}||| \leqslant \frac{1}{|\mathsf{Res}(F,G)|}$, so that $\|(\Theta^{-1} \circ \Phi)(f, g)\| \leqslant \varepsilon\, |\mathsf{Res}(F, G)|$, *i.e.* $(\Theta^{-1} \circ \Phi)(f, g) \in V_n \oplus V_m$. This implies that $\Theta^{-1} \circ \Phi$ induces a map $\Lambda\colon (V_n \oplus V_m) \to V_n \oplus V_m$.

[33] Again, this is not really necessary once the discriminant ideal has been properly defined.

- Let $(f_1, g_1), (f_2, g_2) \in V_n \oplus V_m$. We have

$$\begin{aligned}\|\Lambda(f_1,g_1) - \Lambda(f_2,g_2)\| &= \|\Theta^{-1}(f_2g_2 - f_1g_1)\| \\ &= \|\Theta^{-1}(f_2(g_2-g_1) + g_1(f_2-f_1))\| \\ &\leqslant \frac{1}{|\mathsf{Res}(P,Q)|}\max\{|f_2|_{\mathrm{Gauss}}\,|g_2-g_1|_{\mathrm{Gauss}}\,, |g_1|_{\mathrm{Gauss}}\,|f_2-f_1|_{\mathrm{Gauss}}\} \\ &\leqslant \varepsilon\max\{|g_2-g_1|_{\mathrm{Gauss}}\,, |f_2-f_1|_{\mathrm{Gauss}}\}\end{aligned}$$

which shows that Λ is a contractive map. Now W_n and W_m are finite dimensional K-vector spaces: they are complete (*cf* theorem 3.4.12). The same holds for the closed subsets V_n and V_m. We may thus apply the fixed point theorem: there exists $(f,g) \in V_n \oplus V_m$ such that $\Lambda(f,g) = (f,g)$, *i.e.* $\Phi(f,g) = \Theta(f,g)$, which means that $P - FG - fg = fG + gF$, in other words $P = (F+f)(G+g)$, so that $P = \widetilde{F}\widetilde{G}$ where $\widetilde{F} = F + f$ and $\widetilde{G} = G + g$ satisfy the contition of the statement. □

Remark 3.6.2. Newton's lemma (theorem 3.3.10) is a special case of theorem 3.6.1: let $\alpha \in \mathcal{O}_K$ be such that $|P(\alpha)| \leqslant \varepsilon\,|P'(\alpha)|^2$. Put $F(X) = X - \alpha$ and $G(X) = \frac{P(X)-P(\alpha)}{X-\alpha} = \sum\limits_{i=1}^{\deg(P)} P^{[i]}(\alpha)(X-\alpha)^{i-1}$ in $\mathcal{O}_K[X]$. The assumption (i) of theorem 3.6.1 is satisfied with $n = 1$ and $m = d-1$ where $d = \deg(P)$. As $P - FG = P(\alpha)$, the assumtion (iii) is also satisfied. As $\mathsf{Res}(F,G)$ is the determinant

$$\begin{vmatrix} 1 & 0 & \cdots & 0 & P^{[d]}(\alpha) \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ \vdots & & \ddots & 1 & P^{[2]}(\alpha) \\ 0 & \cdots & \cdots & 0 & P'(\alpha) \end{vmatrix} = P'(\alpha)$$

(we made the change of variable $Y = X - \alpha$), the hypothesis $|P(\alpha)| \leqslant \varepsilon\,|P'(\alpha)|^2$ translates into the inequality $|P - FG|_{\mathrm{Gauss}} \leqslant \varepsilon\,|\mathsf{Res}(F,G)|^2$, which is precisely assumtion (ii) of theorem 3.6.1. We thus have $\widetilde{F}, \widetilde{G} \in \mathcal{O}_K[X]$ satisfying the conclusion thereof: we have $P = \widetilde{F}\widetilde{G}$ and $\widetilde{F}(X) = X - \widetilde{\alpha}$, so that $P(\widetilde{\alpha}) = 0$, and $|\widetilde{\alpha} - \alpha| = |\widetilde{F} - F|_{\mathrm{Gauss}} \leqslant \varepsilon\,|\mathsf{Res}(F,G)| = \varepsilon\,|P'(\alpha)|$.

Corollary 3.6.3. Let $P, F, G \in \mathcal{O}_K[X]$ be such that:

(i) $\deg(F) = n$, $\deg(G) = m$ and $\deg(P) = n + m$;
(ii) $\overline{P} = \overline{F}\,\overline{G}$ has degree $n + m$ and $\mathsf{gcd}(\overline{F}, \overline{G}) = 1$ (where $\overline{P}$ denotes the image of P in $\kappa_K[X]$);
(iii) $P - FG \in W_{n+m}$,

Then there exist $\widetilde{F}, \widetilde{G} \in \mathcal{O}_K[X]$ such that:

- $P = \widetilde{F}\widetilde{G}$;
- $\widetilde{F} - F \in W_n$ and $\widetilde{G} - G \in W_m$;
- $|\widetilde{F} - F|_{\mathrm{Gauss}} < 1$ and $|\widetilde{G} - G|_{\mathrm{Gauss}} < 1$.

Proof. As $F, G \in \mathcal{O}_K[X]$, we have $\mathsf{Res}(F,G) \in \mathcal{O}_K$. As $\deg(\overline{P}) = n + m$, we have $\deg(\overline{F}) = n$ and $\deg(\overline{G}) = m$, so that $\overline{\mathsf{Res}(F,G)} = \mathsf{Res}(\overline{F}, \overline{G})$. As $\gcd(\overline{F}, \overline{G}) = 1$ by hypothesis, we have $\mathsf{Res}(\overline{F}, \overline{G}) \in \kappa_K^\times$, so $|\mathsf{Res}(F,G)| = 1$. As $\overline{P} = \overline{F}\,\overline{G}$, we have $\varepsilon := |P - FG| \in [0, 1[$: the result follows from theorem 3.6.1. □

3.7. **Structure of complete discrete valuation fields.** In this section, we assume that $(K, |.|)$ is a *complete and discrete* non archimedean valued field. This implies that $\mathcal{O}_K$ is noetherian. Let v_K be the *normalized* valuation associated to $|.|$, *i.e.* such that $v_K(K^\times) = \mathbf{Z}$, and π_K a uniformizer of K.

3.7.1. *Structure of the additive group.*

Proposition 3.7.2. (Structure of the ring of integers of a finite extension). If L/K be a *finite separable* extension of degree d, then $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank d.

Proof. As $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L (*cf* corollary 3.5.10), it is noetherian hence of finite type over $\mathcal{O}_K$ (*cf* corollary 1.10.39 (1)). As $\mathcal{O}_K$ is a PID and $\mathcal{O}_L$ is torsionfree, it is a free $\mathcal{O}_K$-module (*cf* corollary 1.4.15). Its rank is $d = [L : K]$ since $L = \mathcal{O}_L\big[\frac{1}{\pi_K}\big] \simeq K \otimes_{\mathcal{O}_K} \mathcal{O}_L$. □

We have the filtration

$$\{0\} \subset \cdots \subset \mathfrak{m}_K^{n+1} \subset \mathfrak{m}_K^n \subset \cdots \subset \mathfrak{m}_K \subset \mathcal{O}_K$$

and fractional ideals in K are of the form $\mathfrak{m}_K^n = \pi_K^n \mathcal{O}_K$ with $n \in \mathbf{Z}$.

Proposition 3.7.3. Let $\Sigma \subset \mathcal{O}_K$ be a complete set of representatives for κ_K containing 0. For each $n \in \mathbf{Z}$, let $\pi_n \in K^\times$ be such that $v_K(\pi_n) = n$ (for instance one may take $\pi_n = \pi_K^n$ for all $n \in \mathbf{Z}$). Put $\mathscr{E} = \{(x_n)_{n\in\mathbf{Z}} \in \Sigma^{\mathbf{Z}}\,;\, x_n = 0 \text{ for } n \ll 0\}$, and

$$\begin{aligned} f\colon \mathscr{E} &\to K \\ (x_n)_{n\in\mathbf{Z}} &\mapsto \sum_{n\in\mathbf{Z}} x_n\pi_n. \end{aligned}$$

Then f is a bijection.

Proof. First observe that f is well defined, because K is complete for v_K.
• Let $\mathbf{x} = (x_n)_{n\in\mathbf{Z}}$ and $\mathbf{y} = (y_n)_{n\in\mathbf{Z}}$ be distinct elements in $\mathscr{E}$: there exists $N \in \mathbf{Z}$ such that $x_N \neq y_N$ and $(\forall i < N)\, x_i = y_i$. We thus have $f(\mathbf{y}) - f(\mathbf{x}) = \sum\limits_{n=N}^{\infty} (y_n - x_n)\pi_n \in K$. As $y_N \neq x_N$, we have $v_K(y_N - x_N) = 0$, hence $v_K((y_N - x_N)\pi_N) = N < n \leqslant v_K((y_n - x_n)\pi_n)$ for all $n > N$. This implies that $v_K(f(\mathbf{y}) - f(\mathbf{x})) = N < +\infty$, so that $f(\mathbf{y}) - f(\mathbf{x}) \neq 0$, showing that the map f is injective.
• Let $x \in K^\times$. There exists a unique $n_0 \in \mathbf{Z}$ such that $x \in \pi_K^{n_0}\mathcal{O}_K \backslash \pi_K^{n_0+1}\mathcal{O}_K$, *i.e.* $x \in \pi_{n_0}\mathcal{O}_K^\times$ (we have $v_K(x) = n_0 v_K(\pi_K)$). By definition of Σ, there exists a unique $x_{n_0} \in \Sigma\backslash\{0\}$ such that $x - x_{n_0}\pi_{n_0} \in \pi_{n_0+1}\mathcal{O}_K$. Let $m \geqslant n_0$ be such that $x_{n_0}, \ldots, x_m \in \Sigma$ have been constructed such that $x - \sum\limits_{n=n_0}^{m} x_n\pi_n \in \pi_{m+1}\mathcal{O}_K$: write $x - \sum\limits_{n=n_0}^{m} x_n\pi_n = \pi_{m+1}y_{m+1}$ with $y_{m+1} \in \mathcal{O}_K$. By definition of Σ again, there exists a unique $x_{m+1} \in \Sigma$ such that $y_{m+1} \equiv x_{m+1} \mod \mathfrak{m}_K$, and we have $x - \sum\limits_{n=n_0}^{m+1} x_n\pi_n \in \pi_{m+2}\mathcal{O}_K$. By induction, we thus construct a sequence $\mathbf{x} = (x_n)_{n\in\mathbf{Z}} \in \mathscr{E}$ such that $x_n = 0$ for all $n < n_0$ and $x - \sum\limits_{n=n_0}^{m} x_n\pi_n \in \pi_{m+1}\mathcal{O}_K$ for all $n \in \mathbf{Z}_{\geqslant n_0}$. Passing to the limit an $m \to \infty$, we get $x = f(\mathbf{x})$, showing that f is surjective. □

Corollary 3.7.4. We have $\mathsf{Card}(K) = \mathsf{Card}(\kappa_K)^{\mathbf{N}}$. In particular, K is uncountable.

Corollary 3.7.5. The restriction of f induces an homeomorphism

$$f\colon \Sigma^{\mathbf{Z}_{\geqslant 0}} \xrightarrow{\sim} \mathcal{O}_K$$

where $\Sigma^{\mathbf{Z}_{\geqslant 0}}$ is endowed with the product topology, each copy of Σ being endowed with the discrete topology.

Proof. • We know that $f\colon \Sigma^{\mathbf{Z}_{\geqslant 0}} \xrightarrow{\sim} \mathcal{O}_K$ is bijective by proposition 3.7.3.
• Let $a \in \mathcal{O}_K$ and $N \in \mathbf{Z}_{\geqslant 0}$. Write $f^{-1}(a) = (a_n)_{n\in\mathbf{Z}_{\geqslant 0}}$. By construction we have

$$f^{-1}(a + \pi_K^N\mathcal{O}_K) = \{(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}\,;\, (\forall n < N)\, x_n = a_n\}.$$

This implies that via f, the open subsets $\{a + \pi_K^N\mathcal{O}_K\}_{\substack{a\in\mathcal{O}_K \\ N\in\mathbf{Z}_{\geqslant 0}}}$ (which form a basis for the topology on $\mathcal{O}_K$) correspond to the open subsets $\big\{\{(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}\,;\, (\forall n < N)\, x_n = a_n\}\big\}_{\substack{a\in\mathcal{O}_K \\ N\in\mathbf{Z}_{\geqslant 0}}}$ (which form a basis for the product topology on $\Sigma^{\mathbf{Z}_{\geqslant 0}}$). This precisely means that the bijection f is an homeomorphism. □

Example 3.7.6. If $K = \mathbf{Q}_p$, we have $\kappa_K = \mathbf{F}_p$, and we can take $\Sigma = \{0, 1, \ldots, p-1\}$. An other choice is given by $\Sigma = \{0\} \cup \mu_{p-1}$ (*cf* example 3.3.12). In particular, we have $\mathsf{Card}(\mathbf{Q}_p) = \mathsf{Card}(\mathbf{Z}_p) = p^{\mathbf{N}} = \mathsf{Card}(\mathbf{R})$.

3.7.7. *Structure of the multiplicative group.* The sequence

$$\{1\} \to \mathcal{O}_K^\times \to K^\times \xrightarrow{v_K} \mathbf{Z} \to \{0\}$$

is exact. The choice of the uniformizer π_K provides a splitting for this sequence: we have

$$K^\times \simeq \mathcal{O}_K^\times \times \pi_K^{\mathbf{Z}}$$

Definition 3.7.8. For $i \in \mathbf{Z}_{\geqslant 0}$, we put

$$U_K^{(i)} = \begin{cases} \mathcal{O}_K^\times & \text{if } i = 0 \\ 1 + \mathfrak{m}_K^i = \{x \in K\,;\, v_K(x-1) \geqslant i\} & \text{if } i > 0 \end{cases}$$

This defines a filtration of $\mathcal{O}_K^\times$ by subgroups

$$\{1\} \subset \cdots \subset U_K^{(i+1)} \subset U_K^{(i)} \subset \cdots \subset U_K^{(1)} \subset U_K^{(0)} = \mathcal{O}_K^\times$$

Remark 3.7.9. As $\mathcal{O}_K = \overline{\mathsf{B}}(0,1) = \mathsf{B}\big(0, \frac{1}{\sqrt{|\pi_K|}}\big)$ is both open and closed in K, so are the subgroups $U_K^{(i)}$ in $K^\times$. Note that as open balls are both open and closed, the topology on K is totally disconnected, *i.e.* its connected components are its points.

Proposition 3.7.10. (1) The canonical projection $\mathcal{O}_K \to \kappa_K$; $x \mapsto (x \mod \mathfrak{m}_K)$ induces a group isomorphism

$$U_K^{(0)}/U_K^{(1)} \xrightarrow{\sim} \kappa_K^\times.$$

(2) The map $U_K^{(i)} \to \kappa_K$; $1 + \pi_K^i x \mapsto (x \mod \mathfrak{m}_K)$ induces a group isomorphism

$$U_K^{(i)}/U_K^{(i+1)} \xrightarrow{\sim} \kappa_K.$$

Proof. (1) As $x \in \mathcal{O}_K$ is invertible if and only if $x \mod \mathfrak{m}_K \in \kappa_K^\times$, the canonical map $U_K^{(0)} \to \kappa_K^\times$ is surjective. Its kernel is $\{x \in \mathcal{O}_K\,;\, x \equiv 1 \mod \mathfrak{m}_K\} = U_K^{(1)}$, whence the result.
(2) The map $U_K^{(i)} \to \kappa_K$; $1 + \pi_K^i x \mapsto (x \mod \mathfrak{m}_K)$ is surjective (because $\mathcal{O}_K \to \kappa_K$ is) and its kernel is $U_K^{(i+1)}$. □

3.8. **Ramification.** Here again, we assume that $(K, |.|)$ is a non archimedean valued field.

Definition 3.8.1. Let L/K be a finite extension, and $|.|_L$ an absolute value extending $|.|$ to L. As $(K, |.|)$ is non archimedean, so is $(L, |.|_L)$. Denote by $\mathcal{O}_K$ and $\mathcal{O}_L$ (resp. κ_K and κ_L) the rings of integers (resp. the residue fields) of $(K, |.|)$ and $(L, |.|_L)$ respectively (note that $\mathcal{O}_L$ and κ_L depend on the extension $|.|_L$). The inclusion $\mathcal{O}_K \subset \mathcal{O}_L$ induces a field extension κ_L/κ_K, whose degree

$$f_{L/K} = \big[\kappa_L : \kappa_K\big]$$

is called the *residual degree* of the extension $(L, |.|_L)/(K, |.|)$. As $|.|_L$ extends $|.|$, the subgroup $|K^\times| \subset \mathbf{R}_{>0}$ is a subgroup in $|L^\times|_L$. The index

$$e_{L/K} = \big[\,|L^\times|_L : |K^\times|\,\big]$$

is called the *ramification index* of the extension $(L, |.|_L)/(K, |.|)$.

Theorem 3.8.2. $e_{L/K} f_{L/K} \leqslant [L : K]$.

Proof. Let $n, m \in \mathbf{Z}_{>0}$ be such that $n \leqslant e_{L/K}$ and $m \leqslant f_{L/K}$. Fix $x_1, \ldots, x_n \in L^\times$ such that the cosets $\{|x_i|_L\,|K^\times|\}_{1 \leqslant i \leqslant n}$ are pairwise distinct. Similarly, let $y_1, \ldots, y_m \in \mathcal{O}_L$ whose images $\overline{y}_1, \ldots, \overline{y}_m \in \kappa_L$ are linearly independant over κ_K: we have to show that $\{x_i y_j\}_{\substack{1 \leqslant i \leqslant n\\ 1 \leqslant j \leqslant m}}$ are linearly independent over K.

- We first prove that if $\lambda_1, \ldots, \lambda_m \in K$ and $\alpha = \sum\limits_{j=1}^m \lambda_j y_j \in L$, then $|\alpha|_L = \max\limits_{1 \leqslant j \leqslant m} |\lambda_j|$. This is obvious if $\lambda_1 = \cdots = \lambda_m = 0$: assume the contrary. Renumbering if necessary, we may assume that $|\lambda_1| = \max\limits_{1 \leqslant j \leqslant m} |\lambda_j|$. Dividing α by λ_1, we reduce to the case where $\lambda_1 = 1$ and $\lambda_j \in \mathcal{O}_K$ for all $j \in \{1, \ldots, m\}$. As the elements $\overline{y}_1, \ldots, \overline{y}_m \in \kappa_L$ are linearly independant over κ_K, the image of α in κ_L is non zero, so $|\alpha|_L = 1$, proving the claim.
- Let $(\lambda_{i,j})_{\substack{1 \leqslant i \leqslant n\\ 1 \leqslant j \leqslant m}}$ be elements in K such that $\sum\limits_{\substack{1 \leqslant i \leqslant n\\ 1 \leqslant j \leqslant m}} \lambda_{i,j} x_i y_j = 0$: we have $\sum\limits_{i=1}^n \alpha_i x_i = 0$ with $\alpha_i = \sum\limits_{j=1}^m \lambda_{i,j} y_j$ for $i \in \{1, \ldots, n\}$. If one among the $\alpha_1, \ldots, \alpha_n$ is non zero, there exist $1 \leqslant i_1 < i_2 \leqslant n$ such that $|\alpha_{i_1} x_{i_1}|_L = |\alpha_{i_2} x_{i_2}|_L > 0$. Then $\alpha_{i_1}, \alpha_{i_2} \neq 0$, so $|\alpha_{i_1}|_L = \max\limits_{1 \leqslant j \leqslant m} |\lambda_{i_1,j}| \in |K^\times|$, and similarly $|\alpha_{i_2}|_L \in |K^\times|$, contradicting the fact that the cosets $|x_{i_1}|\,|K^\times|$ and $|x_{i_2}|_L\,|K^\times|$ are distinct. This implies that we have $\alpha_1 = \cdots = \alpha_n = 0$, whence $\lambda_{i,j} = 0$ for all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$ (since $|\alpha_i| = \max\limits_{1 \leqslant j \leqslant m} |\lambda_{i,j}|$ by what precedes). □

Remark 3.8.3. The theorem implies the finiteness of $e_{L/K}$ and $f_{L/K}$. Note that the inequality in theorem 3.8.2 can be strict.

Theorem 3.8.4. Assume $(K, |.|)$ is complete and $|.|$ is discrete. Then $e_{L/K} f_{L/K} = [L : K]$.

Proof. Put $e = e_{L/K}$ and $f = f_{L/K}$. We know that $|.|_L$ is unique (*cf* theorem 3.5.6). As e is finite and $|.|$ is discrete, so is $|.|_L$: let $\pi_L \in \mathcal{O}_L$ be a uniformizer. As $|L^\times|_L$ and $|K^\times|$ are isomorphic to $\mathbf{Z}$, the quotient group $|L^\times|_L \,/\, |K^\times|$ is cyclic of order e. This implies that $|\pi_L|_L^{e\mathbf{Z}} = |K^\times|$.

Let $y_1, \ldots, y_f \in \mathcal{O}_L$ whose images $\overline{y}_1, \ldots, \overline{y}_f \in \kappa_L$ are linearly independant over κ_K. This implies that $\mathcal{O}_L = y_1\mathcal{O}_K + \cdots + y_f\mathcal{O}_K + \pi_L\mathcal{O}_L$: an immediate induction shows that

$$\mathcal{O}_L = \sum_{\substack{0\leqslant i\leqslant e-1\\1\leqslant j\leqslant f}} \pi_L^i y_j \mathcal{O}_K + \pi_L^e\mathcal{O}_L = \sum_{\substack{0\leqslant i\leqslant e-1\\1\leqslant j\leqslant f}} \pi_L^i y_j \mathcal{O}_K + \pi_K\mathcal{O}_L$$

where π_K is a uniformizer of K. By induction, we have $\mathcal{O}_L = \sum\limits_{\substack{0\leqslant i\leqslant e-1\\1\leqslant j\leqslant f}} \pi_L^i y_j\mathcal{O}_K + \pi_K^n\mathcal{O}_L$ for all $n\in\mathbf{Z}_{>0}$. As $\mathcal{O}_L$ is complete for the π_K-adic topology, we deduce $\mathcal{O}_L = \sum\limits_{\substack{0\leqslant i\leqslant e-1\\1\leqslant j\leqslant f}} \pi_L^i y_j\mathcal{O}_K$, whence $L = \sum\limits_{\substack{0\leqslant i\leqslant e-1\\1\leqslant j\leqslant f}} K\pi_L^i y_j$, so $[L:K] = ef$. □

Proposition 3.8.5. Assume that $(K, |.|)$ is complete, $|.|$ discrete, and let L/K be a finite extension such that κ_L/κ_K is separable. Then there exists $\alpha\in\mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

Proof. • As κ_L/κ_K is separable, there exists $\alpha\in\mathcal{O}_L$ whose image $\overline{\alpha}\in\kappa_L$ is a primitive element, *i.e.* such that $\kappa_L = \kappa_K(\overline{\alpha})$. Let $\pi_L\in\mathcal{O}_L$ be a uniformizer. Put $e = e_{L/K}$ and $f = f_{L/K}$. The proof of previous theorem shows that $\{\pi_L^i\alpha^j\}_{\substack{0\leqslant i<e\\0\leqslant j<f}}$ generates the $\mathcal{O}_K$-module $\mathcal{O}_L$. As $\mathcal{O}_K$ is a DVR hence a PID, the $\mathcal{O}_K$-module $\mathcal{O}_L$ is free (of rank $n = ef$): this shows that $\{\pi_L^i\alpha^j\}_{\substack{0\leqslant i<e\\0\leqslant j<f}}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

• Denote by v_L the normalized valuation on $\mathcal{O}_L$. Let $P\in\mathcal{O}_K[X]$ be a monic polynomial (necessarily of degree f) lifting the minimal polynomial of $\overline{\alpha}$ over $\kappa_K = A/\mathfrak{m}_A$: we have $P(\alpha)\in\mathfrak{m}_L$.

Assume that $v_L(P(\alpha)) > 1$. As κ_L/κ_K is separable, we have $\overline{P}'(\overline{\alpha})\neq 0$ (where $\overline{P}\in\kappa_K[X]$ denotes the image of P mod $\mathfrak{m}_A[X]$), *i.e.* $P'(\alpha)\in\mathcal{O}_L^\times$. Now we have $P(\alpha+\pi_L) = P(\alpha) + P'(\alpha)\pi_L + \beta\pi_L^2$ (where $\beta = \sum\limits_{i=2}^{f} P^{[i]}(\alpha)\pi_L^{i-2}\in\mathcal{O}_L$). As $v_L(P'(\alpha)\pi_L) = 1 < \min\{v_L(P(\alpha)), v_L(\beta\pi_L^2)\}$, we have $v_L(P(\alpha+\pi_L)) = 1$: replacing α by $\alpha+\pi_L$ if necessary, we can assume that $v_L(P(\alpha)) = 1$, *i.e.* that $\pi := P(\alpha)$ is a uniformizer of L.

• As above, $\{\pi^i\alpha^j\}_{\substack{0\leqslant i<e\\0\leqslant j<f}}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. As $\pi^i\alpha^j\in\mathcal{O}_K[\alpha]$ for all $i,j\in\mathbf{Z}_{\geqslant 0}$, this implies that $\mathcal{O}_L\subset\mathcal{O}_K[\alpha]$. The reverse inclusion is trivial since $\alpha\in\mathcal{O}_L$. □

Definition 3.8.6. Assume that $(K, |.|)$ is complete, and let L/K be a finite extension: the absolute value $|.|$ extends uniquely into an absolute value $|.|$ on L.

(1) The extension L/K is *unramified* when κ_L/κ_K is a *separable* extension of degree $[L:K]$. By theorem 3.8.2, this implies that $e_{L/K} = [|L^\times| : |K^\times|] = 1$ (the converse holds automatically when $|.|$ is discrete and κ_K perfect by theorem 3.8.4).

(2) The extension L/K is *totally ramified* when $\kappa_L = \kappa_K$ (*i.e.* $f_{L/K} = 1$).

Theorem 3.8.7. Assume that $(K, |.|)$ is complete, let L/K be a finite extension, and k a subextension of κ_L/κ_K such that k/κ_K is separable. Then there exists a unique subextension M of L/K such that M/K is unramified and $\kappa_M = k$.

Proof. • Existence. By hypothesis, there exists $\overline{\alpha}\in\kappa_L$ such that $k = \kappa_K[\overline{\alpha}]$ and the minimal polynomial $\overline{P}$ of $\overline{\alpha}$ over κ_K is separable, whence $\overline{P}'(\overline{\alpha})\neq 0$. Let $P\in\mathcal{O}_K[X]$ be any monic lift of $\overline{P}$, and $\alpha\in\mathcal{O}_L$ any lift of $\overline{\alpha}$. Put $\varepsilon = |P(\alpha)|\in[0,1[$ (since the image of $P(\alpha)$ in κ_L is $\overline{P}(\overline{\alpha}) = 0$). We have $|P'(\alpha)| = 1$ since the image of $P'(\alpha)$ in κ_L is $\overline{P}'(\overline{\alpha})\neq 0$. As $|P(\alpha)|\leqslant\varepsilon\,|P'(\alpha)|^2$, Newton's lemma (*cf* theorem 3.3.10) implies the existence of a root $\tilde{\alpha}$ of P in L, such that $|\tilde{\alpha}-\alpha|\leqslant\varepsilon\,|P'(\alpha)| = \varepsilon < 1$, so that the image of $\tilde{\alpha}$ in κ_L is $\overline{\alpha}$. Replacing α by $\tilde{\alpha}$, we may assume that $P(\alpha) = 0$. Put $M = K(\alpha)\subset L$. Note that since P is monic and $\overline{P}$ is irreducible in $\kappa_K[X]$, the polynomial P is irreducible in $\mathcal{O}_K[X]$, hence in $K[X]$ (assume $P = P_1P_2$ in $K[X]$: rescaling P_1 and P_2, we can assume that P_1 and P_2 are monic, so that $|P_1|_{\text{Gauss}}\geqslant 1$ and $|P_2|_{\text{Gauss}}\geqslant 1$; as $|P_1|_{\text{Gauss}}|P_2|_{\text{Gauss}} = |P|_{\text{Gauss}} = 1$, we have in fact $|P_1|_{\text{Gauss}} = |P_2|_{\text{Gauss}} = 1$, *i.e.* $P_1, P_2\in\mathcal{O}_K[X]$). This implies that $[M:K] = \deg(P) = \deg(\overline{P}) = [k:\kappa_K]$. As $\overline{\alpha}\in\kappa_M$, we have $k\subset\kappa_M$, whence

$$[M:K] = [k:\kappa_K]\leqslant[\kappa_M:\kappa_K]\leqslant[M:K]$$

(the second inequality follows from theorem 3.8.2), so $\kappa_M = k$ and $[\kappa_M:\kappa_K] = [M:K]$, whence M/K is unramified.

• Unicity. Let M' be an other subextension of L/K such that M'/K is unramified and $\kappa(M') = k$. As $\overline{\alpha}\in k = \kappa(M')$, Newton's lemma (*cf* theorem 3.3.10) applied to $P\in M'[X]$ provides a root $\beta\in M'$ of P, whose image in $\kappa(M')$ is $\overline{\alpha}$. Then we have $0 = P(\beta) - P(\alpha) = \sum\limits_{i=1}^{\deg(P)}(\beta-\alpha)^iP^{[i]}(\alpha)$. If $\beta\neq\alpha$, we can divide this equality by $\beta-\alpha$, and get $0 = P'(\alpha) + \sum\limits_{i=2}^{\deg(P)} (\beta-\alpha)^{i-1}P^{[i]}(\alpha)$. As $P^{[i]} \in \mathcal{O}_K[X]$ for all $i \in \mathbf{Z}_{>0}$ and $\alpha, \beta \in \mathcal{O}_L$, we have $P'(\alpha) \in (\beta-\alpha)\mathcal{O}_L$, thus $|P'(\alpha)| < 1$ since $\beta - \alpha \in \mathfrak{m}_L$ (because β and α both lift $\overline{\alpha}$). This contradicts the fact that $|P'(\alpha)| = 1$: we have $\beta = \alpha$, so that $M = K(\alpha) \subset M'$. As $[M' : K] = [k : \kappa_K] = [M : K]$, we have $M' = M$. □

Proposition 3.8.8. Under the assumptions of theorem 3.8.7, if $\alpha \in \mathcal{O}_M$ maps to $\overline{\alpha} \in k$ such that $k = \kappa_K(\overline{\alpha})$, then $\mathcal{O}_M = \mathcal{O}_K[\alpha]$. Moreover, if $x = \sum\limits_{i=0}^{d-1} \lambda_i\alpha^i \in M = K(\alpha)$ (with $d = [M : K]$ and $\lambda_0, \ldots, \lambda_{d-1} \in K$), then $|x| = \max\limits_{0 \leqslant i < d} |\lambda_i|$.

Proof. We have $\alpha \in M$ thus $K(\alpha) \subset M$, and $k \subset \kappa_{K(\alpha)}$, thus $[M : K] = [k : \kappa_K] \mid [K(\alpha) : K] \mid [M : K]$: this implies that $[K(\alpha) : K] = [M : K]$, *i.e.* $M = K(\alpha)$. Let $x = \sum\limits_{i=0}^{d-1} \lambda_i\alpha^i \in M$ with $\lambda_0, \ldots, \lambda_{d-1} \in K$. Fix $i_0 \in \{0, \ldots, d-1\}$ such that $|\lambda_{i_0}| = \max\limits_{0 \leqslant i < d} |\lambda_i|$: if $x \neq 0$, we have $\lambda_{i_0} \neq 0$. Then $\lambda_{i_0}^{-1}x = \sum\limits_{i=0}^{d-1} \lambda_{i_0}^{-1}\lambda_i\alpha^i \in \mathcal{O}_K[\alpha]$ because $|\lambda_{i_0}^{-1}\lambda_i| \leqslant 1$, with equality for $i = i_0$: as $(1, \overline{\alpha}, \overline{\alpha}^2, \ldots, \overline{\alpha}^{d-1})$ is a basis of k over κ_K, this implies that the image of $\lambda_{i_0}^{-1}x$ in $\kappa_M = k$ is not zero, whence $|\lambda_{i_0}^{-1}x| = 1$, *i.e.* $|\lambda_{i_0}| = |x|$, proving the second assertion. If $x \in \mathcal{O}_M$, this implies that $|\lambda_i| \leqslant |x| \leqslant 1$ *i.e.* $\lambda_i \in \mathcal{O}_K$ for all $i \in \{0, \ldots, d-1\}$, so that $x \in \mathcal{O}_K[\alpha]$: we have $\mathcal{O}_M \subset \mathcal{O}_K[\alpha]$. The reverse inclusion is obvious. □

Corollary 3.8.9. Assume that $(K, |.|)$ is complete, and let L/K be a finite extension such that κ_L/κ_K is separable. There exists a unique subextension T of L/K such that T/K is unramified and L/T is totally ramified. If M is a subextension of L/K such that M/K is unramified, then $M \subset T$. Conversely, any subextension M of T/K is unramified over K.

Proof. By theorem 3.8.7 applied to $k = \kappa_L$, there exists a unique subextension T of L/K such that T/K is unramified and $\kappa_T = \kappa_L$. This last property means that L/T is totally ramified.

Let M be a subextension of L/K such that M/K is unramified. Theorem 3.8.7 applied to the extension T/K and $k = \kappa_M$ implies that there exists a unique subextension M' of T/K such that M'/K is unramified and $\kappa_{M'} = \kappa_M$. Similarly, it implies that M is the unique subextension of L/K such that M/K is unramified and whose residue field is κ_M: by unicity, we have $M' = M$, so that $M \subset T$.

If M is a subextension of T/K, we have $[\kappa_T : \kappa_M] \leqslant [T : M]$ and $[\kappa_M : \kappa_K] \leqslant [M : K]$. The product of these inequalities is the equality $[\kappa_T : \kappa_K] = [T : K]$: these inequalities must be equalities, in particular $[\kappa_M : \kappa_K] = [M : K]$. As κ_M/κ_K is separable since κ_T/κ_K is, the extension M/K is unramified. □

Definition 3.8.10. The subextension T of L/K is called the *maximal unramified subextension*[34] of L/K.

Corollary 3.8.11. Under the assumptions of corollary 3.8.9, if M_1 and M_2 are two subextensions of L/K that are unramified over K, their compositum M_1M_2 is unramified over K.

Theorem 3.8.12. Assume that $(K, |.|)$ is complete, and let L/K be a finite Galois extension such that κ_L/κ_K is separable. Then κ_L/κ_K is Galois, and there exists a natural, surjective group homomorphism $\mathsf{Gal}(L/K) \to \mathsf{Gal}(\kappa_L/\kappa_K)$, whose kernel is $\mathsf{Gal}(L/T)$, where T is the maximal unramified subextension of L/K. It induces a group isomorphism $\mathsf{Gal}(T/K) \xrightarrow{\sim} \mathsf{Gal}(\kappa_L/\kappa_K)$.

Proof. As we have seen during the proof of theorem 3.8.7, if $\overline{\alpha} \in \kappa_L$ is such that $\kappa_L = \kappa_K(\overline{\alpha})$, and if $P \in \mathcal{O}_K[X]$ is any monic polynomial lifting the minimal polynomial $\overline{P} \in \kappa_K[X]$ of $\overline{\alpha}$ over κ_K, then P is irreducible in $K[X]$, has a unique root $\alpha \in L$ lifting $\overline{\alpha}$, and $T = K(\alpha)$.

- As L/K is Galois and $P(\alpha) = 0$, the polynomial P is split in $L[X]$ with simple roots in L (since α is separable over K since L is): we can write $P(X) = \prod\limits_{i=1}^{d} (X - \alpha_i)$, where $\alpha = \alpha_1, \ldots, \alpha_d$ are pairwise distinct elements in L. If $i \in \{1, \ldots, d\}$, there exists $\sigma \in \mathsf{Gal}(L/K)$ such that $\alpha_i = \sigma(\alpha)$, which implies that $|\alpha_i| = |\sigma(\alpha)| = |\alpha|$, so that $\alpha_i \in \mathcal{O}_L$: let $\overline{\alpha_i}$ be its image in κ_L. The factorization above induces the factorization $\overline{P}(X) = \prod\limits_{i=1}^{d} (X - \overline{\alpha}_i)$. This implies in particular that $\kappa_L = \kappa_K(\overline{\alpha})$ is a splitting field for $\overline{P}$ over κ_K: as $\overline{P}$ is separable over κ_K (since α is, because κ_L/κ_K is), the extension κ_L/κ_K is Galois.
- Let $\sigma \in \mathsf{Gal}(L/K)$. We have $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ and $\sigma(\mathfrak{m}_L) = \mathfrak{m}_L$ (because σ is an isometry by unicity of the absolute value on L extending $|.|$ on K). This implies that σ induces a ring homomorphism $\overline{\sigma}\colon \kappa_L \to \kappa_L$,

[34] *Trägheitskörper* in German.

i.e. a field automorphism of κ_L. As $\sigma_{|K} = \mathsf{Id}_K$, we have $\overline{\sigma}_{|\kappa_K} = \mathsf{Id}_{\kappa_K}$, so that $\overline{\sigma} \in \mathsf{Gal}(\kappa_L/\kappa_K)$. The induced map $\mathsf{Gal}(L/K) \to \mathsf{Gal}(\kappa_L/\kappa_K)$ is obviously a group homomorphism.

- Let $\gamma \in \mathsf{Gal}(\kappa_L/\kappa_K)$: there exists $i \in \{1, \ldots, d\}$ such that $\gamma(\overline{\alpha}) = \overline{\alpha}_i$ (since the conjugates of $\overline{\alpha}$ over κ_K are $\overline{\alpha}_1, \ldots, \overline{\alpha}_d$ because $\overline{P}$ is irreducible). As α and α_i are conjugate over K (being roots of the irreducible polynomial P), there exists $\sigma \in \mathsf{Gal}(L/K)$ such that $\sigma(\alpha) = \alpha_i$. This implies that γ and $\overline{\sigma}$ coincide on $\overline{\alpha}$: they are equal since $\kappa_L = \kappa_K(\overline{\alpha})$. This shows the surjectivity of the map $\mathsf{Gal}(L/K) \to \mathsf{Gal}(\kappa_L/\kappa_K)$.
- Let $\sigma \in \mathsf{Gal}(L/K)$ be such that $\overline{\sigma} = \mathsf{Id}_{\kappa_L}$. This implies that $\sigma(\alpha)$ maps to $\overline{\alpha}$ in κ_L. As the only root of P lifting $\overline{\alpha}$ is α, we have $\sigma(\alpha) = \alpha$, and $\sigma \in \mathsf{Gal}(L/T)$. The converse is obvious.
- As $\mathsf{Gal}(L/T) = \mathsf{Ker}(\mathsf{Gal}(L/K) \to \mathsf{Gal}(\kappa_L/\kappa_K))$, the subgroup $\mathsf{Gal}(L/T)$ is normal in $\mathsf{Gal}(L/K)$, so that T/K is Galois (a fact that can be checked directly by observing that $T = K(\alpha)$ contains all the conjugates $\alpha_1, \ldots, \alpha_d$ of α over K), thus $\mathsf{Gal}(T/K) \xrightarrow{\sim} \mathsf{Gal}(\kappa_L/\kappa_K)$ passing to the quotient. □

Definition 3.8.13. Under the assumptions of theorem 3.8.12, the subgroup $I_{L/K} := \mathsf{Gal}(L/T)$ is normal in $\mathsf{Gal}(L/K)$. It is called the *inertia subgroup* of the extension L/K. We thus have an exact sequence

$$\{1\} \to I_{L/K} \to \mathsf{Gal}(L/K) \to \mathsf{Gal}(\kappa_L/\kappa_K) \to \{1\}$$

Proposition 3.8.14. Assume that $(K, |.|)$ is complete, and let L/K and L'/K two finite and unramified extensions. The natural map

$$\mathsf{Hom}_{K\text{-alg}}(L, L') \to \mathsf{Hom}_{\kappa_K\text{-alg}}(\kappa_L, \kappa_{L'})$$

is a bijection.

Proof. • The extension κ_L/κ_K is finite and separable: there exists $\overline{\alpha} \in k$ such that $k = \kappa_K(\overline{\alpha})$ (primitive element theorem). Let $\overline{P} \in \kappa_K[X]$ be the minimal polynomial of $\overline{\alpha}$ over κ_K, and $P \in \mathcal{O}_K[X]$ a monic lifting of $\overline{P}$. As $\overline{\alpha}$ is separable over κ_K, we have $\overline{P}'(\overline{\alpha}) \neq 0$: we can apply Newton's lemma (*cf* theorem 3.3.10), so there exists a unique element $\alpha \in \mathcal{O}_L$ mapping to $\overline{\alpha}$ in κ_L and such that $P(\alpha) = 0$.

- Let $\sigma \in \mathsf{Hom}_{K\text{-alg}}(L, L')$: we have $\sigma(\mathcal{O}_L) \subset \mathcal{O}_{L'}$, so that σ induces a morphism $\overline{\sigma}\colon \kappa_L \to \kappa_{L'}$ of κ_K-algebras. As $P(\alpha) = 0$ in L, we have $P(\sigma(\alpha)) = 0$ in L' as well (since $P \in \mathcal{O}_K[X]$). The image of $\sigma(\alpha)$ in $\kappa_{L'}$ coincides with $\overline{\sigma}(\overline{\alpha})$. Again, we can apply Newton's lemma to P in $\mathcal{O}_{L'}$: the unicity implies that $\sigma(\alpha)$ is the unique element $\alpha' \in \mathcal{O}_{L'}$ mapping to $\overline{\sigma}(\overline{\alpha})$ in $\kappa_{L'}$ and such that $P(\alpha') = 0$. This shows that there is a bijection between the possible values for $\overline{\sigma}(\overline{\alpha})$ (these are the roots of $\overline{P}$ in $\kappa_{L'}$) and the possible values for $\sigma(\alpha)$ (these are the roots of P in L'). As $\overline{\sigma}$ and σ are uniquely determined by $\overline{\sigma}(\overline{\alpha})$ and $\sigma(\alpha)$ respectively, this proves the bijectivity. □

Theorem 3.8.15. Assume that $(K, |.|)$ is complete, and let k/κ_K be a finite and separable extension. There exists a finite unramified extension L/K such that $\kappa_L \simeq k$. This extension is unique up to isomorphism.

Proof. • As k/κ_K is finite and separable, there exists $\overline{\alpha} \in k$ such that $k = \kappa_K(\overline{\alpha})$ (primitive element theorem): let $\overline{P} \in \kappa_K[X]$ be its minimal polynomial over κ_K. Let $P \in \mathcal{O}_K[X]$ be any monic lift of $\overline{P}$: as $\overline{P}$ is irreducible in $\kappa_K[X]$, so is P in $\mathcal{O}_K[X]$, hence in $K[X]$. This implies that $L = K[X]/\langle P(X)\rangle$ is a finite field extension of K, and that $[L : K] = [k : \kappa_K]$. Put $A = \mathcal{O}_K[X]/\langle P(X)\rangle$: as $P \in \mathcal{O}_K[X]$, the inclusion $\mathcal{O}_K \subset K[X]$ induces a morphism of $\mathcal{O}_K$ algebras $A \to \mathcal{O}_L$, whence a morphism of κ_K-algebras $\kappa_K[X]/\langle\overline{P}\rangle \to \mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$. Composed with the canonical map $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L \to \kappa_L$, we deduce a morphism $k \to \kappa_L$ of extensions of κ_K. This implies in particular that $[\kappa_L : \kappa_K] \geqslant [k : \kappa_K] = [L : K]$: we must have $[\kappa_L : \kappa_K] = [k : \kappa_K] = [L : K]$, so that the map $k \to \kappa_L$ is an isomorphism, and L/K is unramified.

- The unicity follows from proposition 3.8.14. □

Corollary 3.8.16. Assume that $(K, |.|)$ is complete. The functor $L \mapsto \kappa_L$ is an equivalence of categories between the category of finite unramified extensions of K and that of finite and separable extensions of κ_K.

Proof. This is proposition 3.8.14 and theorem 3.8.15. □

Remark 3.8.17. The preceding statement is a special case of a very general result (on finite étale coverings of schemes).

3.8.18. *The case of a finite residue fields.* Here we assume that $(K, |.|)$ is a non archimedean complete valued field, such that $\kappa_K = \mathbf{F}_q$ is a finite field (so that q is a power of a prime p). If L/K is a finite extension, then κ_L/κ_K is a finite extension of degree f, so $\kappa_L = \mathbf{F}_{q^f} = \mathbf{F}_q\left(\overline{\zeta}_{q^f-1}\right)$, where $\overline{\zeta}_{q^f-1}$ is a primitive $(q^f - 1)$-th root of unity, *i.e.* a root of the separable polynomial $\Phi_{q^f-1}(X)$, the latter has a root in L, and T is a splitting field of $\Phi_{q^f-1}(X)$: we have $T = K(\zeta_{q^f-1})$ where ζ_{q^f-1} is a (any) primitive $(q^f - 1)$-th root of unity in L.

The extension κ_L/κ_K being Galois, T/K is Galois as well, and $\mathsf{Gal}(T/K) \xrightarrow{\sim} \mathsf{Gal}(\mathbf{F}_{q^f}/\mathbf{F}_q)$ is cyclic of order f, generated by the Frobenius automorphism $\overline{\varphi}$ defined by $\overline{\varphi}(x) = x^q$ for all $x \in \mathbf{F}_{q^f}$. This means that $\mathsf{Gal}(T/K)$ is generated by the Frobenius automorphism φ, which is characterized by

$$\varphi(x) \equiv x^q \mod \mathfrak{m}_T$$

for all $x \in T$. Note that by unicity of lifts of roots of $X^{q^f-1} - 1$ in T, we have $\varphi(\zeta_{q^f-1}) = \zeta_{q^f-1}^q$.

Proposition 3.8.19. Let $\overline{K}$ be an algebraic closure of K. For $f \in \mathbf{Z}_{>0}$, there exists a unique subextension K_f of $\overline{K}/K$ which is unramified and whose residue field is $\mathbf{F}_{q^f}$.

By what theorem 3.8.15, K_f is the splitting field of $X^{q^f} - X$ in $\overline{K}$.

Notation. We denote by $\mathbf{Q}_q$ the unique unramified extension of $\mathbf{Q}_p$ (in some fixed algebraic closure of $\mathbf{Q}_p$) whose residue field is $\mathbf{F}_q$. Its ring of integers is denoted $\mathbf{Z}_q$.

Definition 3.8.20. (Teichmüller representatives) Let $\overline{\mathbf{Q}}_p$ be an algebraic closure of $\mathbf{Q}_p$. If $f \in \mathbf{Z}_{>0}$ and $x \in \mathbf{F}_{p^f}$, then x is a root of the polynomial $X^{p^f} - X$. As the latter is separable modulo p, Newton's lemma (*cf* theorem 3.3.10) implies that there is a unique element $[x] \in \mathbf{Z}_{p^f}$ which is a root of $X^{p^f} - X$, and whose image in $\mathbf{F}_{p^f}$ is x. Put together, those maps provide a canonical map

$$[.] \colon \overline{\mathbf{F}}_p \to \mathcal{O}_{\overline{\mathbf{Q}}_p}$$

which is a section of the canonical projection $\mathcal{O}_{\overline{\mathbf{Q}}_p} \to \overline{\mathbf{F}}_p$. Note that by unicity, we have $[xy] = [x][y]$ for all $x, y \in \overline{\mathbf{F}}_p$. The element $[x]$ is called the *Teichmüller* (or *multiplicative*) representative of x.
Of course, we have $[0] = 0$ and $[1] = 1$. If x generates $\mathbf{F}_{p^f}$, then x is a primitive $(p^f - 1)$-th root of unity in $\overline{\mathbf{F}}_p$, hence $[x]$ is a primitive $(p^f - 1)$-th root of unity in $\overline{\mathbf{Q}}_p$.

3.8.21. *Totally ramified extensions.* If L/K is a finite extension whose residual extension κ_L/κ_K is separable, there is a unique subextension T of L/K such that T/K is unramified with residue field κ_L, and L/T is totally ramified. We have $[T : K] = f_{L/K}$, whence $[L : T] = e_{L/K}$ (because $[L : K] = e_{L/K} f_{L/K}$ by theorem 3.8.4). As unramified finite extensions are well understood by corollary 3.8.9 and theorem 3.8.12, we now explain the structure of totally ramified finite extensions, in the case where the value group $|K^\times|$ is *discrete.*
We henceforth assume that $(K, |.|)$ is a *complete and discrete* non archimedean valued field.
Let $\overline{K}$ be a fixed algebraic closure of K and $E(X) = X^e + a_1 X^{e-1} + \cdots + a_{e-1}X + a_e \in K[X]$ an *Eisenstein polynomial, i.e.* such that $a_i \in \mathfrak{m}_K$ for all $i \in \{1, \ldots, e\}$ and $a_e \in \mathfrak{m}_K \backslash \mathfrak{m}_K^2$ (in other words $v_K(a_i) > 0$ for $i \in \{1, \ldots, e\}$ and $v_K(a_e) = v_K(\pi_K)$). Let $\Pi \in \overline{K}$ be a root of E and $L = K(\Pi)$. As $[L : K] = e$ is finite, $|.|$ extends uniquely to L by theorem 3.5.6 (*i.e.* v_K extends uniquely into a valuation v_L on L).

Lemma 3.8.22. The extension L/K is totally ramified, Π is a uniformizer of L and $\mathcal{O}_L = \mathcal{O}_K[\Pi]$.

Proof. • Note that L is complete since it is finite dimensional over K (*cf* theorem 3.4.12). As $P(\Pi) = 0$, we have $\Pi \in \mathcal{O}_L$, and

$$(*) \qquad \Pi^e = u\pi_K$$

where $u = -\frac{1}{\pi_K}\big(a_e + a_{e-1}\Pi + \cdots + a_1\Pi^{e-1}\big)$. For $i \in \{1, \ldots, e\}$, we have $\left|\frac{a_i\Pi^{e-i}}{\pi_K}\right| \leqslant 1$ since $|a_i| \leqslant |\pi_K|$ (because $a_i \in \mathfrak{m}_K = \pi_K\mathcal{O}_K$) and $|\Pi| \leqslant 1$ since $\Pi \in \mathcal{O}_L$. This implies that $u \in \mathcal{O}_L$: equation $(*)$ implies that $|\Pi|^e = |u|\,|\pi_K| < 1$, showing that $\Pi \in \mathfrak{m}_L$. This implies that $\left|\frac{a_i\Pi^{e-i}}{\pi_K}\right| < 1$ if $i \in \{1, \ldots, e-1\}$. On the other hand, we have $\left|\frac{a_e}{\pi_K}\right| = 1$ because $a_e \in \pi_K\mathcal{O}_K^\times$ (since E is an Eisenstein polynomial). As $\left|\frac{a_e}{\pi_K}\right| > \left|\frac{a_i\Pi^{e-i}}{\pi_K}\right|$ for all $i \in \{1, \ldots, e-1\}$, we have $|u| = \max\limits_{1 \leqslant i \leqslant e}\left|\frac{a_i\Pi^{e-i}}{\pi_K}\right| = 1$, so that $u \in \mathcal{O}_L^\times$. This implies that $|\Pi| = |\pi_K|^{1/e}$, showing that $\sqrt[e]{|K^\times|} \subset |L^\times|$, whence $[|L^\times| : |K^\times|] \geqslant e = [L : K]$. By theorem 3.8.4, this implies that L/K is totally ramified, and $|L^\times| = |\Pi|^{\mathbf{Z}} = \sqrt[e]{|K^\times|}$. In particular, Π is a uniformizer of L.
• As $\Pi \in \mathcal{O}_L$, we have $\mathcal{O}_K[\Pi] \subset \mathcal{O}_L$. Conversely, let $x \in \mathcal{O}_L \backslash \{0\}$. As $(1, \Pi, \Pi^2, \ldots, \Pi^{e-1})$ is a K-basis of L, we can write $x = \lambda_0 + \lambda_1\Pi + \cdots + \lambda_{e-1}\Pi^{e-1}$ with $\lambda_0, \ldots, \lambda_{e-1} \in K$. If $0 \leqslant i < j < e$ are integers, we have $|\lambda_i\Pi^i| \neq |\lambda_j\Pi^j|$ unless $\lambda_i = \lambda_j = 0$, because $|\Pi|^{j-i} \notin |K^\times|$. This implies that $|x| = \max\limits_{0 \leqslant i < e}|\lambda_i|\,|\Pi|^i$. As $x \in \mathcal{O}_L$, have thus $|\lambda_i|\,|\Pi|^i \leqslant 1$, *i.e.* $|\lambda_i| \leqslant |\Pi|^{-i} < |\pi_K|^{-1}$ for all $i \in \{0, \ldots, e-1\}$, *i.e.* $|\lambda_i| \leqslant 1$ *i.e.* $\lambda_i \in \mathcal{O}_K$ for all $i \in \{0, \ldots, e-1\}$, hence $x \in \mathcal{O}_K[\Pi]$. □

Theorem 3.8.23. A finite extension L/K is totally ramified if and only if $L = K(\pi_L)$, where π_L is a uniformizer of L, and a root of an Eisenstein polynomial over K. Then $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

Proof. • Assume L/K is totally ramified, and let π_L a uniformizer of L. We have $|L^\times| = |\pi_L|^{\mathbf{Z}}$ and $|K^\times| = |\pi_K|^{\mathbf{Z}}$: as $[|L^\times| : |K^\times|] = e := [L : K]$, we have $|\pi_K| = |\pi_L|^e$. The family $(1, \pi_L, \pi_L^2, \ldots, \pi_L^{e-1})$ is linearly independent over K: if we had a non trivial relation $\lambda_0 + \lambda_1\pi_L + \cdots + \lambda_{e-1}\pi_L^{e-1} = 0$ with $\lambda_0, \ldots, \lambda_{e-1} \in K$, there would be $0 \leqslant i < j < e$ integers such that $0 < \left|\lambda_i\pi_L^i\right| = \left|\lambda_j\pi_L^j\right|$, contradicting the fact that ${\pi_L}^{j-i} \notin |K^\times|$. This implies that $(1, \pi_L, \pi_L^2, \ldots, \pi_L^{e-1})$ is a basis of L over K, so that $L = K(\pi_L)$. Let $E(X) = X^e + a_1X^{e-1} + \cdots + a_{e-1}X + a_e \in K[X]$ be the minimal polynomial of π_L over K. As π_L belongs to $\mathcal{O}_L$, it is integral over $\mathcal{O}_K$ (*cf* corollary 3.5.10): we have $E(X) \in \mathcal{O}_K[X]$. If $i \in \{1, \ldots, e\}$, the coefficient a_i is, up to the sign, the i-th elementary symmetric polynomial in the conjugates of π_L. Since all of these belong to $\mathfrak{m}_N$ (where N is a normal closure of L/K), we have $a_i \in \mathfrak{m}_N \cap K = \mathfrak{m}_K$. Moreover, the constant term satisfies $a_e = \pm\mathsf{N}_{L/K}(\pi_L)$, so that $|a_e| = \left|\mathsf{N}_{L/K}(\pi_L)\right| = |\pi_L|^e = |\pi_K|$ (*cf* proposition 3.5.9), which shows that E is an Eisenstein polynomial.
• The converse and the statement on $\mathcal{O}_L$ are nothing but lemma 3.8.22. □

3.8.24. *Tame and wild ramification.* Here again, we assume that $(K, |.|)$ is a *complete and discrete* non archimedean valued field.

Definition 3.8.25. A finite extension L/K is *tamely ramified* when its residual extension is separable and $e_{L/K}$ is prime to $\mathsf{char}(\kappa_K)$, and *wildly ramified* otherwise.

Remark 3.8.26. When $\mathsf{char}(\kappa_K) = 0$, every finite extension is tamely ramified.

In what follows, we put $p = \mathsf{char}(\kappa_K)$ if $\mathsf{char}(\kappa_K) > 0$ and $p = 1$ if $\mathsf{char}(\kappa_K) = 0$.

Lemma 3.8.27. Let L/K be a totally ramified extension. Write $[L : K] = p^r m$ with $\mathsf{gcd}(p, m) = 1$. It $z \in L$ is such that $z^m = 1$, then $z \in K$.

Proof. Put $e = [L : K]$, and let π_L be a uniformizer of L: we have $\mathcal{O}_L = \bigoplus\limits_{i=0}^{e-1} \mathcal{O}_K\pi_L^i$. As $|z| = 1$, we have $z \in \mathcal{O}_L$: there exists a unique $y \in \mathcal{O}_K$ such that $z - y \in \bigoplus\limits_{i=1}^{e-1} \mathcal{O}_K\pi_L^i$: we have $|z - y| \leqslant |\pi_L|$, so in particular $|y| = 1$. Let $P(X) = X^m - 1 \in \mathcal{O}_K[X]$. We have $|P(y)| = |P(y) - P(z)| = |y^m - z^m| \leqslant |y - z| \leqslant |\pi_L|$. On the other hand, we have $P'(y) = my^{m-1}$, so that $|P'(y)| = 1$ since $\mathsf{gcd}(p, m) = 1$ and $|y| = 1$. Newton's lemma (*cf* theorem 3.3.10) implies that there exists a unique element $\widetilde{y} \in K$ such that $P(\widetilde{y}) = 0$ and $|\widetilde{y} - y| \leqslant |\pi_L|$. This implies that $|\widetilde{y} - z| \leqslant |\pi_L|$. Applying unicity in L then shows that $z = \widetilde{y} \in K$. □

Theorem 3.8.28. Let L/K be a totally ramified extension of degree $e = p^r m$ with $\mathsf{gcd}(p, m) = 1$. There exists a unique subextension V of L/K such that V/K is tamely ramified and $[L : V] = p^r$. Moreover, there exists a uniformizer π of K such that $V = K(\sqrt[m]{\pi})$.

Proof. • Existence of V. Let π_K (resp. π_L) be a uniformizer in K (resp. L). As the extension L/K is totally ramified, we have $\mathcal{O}_L = \bigoplus\limits_{i=0}^{e-1} \mathcal{O}_K\pi_L^i$, and $\pi_L^e = u\pi_K$, with $u \in \mathcal{O}_L^\times$. As $\kappa_L = \kappa_K$, there exists $u_0 \in \mathcal{O}_K^\times$ such that u and u_0 have same image in κ_L, so that $z = \frac{u}{u_0} \in \mathcal{O}_L$ satisfies $|z - 1| < 1$.
Now let $P(X) = X^m - z \in \mathcal{O}_L[X]$: as $|z - 1| < 1$, we have $|P(1)| < 1$. Also, $|P'(1)| = |m| = 1$ since $\mathsf{gcd}(p, m) = 1$: by Newton's lemma (*cf* theorem 3.3.10), there exists a unique $w \in \mathcal{O}_L$ such that $P(w) = 0$ and $|w - 1| \leqslant |P(1)| = |z - 1|$. We thus have $\pi_L^{p^r m} = u_0w^m\pi_K$, so that $\pi_V := \frac{\pi_L^{p^r}}{w} \in \mathcal{O}_L$ is such that $\pi_V^m = u_0\pi_K =: \pi$ is a uniformizer of K. Let $V = K(\pi_V)$: as π_V is a root of the Eisenstein polynomial $X^m - \pi \in \mathcal{O}_K$, we have $[V : K] = m$: the extension V/K is tamely ramified, and $[L : V] = \frac{[L:K]}{[V:K]} = p^r$.
• Unicity of V. Let V' be a subextension of L/K such that $[V : K] = m$. Applying the construction above inside V' instead of L provides an element $\pi_{V'} \in V'$ such that $\pi_{V'}^m$ is a uniformizer of K: if $x = \frac{\pi_{V'}}{\pi_V} \in \mathcal{O}_L$, we have $\lambda := x^m \in \mathcal{O}_K^\times$. There exists $y \in \mathcal{O}_K$ such that $|x - y| \leqslant |\pi_L|$, then $|y^m - x^m| \leqslant |\pi_L|$, *i.e.* $|Q(y)| \leqslant |\pi_L|$, where $Q(X) = X^m - \lambda \in \mathcal{O}_K$. As $|Q'(y)| = \left|my^{m-1}\right| = 1$ (since $\mathsf{gcd}(p, m) = 1$ and $|y| = |x| = 1$), Newton's lemma again provides an element $\widetilde{y} \in \mathcal{O}_K^\times$ such that $\widetilde{y}^m = \lambda$. If $z = \frac{x}{y} \in \mathcal{O}_L$, we have $z^m = 1$. Lemma 3.8.27 implies that $z \in \mathcal{O}_K^\times$, so that $x = \widetilde{y}z \in \mathcal{O}_K^\times$, showing that $\pi_{V'} \in V$, whence $V' = V$. □

Remark 3.8.29. In the previous theorem, one cannot take any uniformizer π.

Definition 3.8.30. Let L/K be a finite field extension such that κ_L/κ_K is separable. Let L/K be a finite extension whose residual extension is separable. What precedes shows that there are unique subextensions

$T \subset V$ such that T/K is unramified, L/T is totally ramified, V/K is tamely ramified and L/V is totally ramified of degree a power of p.

$$\begin{tikzcd} K \arrow[r, dash, "\text{unramified}"'] & T \arrow[r, dash, "\text{tame}"'] \arrow[rr, dash, bend left, "\text{totally ramified}"] & V \arrow[r, dash, "\text{wild}"'] & L \end{tikzcd}$$

The subextension V of L/K is the maximal subextension of L/K which is tamely ramified over K: it is called the *maximal tamely ramified subextension*[35] of L/K. Note that by theorem 3.8.28, there exists a uniformizer π of T such that $V = T(\sqrt[m]{\pi})$, where $e_{L/K} = p^r m$ and $\mathsf{gcd}(p, m) = 1$. Note that in general, one may not take π in K.

3.9. **Exercises.**

Exercise 3.9.1. Let k be a finite field. Show that the only absolute value on k is the trivial one.

Exercise 3.9.2. Let $(K, |.|)$ be a valued field.
(1) Show that if $|.|$ is non archimedean, then $|.|^\gamma$ is an absolute value for all $\gamma \in \mathbf{R}_{>0}$.
(2) Show that if $|.|$ is archimedean, then $|.|^\gamma$ is an absolute value for all $\gamma \in]0, 1]$.
(3) What are the $\gamma \in \mathbf{R}_{>0}$ such that $|.|_\infty^\gamma$ is an absolute value on $\mathbf{Q}$?

Exercise 3.9.3. Let p and q be two distinct prime numbers. Show that the absolute values $|.|_p$ and $|.|_q$ are not equivalent. Show also that $|.|_p$ and $|.|_\infty$ are not equivalent.

Exercise 3.9.4. (Incompleteness of $\mathbf{Q}$). Let $(K, |.|)$ be a complete valued field, such that $|.|$ is non trivial. Using Baire's theorem, show that K is uncountable. Deduce that $\mathbf{Q}$ is non complete any of its non trivial absolute values.

Exercise 3.9.5. Let $(K, |.|)$ be a non archimedean valued field. Show that $\mathsf{Card}(K) \leqslant \mathsf{Card}(\kappa_K)^{\mathsf{Card}(|K^\times|)}$.

Exercise 3.9.6. Let p be a prime number. Show that $\mathbf{Q}_p$ is not algebraically closed.

Exercise 3.9.7. Show that $\mathbf{Q}_p/\mathbf{Z}_p \simeq \mathbf{Z}[p^{-1}]/\mathbf{Z}$.

Exercise 3.9.8. Show that if $p \neq 2$, then 1 is the only p-th root of unity in $\mathbf{Q}_p$.

Exercise 3.9.9. (Approximation). Let K be a field.
(1) Let $|.|$ and $|.|'$ be two absolute values on K. Show that the following are equivalent:

(i) $|.|$ and $|.|'$ are equivalent;
(ii) for all $x \in K$, we have $|x| < 1 \Leftrightarrow |x|' < 1$.

Let $v_0, \ldots, v_n$ be pairwise distinct places, and $|.|_1, \ldots, |.|_n$ absolute values representing $v_1, \ldots, v_n$.
(2) Show by induction on $n \in \mathbf{Z}_{>0}$ that there exists $x \in K$ such that $|x|_0 > 1$ and $|x|_i < 1$ for $i \in \{1, \ldots, n\}$.
(3) Deduce that the diagonal morphism $K \to \prod\limits_{i=1}^{n} K_{v_i}$ has dense image, where K_{v_i} denotes the field K endowed with the topology defined by v_i.

Exercise 3.9.10. Let K be a field, $r_1, \ldots, r_n \in \mathbf{R}$ and $|.|_1, \ldots, |.|_n$ non-trivial inequivalent absolute values on K. Assume that $|x|_1^{r_1} \cdots |x|_n^{r_n} = 1$ for all $x \in K^\times$. Prove that $r_1 = \cdots = r_n = 0$ (in other words, there is no finite product formula).

Exercise 3.9.11. Let $(K, |.|)$ be a valued field.
(1) Show that the following are equivalent:

(i) $|.|$ is ultrametric;
(ii) $|n| \leqslant 1$ for all $n \in \mathbf{Z}$.
(iii) $|2| \leqslant 1$.

[Hint: to prove (ii)$\Rightarrow$(i), use the binomial expansion.]
(2) Deduce that if $\mathsf{char}(K) \neq 0$, then every absolute value on K is ultrametric.

[35] *Verzweigungskörper* in German.

Exercise 3.9.12. Let K be a field, $|.|$ a nontrivial non archimedean absolute value on K, and $\mathcal{O}_K$ its ring of integers.
(1) Show that $\mathcal{O}_K$ is integrally closed.
(2) Show that the following are equivalent:

(i) $\mathcal{O}_K$ is a DVR;
(ii) $\mathcal{O}_K$ is noetherian;
(iii) the maximal ideal $\mathfrak{m}_K := \{x \in K\,;\,|x| < 1\}$ is principal;
(iv) $|K^\times|$ is a discrete subgroup of $\mathbf{R}_{>0}$.

Exercise 3.9.13. Let K be a field. A subring $A \subset K$ is a *valuation ring* of K when $(\forall x \in K)\, x \notin A \Rightarrow x^{-1} \in A$ (this implies in particular that $K = \mathsf{Frac}(A)$).
(1) Show if A is a valuation ring of K and I, J are ideals in A, then either $I \subset J$ or $J \subset I$. Deduce that A is local (we denote henceforth its maximal ideal by $\mathfrak{m}_A$).
(2) Let F be a field, $A = F[\![X,Y]\!]$ the ring of formal series and $K = F(\!(X,Y)\!) = \mathsf{Frac}(A)$ the field of formal Laurent series. Is the local ring A a valuation ring of K?
(3) Show that a valuation ring of K is integrally closed.
(4) Let $A \subset K$ be a subring and $\mathfrak{p} \subset A$ a maximal ideal. The aim of this question is to show that there exists a valuation ring R of K such that $A \subset R$ and $A \cap \mathfrak{m}_R = \mathfrak{p}$.

(a) Show that the set $\mathscr{E}$ of subrings $B \subset K$ such that $A \subset B$ and $1 \notin \mathfrak{p}B$ contains an element R which is maximal for the inclusion [hint: Zorn].
(b) Show that R is local, and that its maximal ideal $\mathfrak{m}_R$ satisfies $A \cap \mathfrak{m}_R = \mathfrak{p}$ [hint: consider the localization of R at maximal ideal $\mathfrak{m} \subset R$ such that $\mathfrak{p}R \subset \mathfrak{m}$].
(c) Let $x \in K^\times$ be such that $x, x^{-1} \notin R$. Using the fact that $R[x], R[x^{-1}] \notin \mathscr{E}$, show that there exist relations $1 = a_1x + \cdots + a_nx^n$ and $1 = b_1x^{-1} + \cdots + b_mx^{-m}$ with $a_1, \ldots, a_n, b_1, \ldots, b_m \in \mathfrak{m}_R$. Assuming $n, m \in \mathbf{Z}_{>0}$ minimal, derive a contradiction an deduce that R is a valuation ring.

(5) Let $A \subset K$ be a subring, $B \subset K$ the integral closure of A in K, and B' the intersection of all the valuation rings of K that contain A.

(a) Show that $B \subset B'$.
(b) Let $x \in K$ such that x is not integral over A. Show that $x^{-1}A[x^{-1}]$ is a strict ideal in $A[x^{-1}]$. Conclude that there exists a valuation ring R such that $x \notin R$ [hint: use question (4)].
(c) Conclude that $B' = B$.

(6) Let A be a PID, $K = \mathsf{Frac}(A)$. Show that the valuation rings of K that contain A and are distinct from K are the localizations A_{pA} where p is a prime element in A.
(7) Let $A \subset K$ be a valuation ring such that there exists a prime ideal $\mathfrak{p} \subset A$ such that $\{0\} \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}_A$. Show that the ring $R = A[\![X]\!]$ is not integrally closed [hint: take $a \in \mathfrak{m}_A \backslash \mathfrak{p}$ and $b \in \mathfrak{p}\backslash\{0\}$, and show that the polynomial $T^2 + aT + X$ has a root f such that $bf \in XR$ but $f \notin R$].

Exercise 3.9.14. Let A be a complete DVR, $\pi \in A$ a uniformizer, and $\Sigma \subset A$ a complete set of representatives for $A/\pi A$. Show that any element in A can be written uniquely as the sum of a convergent series $x_0 + x_1\pi + x_2\pi^2 + \cdots$ in A.

Exercise 3.9.15. Let $(K, |.|)$ be a non archimedean valued field and $(L, |.|)$ its completion. Show that $|K^\times| = |L^\times|$ and that $\kappa_K \simeq \kappa_L$.

Exercise 3.9.16. Let K be a field and $|.|_1, |.|_2$ two equivalent non archimedean absolute values on K. Show that their value groups (resp. residue fields) are isomorphic.

Exercise 3.9.17. Let $(K, |.|)$ be a non archimedean valued field. Prove the following:
(1) for each $r \in \mathbf{R}_{>0}$, the balls $\mathsf{B}(0,r) = \{x \in K\,;\,|x| < r\}$ and $\overline{\mathsf{B}}(0,r) = \{x \in K\,;\,|x| \leqslant r\}$ are additive subgroups of K;
(2) the unit sphere is a multiplicative subgroup of $K^\times$;
(3) $\mathsf{B}(1,1) = \{x \in K\,;\,|x-1| < 1\}$ is a multiplicative subgroup of the unit sphere;
(4) for each $r \in]0,1[$, the balls $\mathsf{B}(1,r)$ and $\overline{\mathsf{B}}(1,r)$ are multiplicative subgroups of $\mathsf{B}(1,1)$.

Exercise 3.9.18. Let $(K, |.|)$ be a non archimedean locally compact valued field. Show that its residue field is finite and its value group is discrete.

Exercise 3.9.19. Find examples of two complete non archimedean valued fields whose respective residue fields and value groups are isomorphic, but which are not isomorphic as fields.

Exercise 3.9.20. Show that every non-trivial non archimedean absolute value on $\mathbf{R}$ has divisible value group and algebraically closed residue field.

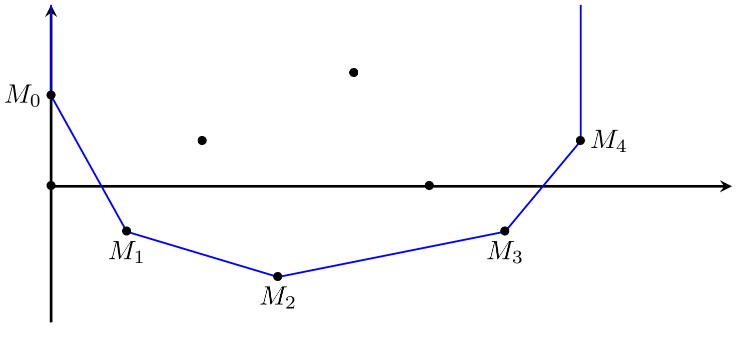
Exercise 3.9.21. Let $(K, |.|)$ be a complete valued field such that $|2| = 2$.
(1) Show that $\mathbf{R} \subset K$ and that $|.|$ extends the "usual" absolute value on $\mathbf{R}$.
(2) Show that if $K \neq \mathbf{R}$, then $K = \mathbf{C}$ endowed with its "usual" absolute value $|.|_\infty$ [hint: if $\alpha \in K \backslash \mathbf{R}$, show that the map $f\colon \mathbf{C} \to \mathbf{R}_{\geqslant 0}; z \mapsto \left|\alpha^2 - (z+\overline{z})\alpha + z\overline{z}\right|$ has a zero.]

Exercise 3.9.22. Let $(V, \|.\|_V)$ and $(W, \|.\|_W)$ be normed vector spaces over a complete valued field $(K, |.|)$. Assume that V is finite dimensional. Show that each sub-K-vector space of V is closed, and that any K-linear map $f\colon V \to W$ is continuous.

Exercise 3.9.23. Find an example of a (necessarilly non complete) non archimedean field $(K, |.|)$ and a finite dimensional K-vector space that admits two unequivalent norms.

Exercise 3.9.24. (Ostrowski for function fields). Let K be a field. As $K[X]$ is factorial, we can associate an absolute value $|.|_P$ on $K(X)$ to any monic irreductible $P \in K[X]$: fix $c \in]0,1[$, we have $|R|_P = c^{v_P(R)}$ where $v_P(R)$ is the P-adic valuation of $R \in K(X)$. Also we have the absolute value $|.|_\infty$ whose restriction to $K[X]$ is given by $|F|_\infty = c^{-\deg(F)}$ for any $F \in K[X]$.
(1) Compute the rings of integers and the residue fields of the absolute values mentionned above.
(2) Show that $|.|_\infty$ can be seen, after an appropriate change of indeterminate, as a P-adic absolute value.
(3) Show that any nontrivial absolute value on $K(X)$ that is trivial on K is equivalent to $|.|_P$ for some monic irreducible $P \in K[X]$ or to $|.|_\infty$.
(4) Explain how to normalize the absolute values $|.|_P$ so that the product formula $\prod_{v \in V} |R|_v = 1$ holds, where V is the set of irreducible monic polynomials union $\{\infty\}$.
(5) When $K = \mathbf{Q}$, construct absolute values on $\mathbf{Q}(X)$ that are not equivalent to the absolute values above.
(6) What happens when K is finite?

Exercise 3.9.25. (Newton polygons). Let $(K, |.|)$ be a complete non archimedean valued field, $\overline{K}$ an algebraic closure of K and v an associated valuation. If $P(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$, the *Newton polygon* $\mathsf{NP}(P)$ of P is the convex hull in $\mathbf{R}^2$ of the set of points $\{(i, v(a_i))\}_{0 \leqslant i \leqslant n} \cup \{\infty\}$ where ∞ denotes the point at infinity of the positive vertical axis.



(1) Let $\lambda \in \mathbf{R}$. Show that $P_\lambda(X) := \prod_{\substack{\alpha \in \overline{K} \\ v(\alpha) = -\lambda \\ P(\alpha) = 0}} (X - \alpha) \in K[X]$.

(2) Let $\lambda \in \mathbf{R}$. Show that the number (counting multiplicities) of roots x of P (in $\overline{K}$) such that $v(x) = -\lambda$ is equal to the length of the projection on the horizontal of the side of $\mathsf{NP}(P)$ of slope λ (so it is 0 if there is no such side).
(3) Deduce that if $\mathsf{NP}(P)$ has more than one finite slope, then P is reducible in $K[X]$.
(4) (Irreducibility criterion) Assume that v is discrete and normalized, that P is monic and that $\mathsf{NP}(P)$ has only one side of finite slope $-\frac{m}{n}$ where $\mathsf{gcd}(m, n) = 1$. Show that P is irreducible in $K[x]$. Recover Eisenstein's irreducibility criterion.

Exercise 3.9.26. Let $x \in \mathbf{Q}_p^\times$ and $x = \sum\limits_{n=v_p(x)}^{\infty} a_n p^n$ (with $a_n \in \{0, 1, \ldots, p-1\}$ for all n) its p-adic development. What is the p-adic development of $-x$?

Exercise 3.9.27. Let $x \in \mathbf{Q}_p$. Show that $x \in \mathbf{Q}$ if and only if its p-adic development $x = \sum\limits_{n=v_p(x)}^{\infty} a_n p^n$ (with $a_n \in \{0, 1, \ldots, p-1\}$) eventually becomes periodic [hint: reduce to the case where $x \in \mathbf{Q}_{<0} \cap \mathbf{Z}_p$].

Exercise 3.9.28. Let $x = \sum\limits_{k=0}^{\infty} 2^{k!} \in \mathbf{Q}_2$. Show that x is transcendental over $\mathbf{Q}$.

Exercise 3.9.29. Let $x \in \mathbf{Q}_p^\times$ and $x = \sum\limits_{n=v}^{\infty} a_n p^n$ its p-adic development. Let $n_0 < n_1 < \cdots$ be the sequence of indices such that $a_{n_k} \neq 0$. Assume that $\limsup\limits_{k\to\infty} \frac{n_{k+1}}{n_k} = +\infty$. Show that x is transcendental over $\mathbf{Q}$.

Exercise 3.9.30. Let $(K, |.|)$ be a complete non archimedean valued field. Denote by $\mathcal{O}_K$ its ring of integers and let $P(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + a_n X^n \in K[X]$ such that $a_0 a_n \neq 0$.
(1) Show that if P is irreducible, then $|P|_{\text{Gauss}} = \max\{|a_0|, |a_n|\}$.
(2) Assume that P is monic, irreducible, and $a_0 \in \mathcal{O}_K$. Show that $P \in \mathcal{O}_K[X]$.

Exercise 3.9.31. Let p be a prime integer.
(1) Let $u \in \mathbf{Q}_p^\times$. Show that the following are equivalent:
(i) $u \in \mathbf{Z}_p^\times$;
(ii) u^{p-1} is an n-th power in $\mathbf{Q}_p$ for infinitely many $n \in \mathbf{Z}_{>0}$.
(2) Prove that the only field automorphism of $\mathbf{Q}_p$ is $\mathsf{Id}_{\mathbf{Q}_p}$.

Exercise 3.9.32. Assume that p is odd. Show that $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times p} \simeq (\mathbf{Z}/p\mathbf{Z})^2$.

Exercise 3.9.33. Let p be a prime number, K be a complete discretely valued extension of $\mathbf{Q}_p$. Denote by $v \colon K^\times \to \mathbf{Z}$ its normalized valuation and by $e = v(p)$ its absolute ramification index. For $i \in \mathbf{N}_{>0}$, put $U_K^i = 1 + \mathfrak{m}_K^i$, where $\mathfrak{m}_K$ is the maximal ideal of K. Prove that $(U_K^i)^p = U_K^{i+e}$ when $i \geqslant \frac{e}{p-1}$.

Exercise 3.9.34. (1) Let F be a field such that $\mathsf{char}(F) \neq 2$ and $x, y \in F \backslash F^2$. Show that $F(\sqrt{x}) = F(\sqrt{y})$ if and only if there exists $z \in F^\times$ such that $y = xz^2$.
(2) Let $x \in \mathbf{Q}_2^\times$: write $x = 2^{v_2(x)} u$ with $u \in \mathbf{Z}_2^\times$. Show that x is a square in $\mathbf{Q}_2$ if and only if $2 \mid v_2(x)$ and $u \equiv 1 \mod 8\mathbf{Z}_2$. Describe the group $\mathbf{Q}_2^\times / \mathbf{Q}_2^{\times 2}$.
(3) Describe quadratic extensions of $\mathbf{Q}_2$.

Exercise 3.9.35. Let $a \in \mathbf{Z}$. Show that the polynomial $X^2 + X + a$ has a root in $\mathbf{Q}_2$ if and only if a is even.

Exercise 3.9.36. Show that $\mathbf{Q}_p^{\times 2} = \{x^2\}_{x \in \mathbf{Q}_p^\times}$ is open in $\mathbf{Q}_p^\times$.

Exercise 3.9.37. (Hensel's lemma). Let $(K, |.|)$ be a complete discretely valued field and $P \in \mathcal{O}_K[X]$ a monic polynomial.
(1) Show that if P is irreducible in $\mathcal{O}_K[X]$, its image in $\kappa_K[X]$ is the power of an irreducible polynomial.
(2) Assume that the image $\overline{P}$ of P in $\kappa_K[X]$ factors as $\overline{P}(X) = g_1(X) g_1(X)$ where $g_1, g_2 \in \kappa_K[X]$ are monic polynomials such that $\mathsf{gcd}(g_1, g_1) = 1$. Show that there exist unique $G_1, G_2 \in \mathcal{O}_K[X]$ monic polynomials whose images in $\kappa_K[X]$ are g_1 and g_2 respectively, and $P(X) = G_1(X) G_2(X)$.

Exercise 3.9.38. (A multivariate Newton's lemma). Let $(K, |.|)$ be a non archimedean valued field, $n \in \mathbf{Z}_{>0}$ and $P_1, \ldots, P_n \in \mathcal{O}_K[X_1, \ldots, X_n]$. Endow K^n with the norm defined by $\|\underline{x}\| = \max\limits_{1 \leqslant i \leqslant n} |x_i|$ for all $\underline{x} = (x_1, \ldots, x_n) \in K^n$, and put $P = (P_1, \ldots, P_n)$. Assume that $\underline{a} = (a_1, \ldots, a_n) \in \mathcal{O}_K^n$ satisfies $\|P(\underline{a})\| \leqslant \varepsilon \left|\det(J(\underline{a}))\right|^2$ with $\varepsilon \in]0, 1[$, where $J(\underline{a}) \in \mathsf{M}_n(\mathcal{O}_K)$ denotes the Jacobian matrix of P at $\underline{a}$. Show that there exists $\underline{b} \in \mathcal{O}_K^n$ such that $\|\underline{b} - \underline{a}\| \leqslant \varepsilon \left|\det(J(\underline{a}))\right|$ and $\|P(\underline{b})\| \leqslant \varepsilon^2 \left|\det(J(\underline{a}))\right|^2$. In particular, if $(K, |.|)$ is complete, there exists $\widetilde{\underline{a}} \in \mathcal{O}_K^n$ such that $\|\widetilde{\underline{a}} - \underline{a}\| \leqslant \varepsilon \left|J(\underline{a})\right|$ and $P(\widetilde{\underline{a}}) = 0$.

Exercise 3.9.39. Let p be a prime. Show that $\mathbf{Z}_p = \{x \in \mathbf{Q}_p\,;\,(\exists y \in \mathbf{Q}_p)\, y^2 = 1 + p^3x^4\}$ (this shows that $\mathbf{Z}_p$ is algebraically definable in $\mathbf{Q}_p$).

Exercise 3.9.40. Is the p-adic absolute value the only non trivial absolute value on $\mathbf{Q}_p$, up to equivalence?

Exercise 3.9.41. Let $(K, |.|)$ be a non archimedean valued field, and $\rho \in \mathbf{R}_{>0}$. If $P(X) = a_0 + a_1X + \cdots + a_nX^n$, put $|P|_\rho = \max\limits_{0 \leqslant i \leqslant n} |a_i|\,\rho^i$. Check that $|.|_\rho$ extends into an absolute value on $K(X)$. When are two such absolute values equivalent?

Exercise 3.9.42. (Classification of degree 1 transcendental valued extensions). (*cf* [16, §0.2]) Let K be an algebraically closed field, X an indeterminate, and $|.|$ be an absolute value on $K(X)$. Put

$$r_X = \inf_{\alpha \in K} |X - \alpha|$$

(1) Assume that there exist $\alpha_0, \pi \in K$ such that $r_X = |X - \alpha_0| = |\pi|$. Show that $|K(X)^\times| = |K^\times|$ and that $\kappa_{K(X)}$ is purely transcendental extension of degree 1 of κ_K (the extension of valued fields $K(X)/K$ is called *inert*).
(2) Assume that there exists $\alpha_0 \in K$ such that $r_X = |X - \alpha_0| \notin |K^\times|$. Show that $|K(X)^\times| = |K^\times|\, r_X^{\mathbf{Z}}$ and $\kappa_{K(X)} = \kappa_K$ (the extension of valued fields $K(X)/K$ is called *totally ramified*).
(3) Assume that $|X - \alpha| > r_X$ for all $\alpha \in K$. Show that $|K(X)^\times| = |K^\times|$ and $\kappa_{K(X)} = \kappa_K$ (then $K(X)$ is called an *immediate (valued) extension* of K).

Exercise 3.9.43. Show that the map $\mathbf{C} \to \mathbf{R}_{\geqslant 0}$; $z \mapsto |z| = \sqrt{z\bar{z}}$ is the unique absolute value on $\mathbf{C}$ that extends the absolute value $|.|$ of $\mathbf{R}$.

Exercise 3.9.44. Let L/K be an algebraic extension, and $|.|$ an absolute value on L. Show that if the restriction of $|.|$ to K is trivial, then $|.|$ is trivial.

Exercise 3.9.45. Let L/K be a finite extension of valued fields. Shows that if $\alpha \in L$ is integral over $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_L$. The converse holds when K is complete: show with an example that the converse does not hold in general.

Exercise 3.9.46. Let L/K be a purely inseparable field extension. Show that any absolute value on K has a unique extension to L.

Exercise 3.9.47. Let $(K, |.|)$ be a complete non archimedean valued field, and L/K a finite extension. Show that if $\|.\|$ is any norm on the K-vector space L, the map $x \mapsto \lim\limits_{n\to\infty} \sqrt[n]{\|x^n\|}$ coincides with the unique absolute value extending $|.|$ on L.

Exercise 3.9.48. Let p be a prime number. Show that $X^2 - p$ is irreducible in $\mathbf{Q}_p[X]$. Let $K = \mathbf{Q}_p(\sqrt{p})$ and $|.|_K$ the extension of $|.|_p$ to K. If $x = a + b\sqrt{p} \in K$ (where $a, b \in \mathbf{Q}_p$), show that $|x|_K = \max\left\{ |a|_p, \frac{|b|_p}{\sqrt{p}} \right\}$. What are the residue field and the value group of $(K, |.|_K)$?

Exercise 3.9.49. Let p be a prime number such that $p \equiv 3 \mod 4$. Show that $X^2 + 1$ is irreducible in $\mathbf{Q}_p[X]$. Let $K = \mathbf{Q}_p(i)$ (where i is a root of $X^2 + 1$) and $|.|_K$ the extension of $|.|_p$ to K. Find a formula for $|a + ib|_K$, where $a, b \in \mathbf{Q}_p$.

Exercise 3.9.50. How many extensions to $\mathbf{Q}(\sqrt[n]{2})$ does the archimedean absolute value $|.|$ of $\mathbf{Q}$ admit?

Exercise 3.9.51. Let $P(X) = X^3 - 17$ and $j \in \overline{\mathbf{Q}}_3$ a primitive cubic root of unity.
(1) Show that $j \notin \mathbf{Q}_3$ [hint: compute $(j-1)^2$].
(2) What are the degrees of the irreducible factors of P in $\mathbf{Q}_3[X]$ [hint: compute $P(5)$]?
(3) How many extensions to $\mathbf{Q}(\sqrt[3]{17})$ does the 3-adic absolute value have?

Exercise 3.9.52. Let $(K, |.|)$ be a non archimedean valued field. Is the map $|.| : K \to \mathbf{R}_{\geqslant 0}$ continuous when $\mathbf{R}_{\geqslant 0}$ is endowed with its “usual” topology? What if $\mathbf{R}_{\geqslant 0}$ is endowed with the discrete topology?

Exercise 3.9.53. Let $(K, |.|)$ be a complete non archimedean valued field and $P \in K[X]\backslash K$.
(1) Let $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ be a sequence of elements in K such that $\lim\limits_{n\to\infty} |P(x_n)| = 0$. Show that there is a subsequence of $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ that converges to a root of P in K.
(2) If $F \subset K$ is closed, then its image $P(F)$ is closed.
(3) If $C \subset K$ is compact, then its inverse image $P^{-1}(C)$ is compact.

Exercise 3.9.54. Let $\overline{\mathbf{Q}}_p$ be an algebraic closure of $\mathbf{Q}_p$. The p-adic absolute value extends uniquely to an absolute value $|.|_p$ on $\overline{\mathbf{Q}}_p$. For $n \in \mathbf{Z}_{>0}$, put $H_n = \{x \in \overline{\mathbf{Q}}_p\,;\, [\mathbf{Q}_p(x) : \mathbf{Q}_p] \leqslant n\}$.
(1) Show that H_n is closed.
(2) Show that $H_n \neq \overline{\mathbf{Q}}_p$ for all $n \in \mathbf{Z}_{>0}$.
(3) Show that $H_n + H_m \subset H_{nm}$ for all $n, m \in \mathbf{Z}_{>0}$.
(4) Deduce that $\overline{\mathbf{Q}}_p$ is not complete for $|.|_p$ [hint: Baire].

Exercise 3.9.55. Prove that there are exactly two non-isomorphic cubic extensions of $\mathbf{Q}_2$.

Exercise 3.9.56. Let $\overline{\mathbf{Q}}_2$ be an algebraic closure of $\mathbf{Q}_2$, and fix a sequence $(\alpha_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ in $\overline{\mathbf{Q}}_2$ such that $\alpha_0 = 2$ and $\alpha_{n+1}^2 = \alpha_n$ for all $n \in \mathbf{Z}_{\geqslant 0}$. Let $F = \mathbf{Q}_2(\alpha_n)_{n\in\mathbf{Z}_{\geqslant 0}} \subset \overline{\mathbf{Q}}_2$: the 2-adic absolute value $|.|_2$ extends uniquely to $\overline{\mathbf{Q}}_2$. Let $(K, |.|)$ be the completion of $(F, |.|_2)$, and $L = K(i)$ where $i^2 = -1$.
(1) For $n \in \mathbf{Z}_{\geqslant 0}$, put $x_n = 1 + 2(\alpha_1^{-1} + \cdots + \alpha_n^{-1})$. Show that $v_2(i - x_n) = 1 - \frac{1}{2^{n+1}}$ [Hint: compute $v_2(1 + x_n^2)$]. Deduce that $[\mathbf{Q}_2(\alpha_n, i) : \mathbf{Q}_2(\alpha_n)] = 2$.
(2) Determine the residue field of $\mathbf{Q}_2(\alpha_n, i)$ for all $n \in \mathbf{Z}_{\geqslant 0}$.
(3) Show that the ramification index e and the residual degree f of L/K are equal to 1, so that the inequality $ef \leqslant [L : K]$ is strict.

Exercise 3.9.57. Let $(K, |.|)$ be a complete non archimedean valued field, and L/K a finite extension such that the residual extension $\kappa(L)/\kappa(K)$ is Galois. Let T be the maximal unramified subextension of L/K. Show that T/K is Galois and that there exists a natural group isomorphism $\mathsf{Gal}(T/K) \xrightarrow{\sim} \mathsf{Gal}(\kappa(L)/\kappa(K))$.

Exercise 3.9.58. Let $(K, |.|)$ be a complete non archimedean valued field, $\overline{K}$ an algebraic closure, and L, M finite subextensions. Show that if L/K is unramified, so is ML/M.

Exercise 3.9.59. Let $(K, |.|)$ be a complete non archimedean valued field, $\overline{K}$ an algebraic closure of K and $e \in \mathbf{Z}_{>0}$ prime to $\mathsf{char}(\kappa_K)$. Show that if $\alpha \in \overline{K}$ is such that $\alpha^e \in \mathcal{O}_K^\times$, the extension $K(\alpha)/K$ is unramified.

Exercise 3.9.60. Let $|.|$ be the Gauss absolute value on $\mathbf{Q}_2(X)$, and $(K, |.|)$ the completion thereof. Let L the decomposition field of the polynomial $P(Y) = (Y^2 - X)^2 - 2 \in K[Y]$, and $|.|$ the unique absolute value on L that extends $|.|$.
(0) What is the residue field κ_K of K?
(1) Show that $[L : K] = 8$, that $e_{L/K} = 4$ and $f_{L/K} = 2$.
(2) Show that there is no subextension M of L/K such that $[M : K] = 2$ and $\kappa_M = \kappa_L$.

Exercise 3.9.61. Let $A = \mathbf{Z}_{(2)}$ and $\alpha = \frac{-1+\sqrt{4\sqrt{2}-3}}{2} \in \mathbf{R}$. Put $B = A[\alpha]$. Show that B is a DVR whose residue field is $\mathbf{F}_4$ and whose ramification index is $e_{B/A} = 2$. Show that there is no DVR $C \subset B$ which is unramified over A and whose residue field is $\mathbf{F}_4$ [hint: determine the subextensions of $\mathbf{Q}(\alpha)/\mathbf{Q}$].

Exercise 3.9.62. Let $(K, |.|)$ be a complete and discrete non archimedean valued field, L/K a finite extension and $\alpha \in \mathcal{O}_L^\times$ such that $L = K(\alpha)$. Denote by $\overline{\alpha}$ the image of α in κ_L. Let $P(X) \in \mathcal{O}_K[X]$ (resp. $\Pi(X) \in \kappa_K[X]$) be the minimal polynomial of α (resp. $\overline{\alpha}$) over K (resp. over κ_K), and $\overline{P}(X)$ the image of $P(X)$ in $\kappa_K[X]$. Show that $\overline{P}(X) = \Pi(X)^d$, for some integer d such that $e \mid d$ (where $e = e_{L/K}$ denotes the ramification index of L/K).

Exercise 3.9.63. Show that the unique unramified extension of degree n of $\mathbf{Q}_p$ (in a fixed algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$) is the decomposition field of $X^{p^n} - X$.

Exercise 3.9.64. Let $(K, |.|)$ be a complete discrete non archimedean valued field, and $\overline{K}$ an algebraic closure.
(1) Let $M \subset L$ be finite subextensions of $\overline{K}/K$. Show that L/K is tamely ramified if and only if L/M and M/K are tamely ramified.
(2) Assume that L/K is a finite subextension of $\overline{K}$, and T/K a finite unramified subextension of $\overline{K}$. Show that L/K is tamely ramified if and only if LT/T is tamely ramified.
(3) Let $e \in \mathbf{Z}_{>0}$ be prime to $\mathsf{char}(\kappa_K)$ and $b \in \mathcal{O}_K \backslash \{0\}$, and $L \subset \overline{K}$ be the extension obtained by adjoining a root of $X^e - b$. Show that L/K is tamely ramified, and that $e_{L/K} = e' := \frac{e}{\mathsf{gcd}(e, v_K(b))}$ (where v_K denotes the normalized valuation on K) [hint: by question (2), this can be checked after composition with any unramified extension of K: use an appropriate one to reduce to the case where $b = \pi_K^{e'}$ with π_K a uniformizer in K].
(4) Let L, M be finite subextensions of $\overline{K}/K$. Show that if L/K is tamely ramified, so is ML/M.
(5) Deduce that if L/K and M/K are both tamely ramified, so is ML/K.

Exercise 3.9.65. Let C be an algebraic closed field of characteristic 0, and $K = C(\!(X)\!) = \mathsf{Frac}(K[\![X]\!])$ the field of formal Laurent series with coefficients in C. Let $\overline{K}$ be an algebraic closure of K. Show that $\overline{K} = \bigcup\limits_{n \in \mathbf{Z}_{>0}} C(\!(X^{1/n})\!)$.

Exercise 3.9.66. Let L/K be a finite extension of local fields, and M_1, M_2 two subextensions such that M_1/K and M_2/K are totally ramified. Is the composite M_1M_2/K necessarily totally ramified?

Exercise 3.9.67. Let p be a prime number. Show that the maximal unramified extension of $\mathbf{Q}_p$ in $\overline{\mathbf{Q}}_p$ is obtained by adjoining all roots of unity of order prime to p.

Exercise 3.9.68. Let L/K be a totally tamely ramified finite extension of complete, discrete non archimedean valued fields. Show that the intermediate fields of L/K correspond bijectively to subgroups of $|L^\times| / |K^\times|$ (where $|.|$ denotes the absolute value on L).

Exercise 3.9.69. (1) Let L/K be a finite tamely ramified Galois extension of complete and discrete non archimedean valued fields. Denote by T be the maximal unramified subextension of L/K. Put $G_{L/K} = \mathsf{Gal}(L/K)$ and $I_{L/K} = \mathsf{Gal}(L/T)$, so that we have an isomorphism $G_{L/K}/I_{L/K} \xrightarrow{\sim} \mathsf{Gal}(\kappa_L/\kappa_K)$. Show that $I_{L/K}$ is abelian and that $\mathsf{Gal}(\kappa_L/\kappa_K)$ acts on I by $(\sigma I, \tau) \mapsto \sigma\tau\sigma^{-1}$.
(2) Show that every tamely ramified extension of K can be embedded into a finite tamely ramified extension L/K such that $G_{L/K} \simeq I_{L/K} \rtimes \mathsf{Gal}(\kappa_L/\kappa_K)$.

Exercise 3.9.70. Show that the maximal tamely ramified abelian extension V of $\mathbf{Q}_p$ is finite over the maximal unramified extension T of $\mathbf{Q}_p$.

Exercise 3.9.71. Show that the maximal unramified extension of $K = \mathbf{F}_p(\!(X)\!)$ is $T = \bigcup\limits_{n \in \mathbf{Z}_{>0}} \mathbf{F}_{p^n}(\!(X)\!)$ and that the maximal tamely ramified extension is $V = T\Big(\{\sqrt[n]{X}\}_{\substack{n \in \mathbf{Z}_{>0} \\ p \nmid n}}\Big)$.

Exercise 3.9.72. Let p be an odd prime number, $\Phi_p(X) = X^{p-1} + \cdots + X + 1 \in \mathbf{Q}_p[X]$ and $\zeta \in \overline{\mathbf{Q}}_p$ a root of Φ_p. Put $K = \mathbf{Q}_p(\zeta)$.
(1) Set $Y = X - 1$: show that $\Phi_p(X) = P(Y)$ where P is an Eisenstein polynomial. Deduce that $K/\mathbf{Q}_p$ is tamely totally ramified.
(2) Show that $K = \mathbf{Q}_p(\pi)$ where $\pi^{p-1} = -p$ [hint: use the polynomial $-\frac{1}{p}P(\pi Z)$ to show that $\zeta \in \mathbf{Q}_p(\pi)$].

Exercise 3.9.73. Let α be a root of $P(X) = X^4 - 50 \in \mathbf{Q}_5[X]$ (in some algebraic closure of $\mathbf{Q}_5$) and $K = \mathbf{Q}_5(\alpha)$.
(1) Prove that $K/\mathbf{Q}_5$ is a cyclic extension of degree 4.
(2) Prove that the maximal unramified subextension T of $K/\mathbf{Q}_5$ is quadratic over $\mathbf{Q}_5$, so K/T is a totally tamely ramified extension with degree 2.
(3) Find a uniformizer π of T such that $K = T(\sqrt{\pi})$.
(4) Show that such a π cannot be found inside $\mathbf{Q}_5$.

Exercise 3.9.74. Let $(K, |.|)$ be a non archimedean complete valued field and L/K a finite separable extension.
(1) Assume that L/K is unramified. Show that $\mathsf{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$.
(2) Assume that $|.|$ is discrete. Show that $\mathsf{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$ if and only if is tamely ramified.

Exercise 3.9.75. Let K be a complete discretely valued field of characteristic 0, whose residue field κ_K has characteristic $p > 0$. We denote by $v_K \colon K \to \mathbf{Z} \cup \{\infty\}$ its normalized valuation.
(1) Let L/K be a totally ramified finite extension and $E(X) = X^e + a_{e-1}X^{e-1} + \cdots + a_0 \in \mathcal{O}_K[X]$ the minimal polynomial over K of a uniformizer π_L of L. Put $c(L) = v_L(\mathfrak{D}_{L/K}) - e + 1$ (where $v_L \colon L \to \mathbf{Z} \cup \{\infty\}$ is the normalized valuation and $\mathfrak{D}_{L/K}$ the different of L/K). Show that $c(L) \in \mathbf{Z}_{\geqslant 0}$ and that $c(L) = 0$ if and only if L/K is tamely ramified [hint: use the equality $\mathfrak{D}_{L/K} = E'(\pi_L)\mathcal{O}_L$].
(2) Show that if L/K is not tamely ramified, then $c(L) = \min\{ev_K(e), ev_K(a_i) - e + i\}_{1 \leqslant i < e}$.
Let $\overline{K}$ be a fixed separable closure of K and π a uniformizer of K. We denote by $U_K = 1 + \pi\mathcal{O}_K$ the group of principal units of K. Henceforth, we assume that κ_K is *finite*: let q be its order.
(3) Show that an element $u \in \mathcal{O}_K^\times$ can be written uniquely $u = [\alpha]\tilde{u}$ where $\alpha \in \kappa_K^\times$, $[\alpha] \in \mathcal{O}_K^\times$ is the unique $(q-1)$-th root of unity lifting α and $\tilde{u} \in U_K$.
We denote by Σ_e the set of subextensions L/K of $\overline{K}$ that are totally ramified of degree $e \in \mathbf{Z}_{>0}$.
(4) Assume that $p \nmid e$. Recall that, being tamely ramified over K, elements in Σ_e are of the form $K_\theta := K(\theta)$ where $\theta \in \overline{K}$ is a root of the polynomial $X^e - u\pi$ for some $u \in \mathcal{O}_K^\times$.

- (a) Let $\tilde{u} \in U_K$. Show that there exists $\lambda \in U_K$ such that $\lambda^e = \tilde{u}$. Deduce that we may restrict to elements u of the form $[\alpha]$ with $\alpha \in \kappa_K^\times$.
- (b) Let $\alpha, \alpha' \in \kappa_K^\times$ and $\theta, \theta' \in \overline{K}$ such that $\theta^e = [\alpha]\pi$ and $\theta'^e = [\alpha']\pi$. Show that $K_\theta = K_{\theta'}$ if and only if there exists $\beta \in \kappa_K^\times$ such that $\alpha' = \beta^e\alpha$ and an e-th root of unity $\zeta \in K$ such that $\theta' = [\beta]\zeta\theta$. Deduce that it is equivalent to the existence of $\gamma \in \kappa_K^\times$ such that $\theta' = [\gamma]\theta$.
- (c) Show that $\#\Sigma_e = e$.

(5) In this question, we assume that $p \mid e$: by question (1), we have $L \in \Sigma_e \Rightarrow c(L) \in \{1, \ldots, ev_K(e)\}$.

- (a) For each $j \in \{1, \ldots, e-1\}$, construct an element $L \in \Sigma_e$ such that $c(L) = j$.
- (b) Deduce that $\#\Sigma_e \geqslant e$.
- (c) Assume $\#\Sigma_e = e$. Using (2), show that $v_K(e) = 1$, then that $e = p$ is a uniformizer of K [hint: consider the extension generated by the roots of $X^e - \pi$, then that generated by a root of $X^e - u\pi$ for an appropriate root of unity $u \in \mathcal{O}_K^\times$].
- (d) Deduce $\#\Sigma_e > e$.

Exercise 3.9.76. Let $(K, |.|)$ be a complete discretely valued field and $\overline{K}$ an algebraic closure of K. We assume that the residue field κ_K of K contains the finite field $\mathbf{F}_q$ (where $q = p^f$ with $f \in \mathbf{Z}_{>0}$). Fix a uniformizer π of K and let $P(X) = X^q + \pi X \in K[X]$. Choose a sequence $(\pi_n)_{n \in \mathbf{Z}_{\geqslant 0}}$ in $\overline{K}$ such that $\pi_0 = 0$, $\pi_1 \neq 0$ and $P(\pi_n) = \pi_{n-1}$ for all $n \in \mathbf{Z}_{>0}$. For $n \in \mathbf{Z}_{\geqslant 0}$, we put $K_n = K(\pi_n)$.
(1) Explain why the group $\mu_{q-1}(K)$ of $(q-1)$-th roots of unity is cyclic of order $q-1$.
(2) Show that K_1/K is totally ramified and that π_1 is a uniformizer of K_1.
(3) Show that K_1/K is Galois and describe its Galois group.
(4) Show that for all $n \in \mathbf{Z}_{>0}$, the extension K_{n+1}/K_n is separable, totally ramified of degree q, and that π_{n+1} is a uniformizer of K_{n+1} [hint: use induction].
(5) Show that $\mathcal{O}_{K_n} = \mathcal{O}_K[\pi_n]$ for all $n \in \mathbf{Z}_{\geqslant 0}$.
(6) Compute the different $\mathfrak{D}_{K_{n+1}/K_n}$ [do the case $n = 0$ separately], and deduce $\mathfrak{D}_{K_n/K}$ and the discriminant $\mathfrak{d}_{K_n/K}$ for all $n \in \mathbf{Z}_{\geqslant 0}$.

4. Local fields

4.1. Definition and first properties.

Definition 4.1.1. A *local field* is a complete discrete valued field $(K, |.|)$ such that $|.|$ is non trivial and whose residue field is perfect[36].

Henceforth, $(K, |.|)$ denotes a local field, π_K a uniformizer of K, and v_K a valuation on K associated to $|.|$.

4.1.2. *Galois extensions of local fields.* Let L/K be a finite Galois extension. By theorem 3.8.12, the extension T/K is Galois, and we have the exact sequence

$$\{1\} \to I_{L/K} \to \mathsf{Gal}(L/K) \to \mathsf{Gal}(\kappa_L/\kappa_K) \to \{1\}$$

where $I_{L/K} = \mathsf{Gal}(L/T)$ is the inertia subgroup. Assume now that $\mathsf{char}(\kappa_K) = p > 0$. The extension L/T is totally ramified. Let V be the unique subextension of L/T such that V/T is tamely ramified and $[L : V] = p^r$, where $r = v_p([L : T])$. If $\sigma \in \mathsf{Gal}(L/T)$, then $\sigma(V) \subset L$ satisfies $[\sigma(V) : T] = [V : T]$, so by unicity we have $\sigma(T) = T$: the extension V/T is Galois.

4.2. Structure of rings of integers of local fields.

Let $(K, |.|)$ be a local field, and π a uniformizer of K. If $\mathsf{char}(K) = p > 0$, then $\mathsf{char}(\kappa_K) = p$. There are two possibilities:

- $\mathsf{char}(K) = \mathsf{char}(\kappa_K)$: this is the *equicharacteristic* case;
- $\mathsf{char}(K) = 0$ and $\mathsf{char}(\kappa_K) = p > 0$: this is the *mixed characteristic* case.

4.2.1. *The equicharacteristic case.*

Theorem 4.2.2. Assume $\mathsf{char}(K) = \mathsf{char}(\kappa_K)$. Then $\mathcal{O}_K$ is isomorphic to $\kappa_K[\![T]\!]$.

Definition 4.2.3. A *field of representatives* in $\mathcal{O}_K$ is a field $F \subset \mathcal{O}_K$ which is also a complete set of representatives for κ_K, in other words such that the canonical map $\mathcal{O}_K \to \kappa_K$ induces an isomorphism $F \xrightarrow{\sim} \kappa_K$.

Lemma 4.2.4. If $\mathsf{char}(\kappa_K) = 0$, then $\mathcal{O}_K$ admits a field of coefficients.

Proof. As $\mathbf{Z} \to \mathcal{O}_K \to \kappa_K$ is injective (since $\mathsf{char}(\kappa_K) = 0$), we have $\mathbf{Z} \cap \mathfrak{m}_K = \{0\}$, so that $\mathbf{Q}$ is a subfield of $\mathcal{O}_K$. By Zorn's lemma (*cf* theorem 9.1.1), there exists a maximal subfield $F \subset \mathcal{O}_K$: we have to show that the composite $F \subset \mathcal{O}_K \to \kappa_K$ is surjective (it is automatically injective since F is a field). Let $\overline{F}$ be the image of F in κ_K.
• Assume $\kappa_K/\overline{F}$ is not algebraic: there exists $x \in \mathcal{O}_K^\times$ whose image $\overline{x}$ in κ_K is transcendental over $\overline{F}$. The projection $\mathcal{O}_K \to \kappa_K$ maps $F[x]$ surjectively hence bijectively onto $\overline{F}[\overline{x}]$. This implies that $F[x] \cap \mathfrak{m}_K = \{0\}$, so that elements in $F[x]\backslash\{0\}$ are invertible in $\mathcal{O}_K$: we have $F(x) \subset \mathcal{O}_K$, contradicting the maximality of F.
• Let $\overline{x} \in \kappa_K$. As $\kappa_K/\overline{F}$ is algebraic, we can consider the minimal polynomial $\overline{P}(X) \in \overline{F}[X]$ of $\overline{x}$ over $\overline{F}$. Let $P(X) \in F[X]$ be a monic lifting of $\overline{P}$ (so P is irreducible in $F[X]$), and $x_0 \in \mathcal{O}_K$ be any lifting of $\overline{x}$. As $\mathsf{char}(\kappa_K) = 0$, the polynomial $\overline{P}$ is separable, so $\overline{P}'(\overline{x}) \neq 0$: we have $|P(x_0)| < 1$ and $|P'(x_0)| = 1$. Newton's lemma (*cf* theorem 3.3.10) implies that there exists a unique $x \in \mathcal{O}_K$ such that $P(x) = 0$ and $|x - x_0| \leqslant |P(x_0)| < 1$. This implies that the composite $F[X]/\langle P\rangle \xrightarrow{\sim} F(x) \to \overline{F}(\overline{x})$ is an isomorphism, hence $F(x)$ is a subfield of $\mathcal{O}_K$: by maximality we have $F(x) = F$, *i.e.* $x \in F$, whence $\overline{x} \in \overline{F}$. This shows that $\overline{F} = \kappa_K$, and F is a field of coefficients for $\mathcal{O}_K$. □

Lemma 4.2.5. If $\mathsf{char}(\kappa_K) = 0$, then $\mathcal{O}_K$ admits a field of coefficients.

Proof. • Let $\overline{x} \in \kappa_K$. For each $n \in \mathbf{Z}_{\geqslant 0}$, let $\widehat{x}_n, \widetilde{x}_n \in \mathcal{O}_K$ be liftings of $\overline{x}^{p^{-n}} \in \kappa_K$ (recall that κ_K is perfect): the elements $\widehat{x}_n^{p^n}$ and $\widetilde{x}_n^{p^n}$ are lifts of $\overline{x}$. We have $\widehat{x}_n \equiv \widetilde{x}_n \mod \pi_K\mathcal{O}_K$, so $\widehat{x}_n^p \equiv \widetilde{x}_n^p \mod \pi_K^p\mathcal{O}_K$ (by the binomial theorem, and the fact that $\mathsf{char}(\mathcal{O}_K) = p$), and $\widehat{x}_n^{p^n} \equiv \widetilde{x}_n^{p^n} \mod \pi_K^{p^n}\mathcal{O}_K$ by an immediate induction. Applied with $\widetilde{x}_n = \widehat{x}_{n+1}^p$, we deduce that $\widehat{x}_{n+1}^{p^{n+1}} \equiv \widehat{x}_n^{p^n} \mod \pi_k^{p^n}\mathcal{O}_K$, which implies that $\big(\widehat{x}_n^{p^n}\big)_{n\in\mathbf{Z}_{\geqslant 0}}$ is a Cauchy sequence in $\mathcal{O}_K$ for the π_K-adic topology. As $\mathcal{O}_K$ is complete, this sequence converges to a limit $\rho(\overline{x}) \in \mathcal{O}_K$, which lifts $\overline{x}$. The congruence $\widehat{x}_n^{p^n} \equiv \widetilde{x}_n^{p^n} \mod \pi_K^{p^n}\mathcal{O}_K$ proved above shows that this limit $\rho(\overline{x})$ does not depend on the choice of the lifts $(\widehat{x}_n)_{n\in\mathbf{Z}_{\geqslant 0}}$, but only on $\overline{x}$. This provides a map $\rho\colon \kappa_K \to \mathcal{O}_K$, that is a section of the canonical map $\mathcal{O}_K \to \kappa_K$.
• If $\overline{x}, \overline{y} \in \kappa_K$, let $(\widehat{x}_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ and $(\widehat{y}_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ sequences in $\mathcal{O}_K$ lifting the sequences $\big(\overline{x}^{p^{-n}}\big)_{n\in\mathbf{Z}_{\geqslant 0}}$ and $\big(\overline{y}^{p^{-n}}\big)_{n\in\mathbf{Z}_{\geqslant 0}}$ respectively. Then the sequence of products $(\widehat{x}_n\widehat{y}_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ lifts $\big((\overline{xy})^{p^{-n}}\big)_{n\in\mathbf{Z}_{\geqslant 0}}$, which implies that $\rho(\overline{xy}) = \lim\limits_{n\to\infty} \widehat{x}_n^{p^n}\widehat{y}_n^{p^n} = \rho(\overline{x})\rho(\overline{y})$. Similarly, the sequence of sums $(\widehat{x}_n + \widehat{y}_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ lifts $\big((\overline{x}+\overline{y})^{p^{-n}}\big)_{n\in\mathbf{Z}_{\geqslant 0}}$

[36] Some authors restrict this terminology to the finite residue field case.

(because $(\overline{x}+\overline{y})^{p^{-n}} = \overline{x}^{p^{-n}} + \overline{y}^{p^{-n}}$), so that $\rho(\overline{x}+\overline{y}) = \lim\limits_{n\to\infty}(\widehat{x}_n+\widehat{y}_n)^{p^n} = \rho(\overline{x})+\rho(\overline{y})$ (as $\mathsf{char}(\mathcal{O}_K) = p$, we have $(\widehat{x}_n+\widehat{y}_n)^{p^n} = \widehat{x}_n^{p^n}+\widehat{y}_n^{p^n}$ for all $n\in\mathbf{Z}_{\geqslant 0}$). This implies that ρ is a ring homomorphism. As κ_K is a field, it is an isomorphism onto its image: the latter is a field of coefficients for $\mathcal{O}_K$. □

Proof of theorem 4.2.2. Lemmas 4.2.4 and 4.2.5 show that $\mathcal{O}_K$ has a field of coefficients F. As $\mathcal{O}_K$ is π_K-adically separated and complete, there exists a unique continuous morphism of F-algebras $h\colon F[\![T]\!]\to\mathcal{O}_K$ such that $h(T)=\pi_K$. Corollary 3.7.5 imply that h is an isomorphism. Composed with the isomorphism $\kappa_K[\![T]\!]\xrightarrow{\sim}F[\![T]\!]$ gives the result. □

4.2.6. *Witt vectors.* The references for this part are [20, Chap. II, §6], [5, Chap. IX, §1] and [10, Chap. I]. In what follows, "ring" means commutative unitary ring. Let p be a prime integer. Let $\underline{X}=(X_0,X_1,\ldots)$ be a indeterminate.

Definition 4.2.7. Let $n\in\mathbf{Z}_{\geqslant 0}$, the n-th *Witt polynomial* is

$$\Phi_n(\underline{X}) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p + p^nX_n = \sum_{i=0}^n p^iX_i^{p^{n-i}}$$

If A is ring, the *ghost map* is:

$$\begin{aligned}\Phi_A\colon A^{\mathbf{Z}_{\geqslant 0}} &\to A^{\mathbf{Z}_{\geqslant 0}}\\ \underline{a} &\mapsto \big(\Phi_n(\underline{a})\big)_{n\in\mathbf{Z}_{\geqslant 0}}\end{aligned}$$

Lemma 4.2.8. Let A be a ring, and $x,y\in A$ such that $x\equiv y \mod pA$. Then $x^{p^i}\equiv y^{p^i} \mod p^{i+1}A$ for every $i\in\mathbf{Z}_{\geqslant 0}$.

Proof. We proceed by induction on $i\in\mathbf{Z}_{\geqslant 0}$, the case $i=0$ being the hypothesis. Let $i\in\mathbf{Z}_{\geqslant 0}$ be such that $x^{p^i}\equiv y^{p^i} \mod p^{i+1}A$: write $x^{p^i}=y^{p^i}+p^{i+1}z$ with $z\in A$. By the binomial theorem, we have $x^{p^{i+1}} = \big(y^{p^i}+p^{i+1}z\big)^p = y^{p^{i+1}} + \sum\limits_{k=1}^{p-1}\binom{p}{k}p^{k(i+1)}y^{p^i(p-k)}z^k + p^{p(i+1)}z^p$. For $k\in\{1,\ldots,p-1\}$, we have $v_p\big(\binom{p}{k}p^{k(i+1)}\big) = 1+k(i+1)\geqslant i+2$, and $p(i+1)\geqslant i+2$ (because $p\geqslant 2$), so $x^{p^{i+1}}\equiv y^{p^{i+1}} \mod p^{i+2}A$. □

Lemma 4.2.9. (Dwork). Let $\varphi\colon A\to A$ be a ring homomorphism such that $\varphi(a)\equiv a^p \mod pA$ for all $a\in A$. Then a sequence $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}\in A^{\mathbf{Z}_{\geqslant 0}}$ is in the image of Φ_A if and only if $\varphi(x_n)\equiv x_{n+1} \mod p^{n+1}A$ for all $n\in\mathbf{Z}_{\geqslant 0}$.

Proof. • As φ is a ring homomorphism, we have $\varphi(\Phi_n(\underline{a})) = \sum\limits_{i=0}^n p^i\varphi(a_i)^{p^{n-i}}$ for all $\underline{a}=(a_n)_{n\in\mathbf{Z}_{\geqslant 0}}$. As $\varphi(a_i)\equiv a_i^p \mod pA$, we have $\varphi(a_i)^{p^{n-i}}\equiv a_i^{p^{n+1-i}} \mod p^{n+1-i}A$ for all $i\in\{0,\ldots,n\}$ by lemma 4.2.8. This implies that $\varphi(\Phi_n(\underline{a}))\equiv\sum\limits_{i=0}^n p^ia_i^{p^{n+1-i}} \mod p^{n+1}A$, *i.e.* $\varphi(\Phi_n(\underline{a}))\equiv\Phi_{n+1}(\underline{a}) \mod p^{n+1}A$.

• Conversely, assume that $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}\in A^{\mathbf{Z}_{\geqslant 0}}$ satisfies $\varphi(x_n)\equiv x_{n+1} \mod p^{n+1}A$ for all $n\in\mathbf{Z}_{\geqslant 0}$: we construct $\underline{a}=(a_n)_{n\in\mathbf{Z}_{\geqslant 0}}\in A^{\mathbf{Z}_{\geqslant 0}}$ inductively such that $x_n=\Phi_n(\underline{a})$ for all $n\in\mathbf{Z}_{\geqslant 0}$. Put $a_0=x_0\in A$. Let $n\in\mathbf{Z}_{\geqslant 0}$ be such that $a_0,\ldots,a_n\in A$ have been constructed such that for all $k\in\{0,\ldots,n\}$, we have $x_k=\Phi_k(a_0,\ldots,a_k)$. By the computation above, we have $\varphi(x_n)=\varphi(\Phi_n(\underline{a}))\equiv\sum\limits_{i=0}^n p^ia_i^{p^{n+1-i}} \mod p^{n+1}A$ *i.e.* $x_{n+1}-\sum\limits_{i=0}^n p^ia_i^{p^{n+1-i}}\in p^{n+1}A$ (since $x_{n+1}-\varphi(x_n)\equiv 0 \mod p^{n+1}A$): there exists $a_{n+1}\in A$ (that may not be unique when A has p-torsion) such that $x_{n+1}=\sum\limits_{i=0}^{n+1}p^ia_i^{p^{n+1-i}}=\Phi_{n+1}(a_0,\ldots,a_{n+1})$. □

Let $\underline{Y}=(Y_0,Y_1,\ldots)$ be a indeterminate.

Proposition 4.2.10. (*cf* [20, Chap. II, §6, Theorem 5]). There exist unique sequences of polynomials $(S_n)_{n\in\mathbf{Z}_{\geqslant 0}},(P_n)_{n\in\mathbf{Z}_{\geqslant 0}}\in\mathbf{Z}[\underline{X},\underline{Y}]^{\mathbf{Z}_{\geqslant 0}}$ and $(I_n)_{n\in\mathbf{Z}_{\geqslant 0}}\in\mathbf{Z}[\underline{X}]^{\mathbf{Z}_{\geqslant 0}}$ such that:

$$\begin{aligned}S_n(\underline{X},\underline{Y}),P_n(\underline{X},\underline{Y}) &\in\mathbf{Z}[X_0,\ldots,X_n,Y_0,\ldots,Y_n]\\ I_n(\underline{X}) &\in\mathbf{Z}[X_0,\ldots,X_n]\\ \Phi_n\big(S_0(\underline{X},\underline{Y}),\ldots,S_n(\underline{X},\underline{Y})\big) &= \Phi_n(\underline{X})+\Phi_n(\underline{Y})\\ \Phi_n\big(P_0(\underline{X},\underline{Y}),\ldots,P_n(\underline{X},\underline{Y})\big) &= \Phi_n(\underline{X})\Phi_n(\underline{Y})\\ \Phi_n\big(I_0(\underline{X}),\ldots,I_n(\underline{X})\big) &= -\Phi_n(\underline{X})\end{aligned}$$

Proof. • Let $A = \mathbf{Z}[\underline{X}, \underline{Y}]$ be the polynomial ring. Denote by $\varphi\colon A \to A$ the unique ring endomorphism such that $\varphi(X_n) = X_n^p$ and $\varphi(Y_n) = Y_n^p$ for all $n \in \mathbf{Z}_{\geqslant 0}$. We have $\varphi(a) \equiv a^p \mod pA$ for all $a \in A$. As φ is a ring endomorphism and Φ_n has integral coefficients, we have $\varphi(\Phi_n(\underline{X}) + \Phi_n(\underline{Y})) = \Phi_n(\varphi(\underline{X})) + \Phi_n(\varphi(\underline{Y}))$ (resp. $\varphi(\Phi_n(\underline{X})\Phi_n(\underline{Y})) = \Phi_n(\varphi(\underline{X}))\Phi_n(\varphi(\underline{Y}))$, resp. $\varphi(-\Phi_n(\underline{X})) = -\Phi_n(\varphi(\underline{X}))$) for all $n \in \mathbf{Z}_{\geqslant 0}$. As $\Phi_n(\varphi(\underline{X})) = \Phi_{n+1}(\underline{X}) - p^{n+1}X_{n+1}$ and $\Phi_n(\varphi(\underline{Y})) = \Phi_{n+1}(\underline{Y}) - p^{n+1}Y_{n+1}$ by definition, this implies that $\varphi(\Phi_n(\underline{X}) + \Phi_n(\underline{Y})) \equiv \Phi_{n+1}(\underline{X}) + \Phi_{n+1}(\underline{Y}) \mod p^{n+1}A$ (resp. $\varphi(\Phi_n(\underline{X})\Phi_n(\underline{Y})) \equiv \Phi_{n+1}(\underline{X})\Phi_{n+1}(\underline{Y}) \mod p^{n+1}A$, resp. $\varphi(-\Phi_n(\underline{X})) \equiv -\Phi_{n+1}(\underline{X}) \mod p^{n+1}A$) for all $n \in \mathbf{Z}_{\geqslant 0}$. Lemma 4.2.9 thus implies that $\Phi_A(\underline{X}) + \Phi_A(\underline{Y})$, $\Phi_A(\underline{X})\Phi_A(\underline{Y})$ and $-\Phi_A(\underline{X})$ belong to the image of Φ_A, which precisely means the existence of the sequences of polynomials $(S_n)_{n \in \mathbf{Z}_{\geqslant 0}}, (P_n)_{n \in \mathbf{Z}_{\geqslant 0}} \in \mathbf{Z}[\underline{X}, \underline{Y}]^{\mathbf{Z}_{\geqslant 0}}$ and $(I_n)_{n \in \mathbf{Z}_{\geqslant 0}} \in \mathbf{Z}[\underline{X}]^{\mathbf{Z}_{\geqslant 0}}$.
• The unicity is obvious in $\mathbf{Z}[p^{-1}][\underline{X}, \underline{Y}]$ by induction. □

Example 4.2.11. One has

$$\begin{cases} S_0(X_0, Y_0) = X_0 + Y_0 \\ P_0(X_0, Y_0) = X_0 Y_0 \end{cases}$$

and

$$\begin{cases} S_1(X_0, X_1, Y_0, Y_1) = X_1 + Y_1 - \sum\limits_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X_0^i Y_0^{p-i} \\ P_1(X_0, X_1, Y_0, Y_1) = X_1 Y_0^p + X_0^p Y_1 + pX_1 Y_1 \end{cases}$$

Definition 4.2.12. Let A be a ring. Put

$$\mathsf{W}(A) = A^{\mathbf{Z}_{\geqslant 0}}$$

(as a set). If $\underline{a} = (a_0, a_1, \ldots), \underline{b} = (b_0, b_1, \ldots) \in \mathsf{W}(A)$, put

$$\begin{aligned} \underline{a} + \underline{b} &= \big(S_n(\underline{a}, \underline{b})\big)_{n \in \mathbf{Z}_{\geqslant 0}} \\ \underline{a}.\underline{b} &= \big(P_n(\underline{a}, \underline{b})\big)_{n \in \mathbf{Z}_{\geqslant 0}} \\ -\underline{a} &= \big(I_n(\underline{a})\big)_{n \in \mathbf{Z}_{\geqslant 0}} \end{aligned}$$

Remark 4.2.13. The map $\Phi_A\colon A^{\mathbf{Z}_{\geqslant 0}} \to A^{\mathbf{Z}_{\geqslant 0}}$ above is seen as a map $\Phi_A\colon \mathsf{W}(A) \to A^{\mathbf{Z}_{\geqslant 0}}$.

Proposition 4.2.14. (1) $A \mapsto (\mathsf{W}(A), +, .)$ is a functor on **Ring** to the category of sets endowed with two composition laws.
(2) If p is not a zero-divisor (resp. is a unit) in A, then Φ_A is injective (resp. bijective).
(3) $(\mathsf{W}(A), +, .)$ is a commutative ring with zero element $\underline{0} = (0, 0, \ldots)$ and unit $(1, 0, 0, \ldots)$. The map Φ_A is a ring homomorphism.

Proof. (1) and (2) are obvious. For (3), let $B \to A$ be a surjective ring homomorphism, such that p is not a zero-divisor in B (one can take $B = \mathbf{Z}[X_a]_{a \in A}$, and $B \to A$; $X_a \mapsto a$). As Φ_B is injective, $(\mathsf{W}(B), +, .)$ identifies (*via* Φ_B) with a subring of $B^{\mathbf{Z}_{\geqslant 0}}$ (with the product structure). Since $B \to A$ is surjective, so is $\mathsf{W}(B) \to \mathsf{W}(A)$, and $(\mathsf{W}(A), +, .)$ fulfills the ring axioms. □

Definition 4.2.15. Let A be a ring. The *Teichmüller representative* of $a \in A$ is $[a] := (a, 0, 0, \ldots) \in \mathsf{W}(A)$.

Proposition 4.2.16. Let A be a ring. If $a, b \in A$, then $[ab] = [a].[b]$ in $\mathsf{W}(A)$.

Proof. Here again, it is enough to check the equality when A has no p-torsion, hence after applying Φ_A (since it is injective in the p-torsionfree case), but $\Phi_A([a]) = (a, a^p, a^{p^2}, \ldots)$ is multiplicative. □

Proposition 4.2.17. There exists a sequence $(F_n)_{n \in \mathbf{Z}_{\geqslant 0}} \in \mathbf{Z}[\underline{X}]^{\mathbf{Z}_{\geqslant 0}}$ such that $F_n(\underline{X}) \in \mathbf{Z}[X_0, \ldots, X_{n+1}]$ and

$$(\forall n \in \mathbf{Z}_{\geqslant 0})\ \Phi_n\big(F_0(\underline{X}), \ldots, F_n(\underline{X})\big) = \Phi_{n+1}(\underline{X})$$

Proof. As in the proof of proposition 4.2.10, it is enough, using lemma 4.2.9, to check that if $A = \mathbf{Z}[\underline{X}]$, we have $\varphi(\Phi_n(\underline{X})) \equiv \Phi_{n+1}(\underline{X}) \mod p^{n+1}A$ for all $n \in \mathbf{Z}_{\geqslant 0}$, which is trivial. Here again, the unicity in $\mathbf{Z}[p^{-1}][\underline{X}]$ is obvious by induction. □

Example 4.2.18. We have

$$\begin{cases} F_0(X_0, X_1) = X_0^p + pX_1 \\ F_1(X_0, X_1, X_2) = X_1^p + pX_2 - \sum\limits_{i=1}^{p} \binom{p}{i} p^{i-1} X_1^i X_0^{p(p-i)} \end{cases}$$

Definition 4.2.19. Let A be a ring. The *Frobenius map* of $\mathsf{W}(A)$ is

$$F(\underline{a}) = \big(F_0(\underline{a}), F_1(\underline{a}), \ldots\big)$$

Proposition 4.2.20. Let A be a ring.
(1) $(\forall a \in A)\, F([a]) = [a^p]$.
(2) $(\forall n \in \mathbf{Z}_{\geqslant 0})\, F_n(\underline{X}) \equiv X_n^p \mod p\,\mathbf{Z}[\underline{X}]$. In particular, it $pA = 0$, then $F(a_0, a_1, \ldots) = (a_0^p, a_1^p, \ldots)$.

Proof. (1) Considering a surjective ring homomorphism $B \to A$ where B has no p-torsion, which gives rise to a surjective ring homomorphism $\mathsf{W}(B) \to \mathsf{W}(A)$, we may reduce to the case where A has no p-torsion. Then $\Phi_A \colon \mathsf{W}(A) \to A^{\mathbf{Z}_{\geqslant 0}}$ is injective: it is enough to check that $\Phi_A(F([a])) = \Phi_A([a^p])$, *i.e.* that $\Phi_{n+1}([a]) = a^{p^{n+1}} = \Phi_n([a^p])$.
(2) By induction on $n \in \mathbf{Z}_{\geqslant 0}$, the case $n = 0$ following from the equality $F_0(\underline{X}) = X_0^p + pX_1$. Let $n \in \mathbf{Z}_{>0}$ be such that $F_i(\underline{X}) \equiv X_i^p \mod p\,\mathbf{Z}[\underline{X}]$ for $i \in \{0, \ldots, n-1\}$: we have $F_i(\underline{X})^{p^{n-i}} \equiv X_i^{p^{n+1-i}} \mod p^{n+1-i}\,\mathbf{Z}[\underline{X}]$ for $i \in \{0, \ldots, n-1\}$ by lemma 4.2.8, hence

$$\Phi_{n+1}(\underline{X}) = \Phi_n\big(F_0(\underline{X}), \ldots, F_n(\underline{X})\big) = \sum_{i=0}^{n} p^i F_i(\underline{X})^{p^{n-i}} \equiv p^n F_n(\underline{X}) + \sum_{i=0}^{n-1} p^i X_i^{p^{n+1-i}} \mod p^{n+1}\,\mathbf{Z}[\underline{X}]$$

As $\sum\limits_{i=0}^{n-1} p^i X_i^{p^{n+1-i}} = \Phi_{n+1}(\underline{X}) - p^n X_n^p - p^{n+1} X_{n+1}$, this implies that $p^n F_n(\underline{X}) \equiv p^n X_n^p \mod p^{n+1}\,\mathbf{Z}[\underline{X}]$ *i.e.* $F_n(\underline{X}) \equiv X_n^p \mod p\,\mathbf{Z}[\underline{X}]$. □

Definition 4.2.21. Let A be a ring. The *Verschiebung* of $\underline{a} = (a_0, a_1, \ldots) \in \mathsf{W}(A)$ is

$$V(\underline{a}) = (0, a_0, a_1, \ldots)$$

Proposition 4.2.22. Let A be a ring and $\underline{a}, \underline{b} \in \mathsf{W}(A)$.
(1) We have

$$\begin{cases} \Phi_A(F(\underline{a})) = \big(\Phi_1(\underline{a}), \Phi_2(\underline{a}), \ldots\big) = f(\Phi_A(\underline{a})) \\ \Phi_A(V(\underline{a})) = \big(0, p\Phi_0(\underline{a}), p\Phi_1(\underline{a}), \ldots\big) = v(\Phi_A(\underline{a})) \end{cases}$$

where $f(\underline{X}) = (X_1, X_2, \ldots)$ and $v(\underline{X}) = (0, pX_0, pX_1, \ldots)$.
(2) F is a ring endomorphism.
(3) V is an group endomorphism of $(\mathsf{W}(A), +)$.
(4) $FV = p\,\mathsf{Id}_{\mathsf{W}(A)}$ and $VF(\underline{a}) = (0, 1, 0, \ldots).\underline{a}$.
(5) $V(\underline{a}.F(\underline{b})) = V(\underline{a}).\underline{b}$ and $V(\underline{a}).V(\underline{b}) = pV(\underline{a}.\underline{b})$.
(6) $F(\underline{a}) \equiv \underline{a}^p \mod p\,\mathsf{W}(A)$.
(7) $\underline{a} = [a_0] + V(\underline{a}')$ where $\underline{a}' = (a_1, a_2, \ldots)$. In particular $\underline{a} = \sum\limits_{n=0}^{\infty} V^n([a_n])$.

Proof. (1) is computation. Using the usual trick, the proof of properties (2)-(7) reduces to the case when A has no p-torsion, hence after applying Φ_A since the latter is injective. (2) (resp. (3)) follows from the fact that f (resp. v) is a ring (resp. a group) homomorphism. (4) follows from the equality $f \circ v = p$ and $\Phi_A(0, 1, 0, 0, \ldots) = (0, p, p, \ldots)$. (5) follows from the corresponding statements on f and v in $\mathbf{Z}[\underline{X}]^{\mathbf{Z}_{\geqslant 0}}$. To prove (6), we check that $\Phi_A(F(\underline{a})) \equiv \Phi_A(\underline{a}^p) \mod p\,\mathsf{Im}(\Phi_A)$, *i.e.* that $f(\Phi_A(\underline{a})) - \Phi_A(\underline{a}^p) \in p\,\mathsf{Im}(\Phi_A)$. By lemma 4.2.9, this follows from the congrucences

$$\varphi\big(\Phi_{n+1}(\underline{X}) - \Phi_n(\underline{X})^p\big) \equiv \Phi_{n+2}(\underline{X}) - \Phi_{n+1}(\underline{X})^p \mod p^{n+2}\,\mathbf{Z}[\underline{X}],$$

which are obvious since $\varphi(\Phi_n(\underline{X})) = \Phi_{n+1}(\underline{X}) - p^{n+1} X_{n+1}$. Finally, (7) follows from the equalities $\Phi_0(\underline{a}) = a_0$ and $\Phi_n(\underline{a}) = a_0^{p^n} + p\Phi_{n-1}(\underline{a}')$ for all $n \in \mathbf{Z}_{>0}$, which precisely mean that $\Phi_A(\underline{a}) = \Phi_A([a_0] + V(\underline{a}'))$. □

Definition 4.2.23. Let A be a ring. For $n \in \mathbf{Z}_{\geqslant 0}$, let

$$\mathsf{Fil}^n\,\mathsf{W}(A) = V^n(\mathsf{W}(A)) = \big\{(0, \ldots, 0, a_n, a_{n+1}, \ldots)\,;\, (a_k)_{k \geqslant n} \in A^{\mathbf{Z}_{\geqslant n}}\big\} \subset \mathsf{W}(A).$$

This defines a decreasing filtration on $\mathsf{W}(A)$.

As $V^n(\underline{a} + \underline{b}) = V^n(\underline{a}) + V^n(\underline{b})$ and $V^n(\underline{a}).\underline{b} = V^n(\underline{a}.F^n(\underline{b}))$, $\mathsf{Fil}^n\,\mathsf{W}(A)$ is an ideal of $\mathsf{W}(A)$.

Definition 4.2.24. Let A be a ring. The *ring of Witt vectors of length n* is $\mathsf{W}_n(A) := \mathsf{W}(A)/\,\mathsf{Fil}^n\,\mathsf{W}(A)$.

Remark 4.2.25. In general, we have $V^n(\mathsf{W}(A))V^m(\mathsf{W}(A)) \not\subset V^{n+m}(\mathsf{W}(A))$, so the filtration is *not* compatible with the ring structure (however this is true if $pA = 0$).

Proposition 4.2.26. Let A be a ring such that $pA = 0$.
(1) $FV(\underline{a}) = VF(\underline{a}) = p\underline{a} = (0, a_0^p, a_1^p, \ldots)$ (so $(0, 1, 0, 0 \ldots) = p$).
(2) $V^n(\underline{a})V^m(\underline{b}) = V^{n+m}\big(F^m(\underline{a}).F^n(\underline{b})\big)$.
(3) The p-adic and the $V(\mathsf{W}(A))$-adic filtration are the same, and finer than that defined by the filtration. In particular, $\mathsf{W}(A)$ is complete and separated for the p-adic topology.

(4) If A is perfect[37], all these topologies are the same, and $\mathsf{W}(A)/p\,\mathsf{W}(A) \xrightarrow{\sim} A$, and[38]

$$\underline{a} = (a_0, a_1, \ldots) = \sum_{n=0}^{\infty} V^n([a_n]) = \sum_{n=0}^{\infty} V^n F^n\big([a_n^{p^{-n}}]\big) = \sum_{n=0}^{\infty} p^n [a_n^{p^{-n}}]$$

Proof. (1) Follows from proposition 4.2.20 (2): if $\underline{a} = (a_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in \mathsf{W}(A)$, we have $F(\underline{a}) = (a_0^p, a_1^p, \ldots)$, so $VF(\underline{a}) = (0, a_0^p, a_1^p, \ldots) = FV(\underline{a})$, so that $VF = FV = p\,\mathsf{Id}_{\mathsf{W}(A)}$.
By proposition 4.2.22 (5), we have $V(\underline{a}).\underline{b} = V(\underline{a}.F(\underline{b}))$, hence $V^n(\underline{a}).\underline{b} = V^n(\underline{a}.F^n(\underline{b}))$ by an immediate induction on $n \in \mathbf{Z}_{\geqslant 0}$. Applied to $V^m(\underline{b})$ instead of $\underline{b}$, we get $V^n(\underline{a}).V^m(\underline{b}) = V^n\big(\underline{a}.F^nV^m(\underline{b})\big)$. As $F^nV^m(\underline{b}) = V^mF^n(\underline{b})$ (by (1)), we have $\underline{a}.F^nV^m(\underline{b}) = V^m(F^m(\underline{a}).F^n(\underline{b}))$, hence the result.
For (3), one proves by induction that $(V(\mathsf{W}(A)))^k = p^{k-1}V(\mathsf{W}(A))$ (using the second formula of proposition 4.2.22 (5)). As $p\,\mathsf{W}(A) = VF(\mathsf{W}(A)) \subset V(\mathsf{W}(A))$, one has $p^k\,\mathsf{W}(A) \subset (V(\mathsf{W}(A)))^k \subset p^{k-1}\,\mathsf{W}(A)$. Moreover, we have

$$(*) \qquad p^k\,\mathsf{W}(A) = V^nF^n(\mathsf{W}(A)) = \big\{(0,\ldots,0,a_k,a_{k+1},\ldots) \in \mathsf{W}(A)\,;\, (\forall n \in \mathbf{Z}_{\geqslant 0})\, a_n \in A^{p^k}\big\} \subset \mathsf{Fil}^k\,\mathsf{W}(A)$$

so that the p-adic topology is finer that that defined by the filtration $\mathsf{Fil}^\bullet\,\mathsf{W}(A)$.
(4) follows from the fact that $(*)$ is an equality when A is perfect. □

4.2.27. *The mixed characteristic case.* In this paragraph, we assume that $\mathsf{char}(K) = 0$ and $\mathsf{char}(\kappa_K) = p > 0$. As $p \in \mathcal{O}_K$ maps to 0 in κ_K, there exists $e_K \in \mathbf{Z}_{>0}$ such that $p \in \pi^{e_K}\mathcal{O}_K^\times$. As $\mathsf{char}(K) = 0$, we have $\mathbf{Q} \subset K$, so that K is an extension of $\mathbf{Q}_p$.

Definition 4.2.28. The integer e_K is called the *absolute ramification index* of K. It is nothing but the ramification index of the extension $K/\mathbf{Q}_p$. The field K is *absolutely unramified* when $e_K = 1$, *i.e.* when p is a uniformizer of $\mathcal{O}_K$.

Lemma 4.2.29. (Multiplicative representants). There exists a unique map $\rho\colon \kappa_K \to \mathcal{O}_K$ which is a section of the canonical map $\mathcal{O}_K \to \kappa_K$ and such that $\rho(x^p) = \rho(x)^p$ for all $x \in \kappa_K$. This map is multiplicative, *i.e.* $\rho(xy) = \rho(x)\rho(y)$ for all $x, y \in \kappa_K$.

Proof. Existence. • Let $s, s'\colon \kappa_K \to \mathcal{O}_K$ be sections of the canonical map $\mathcal{O}_K \to \kappa_K$ (so that $s(x)$ and $s'(x)$ are liftings of x in $\mathcal{O}_K$). For all $n \in \mathbf{Z}_{\geqslant 0}$, the elements $s\big(x^{p^{-n}}\big)$ and $s'\big(x^{p^{-n}}\big)$ both lift $x^{p^{-n}}$: we have $s\big(x^{p^{-n}}\big) \equiv s'\big(x^{p^{-n}}\big) \mod \pi\mathcal{O}_K$, so that

$$(\clubsuit) \qquad s\big(x^{p^{-n}}\big)^{p^n} \equiv s'\big(x^{p^{-n}}\big)^{p^n} \mod \pi^{n+1}\mathcal{O}_K$$

by an argument analogous to that of the lemma 4.2.8 (using the fact that π divides p). Applied with $s'\colon x \mapsto s\big(x^{p^{-1}}\big)^p$, we get

$$(\spadesuit) \qquad s\big(x^{p^{-n}}\big)^{p^n} \equiv s\big(x^{p^{-n-1}}\big)^{p^{n+1}} \mod \pi^{n+1}\mathcal{O}_K,$$

showing that $\big(s\big(x^{p^{-n}}\big)^{p^n}\big)_{n\in\mathbf{Z}_{\geqslant 0}}$ is a Cauchy sequence in $\mathcal{O}_K$: it converges to a limit $\rho(x) \in \mathcal{O}_K$, which is a lifting of x. Equation $(\clubsuit)$ implies that $\rho(x)$ does not depend on the choice of s.
• Passing to the limit as $n \to \infty$ in $(\spadesuit)$, we get $\rho(x) = \rho\big(x^{p^{-1}}\big)^p$ hence $\rho(x^p) = \rho(x)^p$ for all $x \in \kappa_K$.
• If $x, y \in \kappa_K$, and $n \in \mathbf{Z}_{\geqslant 0}$, the elements $\rho\big((xy)^{p^{-n}}\big)$ and $\rho\big(x^{p^{-n}}\big)\rho\big(y^{p^{-n}}\big)$ both lift $(xy)^{p^{-n}}$ in $\mathcal{O}_K$: we have $\rho\big((xy)^{p^{-n}}\big) \equiv \rho\big(x^{p^{-n}}\big)\rho\big(y^{p^{-n}}\big) \mod \pi\mathcal{O}_K$ so $\rho\big((xy)^{p^{-n}}\big)^{p^n} \equiv \rho\big(x^{p^{-n}}\big)^{p^n}\rho\big(y^{p^{-n}}\big)^{p^n} \mod \pi^{n+1}\mathcal{O}_K$ (by lemma 4.2.8 again), *i.e.* $\rho(xy) \equiv \rho(x)\rho(y) \mod \pi^{n+1}\mathcal{O}_K$ for all $n \in \mathbf{Z}_{\geqslant 0}$, hence $\rho(xy) = \rho(x)\rho(y)$.
Unicity. Let $\rho'\colon \kappa_K \to \mathcal{O}_K$ be a section of the canonical map $\mathcal{O}_K \to \kappa_K$ and such that $\rho'(x^p) = \rho'(x)^p$ for all $x \in \kappa_K$. Using $s = \rho'$, we have $\rho(x) = \lim\limits_{n\to\infty} \rho'\big(x^{p^{-n}}\big)^{p^n} = \rho'(x)$ for all $x \in \kappa_K$, hence $\rho' = \rho$. □

Remark 4.2.30. (1) As the proof shows, the previous statement can be generalized to the following situation: let A be a p-adically separated and complete ring such that the Frobenius endomorphism on A/pA is surjective. Then there exists a unique section $\rho\colon A/pA \to A$ of the canonical map $A \to A/pA$ such that $\rho(x^p) = \rho(x)^p$ for all $x \in A/pa$, and ρ is multiplicative.
(2) Of course, ρ is *not* additive since $\mathsf{char}(K) = 0$.

Proposition 4.2.31. There exists a unique ring homomorphism $\mathsf{W}(\kappa_K) \to \mathcal{O}_K$ that induces the identity on residue fields. It is injective and $\mathcal{O}_K$ is a free $\mathsf{W}(\kappa_K)$-module of rank e_K (in particular, we have $\mathcal{O}_K \simeq \mathsf{W}(\kappa_K)$ when K is absolutely unramified).

[37] This means that the p-th power map $A \to A$ is surjective.

[38] Using proposition 4.2.22 (7).

Proof. Unicity. Let $f\colon \mathsf{W}(\kappa_K)\to\mathcal{O}_K$ be a ring homomorphism inducing the identity on residue fields. The map $\kappa_K\to\mathcal{O}_K;\ x\mapsto f([x])$ is a multiplicative (because the Teichmüller map is), and it is a section of the canonical map $\mathcal{O}_K\to\kappa_K$ (because f induces the identity on residue fields). By unicity in lemma 4.2.29, we have $f([x])=\rho(x)$ for all $x\in\kappa_K$. Now if $\underline{a}=(a_0,a_1,\ldots)\in\mathsf{W}(\kappa_K)$, we have $\underline{a}=\sum\limits_{n=0}^{\infty}p^n\big[a_n^{p^{-n}}\big]$ (*cf* proposition 4.2.26 (4)): by continuity of f (since $f(p^m\,\mathsf{W}(\kappa_K))\subset p^m\mathcal{O}_K$ for all $m\in\mathbf{Z}_{\geqslant0}$), we have

$$f(\underline{a})=\sum_{i=0}^{\infty}p^i\rho\big(a_i^{p^{-i}}\big)\qquad(✠)$$

which proves unicity.

Existence. We have to show that the map $f\colon\mathsf{W}(\kappa_K)\to\mathcal{O}_K$ given by formula (✠) is indeed a ring homomorphism that induces the identity on residue fields.

- If $\underline{a}=(a_0,a_1,\ldots)\in\mathsf{W}(\kappa_K)$, the image of $\underline{a}$ in $\kappa_K=\mathsf{W}(\kappa_K)/pW(\kappa_K)$ is a_0 (*cf* proposition 4.2.26 (4)), and that of $f(\underline{a})$ is that of $\rho(a_0)$ *i.e.* a_0: this shows that f induces the identity on residue fields. Formula (✠) also implies that for all $n\in\mathbf{Z}_{\geqslant0}$, we have $f(p^n\,\mathsf{W}(\kappa_K))=f(V^n(\mathsf{W}(\kappa_K)))\subset p^n\mathcal{O}_K$, so that f is continuous for the p-adic topology.
- Let $n\in\mathbf{Z}_{\geqslant0}$. By definitions of Witt vectors, the map $\Phi_n\colon\mathsf{W}(\mathcal{O}_K/p^{n+1}\mathcal{O}_K)\to\mathcal{O}_K/p^{n+1}\mathcal{O}_K$ is a ring homomorphism. Let $\underline{a}=(a_i)_{i\in\mathbf{Z}_{\geqslant0}},\underline{b}=(b_i)_{i\in\mathbf{Z}_{\geqslant0}}\in\mathsf{W}(\mathcal{O}_K/p^{n+1}\mathcal{O}_K)$ such that $a_i\equiv b_i\mod p\mathcal{O}_K/p^{n+1}\mathcal{O}_K$ for all $i\in\mathbf{Z}_{\geqslant0}$: lemma 4.2.8 implies that $a_i^{p^{n-i}}\equiv b_i^{p^{n-i}}\mod p^{n-i+1}\mathcal{O}_K/p^{n+1}\mathcal{O}_K$, so that $p^ia_i^{p^{n-i}}=p^ib_i^{p^{n-i}}$ for all $i\in\mathbf{Z}_{\geqslant0}$. This implies that $\Phi_n(\underline{a})$ only depends on the image of $\underline{a}$ in $\mathsf{W}(\mathcal{O}_K/p\mathcal{O}_K)$, which means that Φ_n factors through a ring homomorphism $\widetilde{\Phi}_n\colon\mathsf{W}(\mathcal{O}_K/p\mathcal{O}_K)\to\mathcal{O}_K/p^{n+1}\mathcal{O}_K$.

$$\begin{tikzcd}
\mathsf{W}(\mathcal{O}_K/p^{n+1}\mathcal{O}_K) \arrow[r, "\Phi_n"] \arrow[d] & \mathcal{O}_K/p^{n+1}\mathcal{O}_K \\
\mathsf{W}(\mathcal{O}_K/p\mathcal{O}_K) \arrow[ur, "\widetilde{\Phi}_n"'] &
\end{tikzcd}$$

For the same reason, if $\underline{a}=(a_i)_{i\in\mathbf{Z}_{\geqslant0}},\underline{b}=(b_i)_{i\in\mathbf{Z}_{\geqslant0}}\in\mathsf{W}(\mathcal{O}_K/p\mathcal{O}_K)$ such that $a_i\equiv b_i\mod\pi\mathcal{O}_K/p\mathcal{O}_K$ for all $i\in\mathbf{Z}_{\geqslant0}$, we have $a_i^{p^k}=b_i^{p^k}$ in $\mathcal{O}_K/p\mathcal{O}_K$ if $k\in\mathbf{Z}_{\geqslant e_K-1}$, so that $F^k(\underline{a})$ only depends on the image of $\underline{a}$ in $\mathsf{W}(\kappa_K)$ (recall that since $\mathcal{O}_K/p\mathcal{O}_K$ has characteristic p, the Frobenius map on $\mathsf{W}(\mathcal{O}_K/p\mathcal{O}_K)$ is just raising the components to the p-th power): the ring endomorphism F^k factors through a ring homomorphism $\varphi_k\colon\mathsf{W}(\kappa_K)\to\mathsf{W}(\mathcal{O}_K/p\mathcal{O}_K)$.

$$\begin{tikzcd}
\mathsf{W}(\mathcal{O}_K/p\mathcal{O}_K) \arrow[r, "F^k"] \arrow[d] & \mathsf{W}(\mathcal{O}_K/p\mathcal{O}_K) \\
\mathsf{W}(\kappa_K) \arrow[ur, "\varphi_k"'] &
\end{tikzcd}$$

Now let $\underline{a}=(a_0,a_1,\ldots)\in\mathsf{W}(\kappa_K)$. As $(\rho(a_i)\mod p\mathcal{O}_K)_{i\in\mathbf{Z}_{\geqslant0}}\in\mathsf{W}(\mathcal{O}_K/p\mathcal{O}_K)$ maps to $\underline{a}\in\mathsf{W}(\kappa_K)$, we have $\varphi_k(\underline{a})=F^k\big((\rho(a_i)\mod p\mathcal{O}_K)_{i\in\mathbf{Z}_{\geqslant0}}\big)=\big(\rho\big(a_i^{p^k}\big)\mod p\mathcal{O}_K\big)_{i\in\mathbf{Z}_{\geqslant0}}$ (here again, we used the fact the F is the Frobenius map on components in $\mathsf{W}(\mathcal{O}_K/p\mathcal{O}_K)$, and that ρ commutes to p-th powers). Similarly, as $\big(\rho\big(a_i^{p^k}\big)\mod p^{n+1}\mathcal{O}_K\big)_{i\in\mathbf{Z}_{\geqslant0}}$ maps to $\big(\rho\big(a_i^{p^k}\big)\mod p\mathcal{O}_K\big)_{i\in\mathbf{Z}_{\geqslant0}}$ in $\mathsf{W}(\mathcal{O}_K/p\mathcal{O}_K)$, we have

$$\begin{aligned}
(\widetilde{\Phi}_n\circ\varphi_k)(\underline{a})=\widetilde{\Phi}_n\Big(\big(\rho\big(a_i^{p^k}\big)\mod p\mathcal{O}_K\big)_{i\in\mathbf{Z}_{\geqslant0}}\Big)&=\Phi_n\Big(\big(\rho\big(a_i^{p^k}\big)\mod p^{n+1}\mathcal{O}_K\big)_{i\in\mathbf{Z}_{\geqslant0}}\Big)\\
&=\sum_{i=0}^{n}p^i\rho\big(a_i^{p^k}\big)^{p^{n-i}}\mod p^{n+1}\mathcal{O}_K\\
&=(f\circ F^{n+k})(\underline{a})\mod p^{n+1}\mathcal{O}_K
\end{aligned}$$

which shows that

$$f\equiv\widetilde{\Phi}_n\circ\varphi_k\circ F^{-n-k}\mod p^{n+1}\mathcal{O}_K$$

for all $k\geqslant e_K-1$. This implies that $f\mod p^{n+1}\mathcal{O}_K$ is a ring homomorphism for all $n\in\mathbf{Z}_{\geqslant0}$, so f is a ring homomorphism (because $\mathcal{O}_K$ is separated for the p-adic topology).

- As f induce the identity on residue fields, we have $\mathsf{Ker}(f)\subset p\,\mathsf{W}(\kappa_K)$: as $\mathcal{O}_K$ has no p-torsion, this implies that $\mathsf{Ker}(f)\subset p^n\,\mathsf{W}(\kappa_K)$ for all $n\in\mathbf{Z}_{\geqslant0}$ by induction, so that $\mathsf{Ker}(f)\subset\bigcap\limits_{n=1}^{\infty}p^n\,\mathsf{W}(\kappa_K)=\{0\}$, and f is injective.
- Passing to fraction fields, we have an extension of local fields $K/\mathsf{W}(\kappa_K)[p^{-1}]$. The residue extension is trivial, and the index of ramification is e_K: by theorem 3.8.4, we have $[K:\mathsf{W}(\kappa_K)[p^{-1}]]=e_K$, and by theorem 3.8.23, the $\mathsf{W}(\kappa_K)$-module $\mathcal{O}_K=\mathsf{W}(\kappa_K)[\pi]$ is free of rank e_K. □

Corollary 4.2.32. $\mathcal{O}_K$ is isomorphic to $\mathsf{W}(\kappa_K)[X]/\langle E(X)\rangle$ where $E(X)\in\mathsf{W}(\kappa_K)[X]$ is an Eisenstein polynomial.

4.3. **Ramification groups.** The content of this section is taken from [20, Chapitre IV]. Henceforth, K denotes a complete discrete valuation field, and L/K a finite and Galois extension, with group G. We assume that the residual extension κ_L/κ_K is separable (this is automatic when K is a local field). Let T the maximal unramified subextension of L/K. Denote by v_L (resp. v_K) the normalized valuation on L (resp. K), so that $v_K = e_{L/K}v_{L|K}$.

4.3.1. *First definitions.* By proposition 3.8.5, there exists $\alpha\in\mathcal{O}_L$ such that $\mathcal{O}_L=\mathcal{O}_K[\alpha]$.

Notation. If $\gamma\in G$, we put $i_G(\gamma)=v_L(\gamma(\alpha)-\alpha)\in\mathbf{Z}_{\geqslant 0}$. If $i\in\mathbf{Z}_{\geqslant -1}$, we put

$$G_i=\{\gamma\in G\,;\,(\forall x\in\mathcal{O}_L)\,v_L(\gamma(x)-x)\geqslant i+1\}.$$

Proposition 4.3.2. Let $\gamma\in G$ and $i\in\mathbf{Z}_{\geqslant -1}$. The following conditions are equivalent:

(i) γ acts trivially on $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$;

(ii) $\gamma\in G_i$;

(iii) $i_G(\gamma)\geqslant i+1$.

In particular, i_G does not depend on the choice of $\alpha\in\mathcal{O}_L$ such that $\mathcal{O}_L=\mathcal{O}_K[\alpha]$. Moreover, $(G_i)_{i\in\mathbf{Z}_{\geqslant -1}}$ is a decreasing sequence of normal subgroups of G such that $G_i=\{\mathsf{Id}_L\}$ for $i\gg 0$.

Proof. (i)⇔(ii) by definition and (ii)⇔(iii) is trivial. We have $i_G^{-1}(\{i\})=G_{i-1}\backslash G_i$ for all $i\in\mathbf{Z}_{\geqslant 0}$, showing that i_G does not depend of the choice of α. Finally, $G_i=\mathsf{Ker}\big(G\to\mathsf{Aut}(\mathcal{O}_L/\mathfrak{m}_L^{i+1})\big)$ so G_i is a normal subgroup of G, and $G_i=\{\mathsf{Id}_L\}$ id $i\geqslant\max\limits_{\gamma\in G\backslash\{\mathsf{Id}_L\}}i_G(\gamma)$. □

Example 4.3.3. We have $G_{-1}=G$ and $G_0=\mathsf{Gal}(L/T)$ is the inertia subgroup of L/K.

Definition 4.3.4. The subgroup G_i is called the *i-th ramification subgroup* (with lower numbering) of G. The groups $(G_i)_{i\in\mathbf{Z}_{\geqslant -1}}$ form a decreasing filtration on G.

Proposition 4.3.5. (Ramification subgroups with lower numbering are compatible with subgroups). Let $H\leqslant G$ be a subgroup and $M=L^H$ (so that $H=\mathsf{Gal}(L/M)$). Then $i_H(\eta)=i_G(\eta)$ for all $\eta\in H$, and $H_i=H\cap G_i$ for all $i\in\mathbf{Z}_{\geqslant -1}$.

Proof. Follows immediately from characterisation (i) of proposition 4.3.2. □

Proposition 4.3.6. Let $H\trianglelefteqslant G$ be a normal subgroup, $M=L^H$ and $\sigma\in G/H=\mathsf{Gal}(M/K)$. Then $i_{G/H}(\sigma)=\frac{1}{e_{L/M}}\sum\limits_{\substack{\gamma\in G\\ \gamma\mapsto\sigma}}i_G(\gamma)$.

Proof. Both sides are equal to $+\infty$ when $\sigma=\mathsf{Id}_M$: assume that $\sigma\neq\mathsf{Id}_M$. Let $\beta\in\mathcal{O}_M$ be such that $\mathcal{O}_M=\mathcal{O}_K[\beta]$: we have $i_{G/H}(\sigma)=v_M(\sigma(\beta)-\beta)$ so that $e_{L/M}i_{G/H}(\sigma)=v_L(\sigma(\beta)-\beta)$. If $\gamma_0\in G$ maps to $\sigma\in G/H$, the others preimages are of the form $\gamma_0\eta$ with $\eta\in H$: we have to prove that $a=\prod\limits_{\eta\in H}(\alpha-\gamma_0\eta(\alpha))$ and $b=\sigma(\beta)-\beta$ have the same valuation, *i.e.* that they generate the same ideal in $\mathcal{O}_L$.

- Let $P\in\mathcal{O}_M[X]$ be the minimal polynomial of α over M: we have $P(X)=\prod\limits_{\eta\in H}(X-\eta(\alpha))$, so that $\sigma(P)(X)=\prod\limits_{\eta\in H}(X-\gamma_0\eta(\alpha))$, *i.e.* $a=\sigma(P)(\alpha)=\sigma(P)(\alpha)-P(\alpha)$. As the coefficients of $\sigma(P)-P$ are divisible by b, we have $a\in b\mathcal{O}_L$.
- To prove that $b\in a\mathcal{O}_L$, write $\beta=Q(\alpha)$, with $Q\in\mathcal{O}_K[X]$. The polynomial $Q(X)-\beta\in\mathcal{O}_M[X]$ vanishes at α: it is divisible by P in $\mathcal{O}_M[X]$. Write $Q(X)-\beta=P(X)D(X)$ with $D\in\mathcal{O}_M[X]$. As $Q\in\mathcal{O}_K[X]$, we have $\sigma(Q)=Q$, so $Q(X)-\sigma(\beta)=\sigma(P)(X)\sigma(D)(X)$: evaluating at α gives $Q(\alpha)-\sigma(\beta)=\sigma(P)(\alpha)\sigma(D)(\alpha)$, *i.e.* $b\in a\mathcal{O}_L$ since $Q(\alpha)-\sigma(\beta)=-b$ and $\sigma(P)(\alpha)=a$. □

Corollary 4.3.7. If $H=G_j$ with $j\in\mathbf{Z}_{\geqslant 0}$, we have

$$(G/H)_i=\begin{cases}G_i/H & \text{if } i\leqslant j\\ \{\mathsf{Id}_M\} & \text{if } i\geqslant j\end{cases}.$$

Proof. Let $\sigma\in G/H\backslash\{\mathsf{Id}_M\}$, there exists a unique $i<j$ such that $\sigma\in(G_i/H)\backslash(G_{i+1}/H)$. If $\gamma\in G$ maps to $\sigma\in G/H$, then $\gamma\in G_i\backslash G_{i+1}$, whence $i_G(\gamma)=i+1$. Moreover, as $j\geqslant 0$, we have $H\leqslant G_0$, so that L/M is totally ramified, *i.e.* $e_{L/M}=[L:M]=\#H$. Proposition 4.3.6 implies thus that $i_{G/H}(\sigma)=i+1$, so that the filtration $(G_i/H)_{i\leqslant j}$ coincides with $((G/H)_i)_{i\leqslant j}$. As moreover $(G/H)_j=G_j/H=\{\mathsf{Id}_M\}$, we also have $(G/H)_i=\{\mathsf{Id}_M\}$ if $i\geqslant j$. □

Remark 4.3.8. For a general normal subgroup $H \trianglelefteq G$, ramification groups of G/H are also images of ramification groups of G in G/H, but one needs to modify the numbering (see theorem 4.3.31).

Theorem 4.3.9. We have

$$v_L(\mathfrak{D}_{L/K}) = \sum_{\gamma\in G\backslash\{\mathsf{Id}_L\}} i_G(\gamma) = \sum_{i=0}^{\infty}(\#G_i - 1)$$

(as $G_i = \{\mathsf{Id}_L\}$ for $i \gg 0$, the sum is finite).

Proof. • Let $P \in \mathcal{O}_K[X]$ be the minimal polynomial of α over K. We have $\mathfrak{D}_{L/K} = P'(\alpha)\mathcal{O}_L$ by proposition 2.5.7 (because $\mathcal{O}_L = \mathcal{O}_K[\alpha]$). As $P(X) = \prod\limits_{\gamma\in G}(X - \gamma(\alpha))$, we have $P'(\alpha) = \prod\limits_{\gamma\in G\backslash\{\mathsf{Id}_L\}}(\alpha - \gamma(\alpha))$, proving the first formula.

• $\sum\limits_{\gamma\in G\backslash\{\mathsf{Id}_L\}} i_G(\gamma) = \sum\limits_{i=0}^{\infty}(i+1)(\#G_i - \#G_{i+1}) = \sum\limits_{i=0}^{\infty}(i+1)(\#G_i - 1) - \sum\limits_{i=0}^{\infty}(i+1)(\#G_{i+1}-1) = \sum\limits_{i=0}^{\infty}(\#G_i - 1).$ □

Remark 4.3.10. We recover the fact that L/K is unramified if and only if $\mathfrak{D}_{L/K} = \mathcal{O}_L$.

Corollary 4.3.11. Let $H \leqslant G$ be a subgroup and $M = L^H$. We have $v_M(\mathfrak{D}_{M/K}) = \frac{1}{e_{L/M}} \sum\limits_{\gamma\in G\backslash H} i_G(\gamma)$.

Proof. By proposition 4.3.9, we have $v_L(\mathfrak{D}_{L/K}) = \sum\limits_{\gamma\in G\backslash\{\mathsf{Id}_L\}} i_G(\gamma)$ and $v_L(\mathfrak{D}_{L/M}) = \sum\limits_{\gamma\in H\backslash\{\mathsf{Id}_L\}} i_G(\gamma)$. By the transitivity of different (*cf* proposition 2.5.10), we have $\mathfrak{D}_{L/K} = \mathfrak{D}_{L/M}\mathfrak{D}_{M/K}$, whence

$$e_{L/M}v_M(\mathfrak{D}_{M/K}) = v_L(\mathfrak{D}_{M/K}) = v_L(\mathfrak{D}_{L/K}) - v_L(\mathfrak{D}_{L/M}) = \sum_{\gamma\in G\backslash H} i_G(\gamma).$$

□

4.3.12. *The quotients G_i/G_{i+1}.* Let π be a uniformizer of L. Recall (*cf* section 3.7.7) that we defined a filtration of $\mathcal{O}_L^\times$ by subgroups

$$U_L^{(i)} := \begin{cases} \mathcal{O}_L^\times & \text{if } i = 0 \\ 1 + \mathfrak{m}_L^i & \text{if } i \in \mathbf{Z}_{>0}\end{cases}$$

This is a basis of neighbourhoods of 1 in $\mathcal{O}_L^\times$ for the topology induced by that on $L^\times$. As $\mathcal{O}_L^\times$ is closed hence complete, we have $\mathcal{O}_L^\times = \varprojlim\limits_i \mathcal{O}_L^\times/U_L^{(i)}$.

Lemma 4.3.13. Let $\gamma \in G_0 = \mathsf{Gal}(L/T)$ and $i \in \mathbf{Z}_{\geqslant 0}$. We have $\gamma \in G_i \Leftrightarrow \frac{\gamma(\pi)}{\pi} \in U_L^{(i)}$.

Proof. By proposition 4.3.5 applied with $H = G_0$, we have $(G_0)_i = G_i$ (since $i \geqslant 0$). As $\mathcal{O}_L = \mathcal{O}_T[\pi]$ (theorem 3.8.23), we have $i_{G_0}(\gamma) = \gamma(\pi) - \pi$, *i.e.* $\gamma \in G_i \Leftrightarrow v_L(\gamma(\pi) - \pi) \geqslant i + 1 \Leftrightarrow \frac{\gamma(\pi)}{\pi} \equiv 1 \mod \mathfrak{m}_L^i$. □

Proposition 4.3.14. If $i \in \mathbf{Z}_{\geqslant 0}$, the map $\gamma \mapsto \frac{\gamma(\pi)}{\pi}$ induces as isomorphism θ_i from G_i/G_{i+1} onto a subgroup of $U_L^{(i)}/U_L^{(i+1)}$. This isomorphism is independent of the choice of π.

Proof. • If π' is another uniformizer, we have $\pi' = u\pi$ with $u \in \mathcal{O}_L^\times$, so that $\frac{\gamma(\pi')}{\pi'} = \frac{\gamma(u)}{u}\frac{\gamma(\pi)}{\pi}$. If $\gamma \in G_i$, we have $\gamma(u) - u \in \mathfrak{m}_L^{i+1}$, so $\frac{\gamma(u)}{u} \equiv 1 \mod \mathfrak{m}_L^{i+1}$, showing that θ_i does not depend on the choice of π.

• If $\gamma_1, \gamma_2 \in G_i$, we have $\frac{(\gamma_1\gamma_2)(\pi)}{\pi} = \frac{\gamma_1(\pi)}{\pi}\frac{\gamma_2(\pi)}{\pi}\frac{\gamma_1(u)}{u}$ with $u = \frac{\gamma_2(\pi)}{\pi} \in \mathcal{O}_L^\times$. As $\frac{\gamma_1(u)}{u} \equiv 1 \mod \mathfrak{m}_L^{i+1}$ (*cf* above), we get $\frac{(\gamma_1\gamma_2)(\pi)}{\pi} \equiv \frac{\gamma_1(\pi)}{\pi}\frac{\gamma_2(\pi)}{\pi} \mod \mathfrak{m}_L^{i+1}$, showing that θ_i is a group homomorphism. It is obviously injective. □

Corollary 4.3.15. (1) The group G_0/G_1 is cyclic, and identifies (*via* θ_0) to a subgroup of the group of roots of unity in $\kappa_L^\times$. Its order is prime to $\mathsf{char}(\kappa_L)$.
(2) If $\mathsf{char}(\kappa_L) = 0$, then $G_1 = \{\mathsf{Id}_L\}$, so G_0 is cyclic.
(3) If $\mathsf{char}(\kappa_L) = p > 0$, and $i \in \mathbf{Z}_{>0}$, the group G_i/G_{i+1} is a $\mathbf{F}_p$-vector space of finite dimension. In particular G_1 is a p-group.

Proof. (1) By proposition 4.3.14, the map θ_0 induces an isomorphism from G_0/G_1 onto a subgroup of $U_L^{(0)}/U_L^{(1)} \xrightarrow{\sim} \kappa_L^\times$ (*cf* proposition 3.7.10). Finite subgroups of $\kappa_L^\times$ are cyclic, made of roots of unity, of order prime to $\mathsf{char}(\kappa_L)$.
(2) By proposition 4.3.14, θ_i induces an isomorphism from G_i/G_{i+1} onto a subgroup of $U_L^{(i)}/U_L^{(i+1)} \xrightarrow{\sim} \kappa_L$ (*cf* proposition 3.7.10). If $\mathsf{char}(\kappa_L) = 0$, the additive group κ_L has no torsion, so that $G_i/G_{i+1} = \{0\}$: this implies that $G_i = G_1$ for all $i \in \mathbf{Z}_{>0}$. As $G_i = \{\mathsf{Id}_L\}$ for $i \gg 0$, we deduce that $G_1 = \{\mathsf{Id}_L\}$, so that $G_0 \xrightarrow{\sim} G_0/G_1$ is cyclic.

(3) If $\mathsf{char}(\kappa_L) = p > 0$, the group $\theta_i(G_i/G_{i+1})$ identifies with a subgroup of the additive group κ_L, which is killed by p: so is G_i/G_{i+1}, which is thus a $\mathbf{F}_p$-vector space, necessarily of finite dimension. □

Corollary 4.3.16. If $\mathsf{char}(\kappa_L) = p > 0$, the group G_0 is a semi-direct product of cyclic subgroup of order prime to p by a normal subgroup of order a power of p. In particular, the group G_0 is solvable. If moreover κ_L is finite, the group G is solvable.

Proof. By corollary 4.3.15, it is enough to show that there exists a subgroup H of G_0 which projects isomorphically onto G_0/G_1. Let $\gamma \in G_0$ whose image in G_0/G_1 is a generator. Put $\#(G_0/G_1) = m$ and $\#G_1 = p^r$. As $p \nmid m$, there exists $N \in \mathbf{Z}_{\geqslant r}$ such that $p^N \equiv 1 \mod m\mathbf{Z}$. Put $\sigma = \gamma^{p^N} \in G_0$. As we have $p^N \equiv 1 \mod m$, the images of γ and σ in G_0/G_1 are the same. Moreover, we have $\#G_0 = mp^r \mid mp^N$ (since $N \geqslant r$), so that $\sigma^m = \gamma^{mp^N} = \mathsf{Id}_L$, showing that the order of σ in G_0 divides m. As it is at least m since the image of σ generates G_0/G_1, it has to be m, thus $H := \langle\sigma\rangle \simeq \mathbf{Z}/m\mathbf{Z}$.
If κ_L is finite, then $G/G_0 \simeq \mathsf{Gal}(\kappa_L/\kappa_K)$ is cyclic, so G is solvable. □

Corollary 4.3.17. Assume k is algebraically closed of characteristic 0, and let $K = k(\!(T)\!)$. An algebraic closure $\overline{K}$ of K is the union of the subfields $K_n := k(\!(T^{1/n})\!)$ for all $n \in \mathbf{Z}_{>0}$, and $\mathsf{Gal}(\overline{K}/K) \simeq \widehat{\mathbf{Z}} := \varprojlim_{n} \mathbf{Z}/n\mathbf{Z}$.

Proof. As k is algebraically closed, we have $G = G_0$ for every finite subextension L of $\overline{K}/K$, and corollary 4.3.15 (2) shows that G is cyclic. If L' is another finite extension of K such that $[L : K] \mid [L' : K]$, the composite extension LL'/K is cyclic: we have $\mathsf{Gal}(LL'/L') \leqslant \mathsf{Gal}(LL'/L)$, which shows that $L \subset L'$. This shows in particular that $K_n \subset L$ *i.e.* $L = K_n$ with $n = [L : K]$. □

Let $i \in \mathbf{Z}_{\geqslant 0}$. As G_i and G_{i+1} are normal subgroups of G_0, the latter acts by conjugation on G_i/G_{i+1}.

Proposition 4.3.18. Let $\gamma \in G_0$ and $\overline{\sigma} \in G_i/G_{i+1}$, where $i \in \mathbf{Z}_{\geqslant 0}$. Then

$$\theta_i(\gamma\overline{\sigma}\gamma^{-1}) = \theta_0(\gamma)^i\theta_i(\overline{\sigma})$$

(here we see $\theta_0(\gamma)$ as an element of $\kappa_L^\times$, acting on the one dimensional κ_L-vector space $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$).

Proof. Let $\sigma \in G_i$ be a lifting of $\overline{\sigma}$ and $\pi' = \gamma^{-1}(\pi)$ (this is a uniformizer of L). We have $\sigma(\pi') = \pi'(1+a)$ with $a \in \mathfrak{m}_L^i$, and $\theta_i(\overline{\sigma})$ is the image $\overline{a}$ of a in $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$. Applying γ, we have $(\gamma\sigma\gamma^{-1})(\pi) = \gamma(\pi')(1+\gamma(a))$, *i.e.* $\frac{(\gamma\sigma\gamma^{-1})(\pi)}{\pi} = 1+\gamma(a)$, so that $\theta_i(\gamma\overline{\sigma}\gamma^{-1})$ is the image of $\gamma(a)$ in $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$. Write $a = b\pi^i$ with $b \in \mathcal{O}_L$, so that $\gamma(a) = \gamma(b)\gamma(\pi)^i$. As $\gamma \in G_0$, we have $\gamma(b) \equiv b \mod \mathfrak{m}_L$, so that $\gamma(a) \equiv \big(\frac{\gamma(\pi)}{\pi}\big)^i a \mod \mathfrak{m}_L^{i+1}$, *i.e.* the image of $\gamma(a)$ in $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$ is $\theta_0(\gamma)^i\theta_i(\overline{\sigma})$. □

Corollary 4.3.19. Let $\gamma \in G_0$ and $\sigma \in G_i$ with $i \in \mathbf{Z}_{>0}$. Then $\gamma\sigma\gamma^{-1}\sigma^{-1} \in G_{i+1}$ if and only if $\gamma^i \in G_1$ or $\sigma \in G_{i+1}$.

Proof. We have $\gamma\sigma\gamma^{-1}\sigma^{-1} \in G_{i+1}$ if and only if $\gamma\sigma\gamma^{-1}$ and σ have same image in G_i/G_{i+1}: by injectivity of θ_i, this is equivalent to $\theta_i(\gamma\sigma\gamma^{-1}) = \theta_i(\sigma)$, *i.e.* $\theta_0(\gamma)^i\theta_i(\sigma) = \theta_i(\sigma)$ in $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$. As $i > 0$, the latter is a κ_L-vector space of dimension 1: this is equivalent to $\theta_0(\gamma)^i = 1$ (*i.e.* $\gamma^i \in \mathsf{Ker}(\theta_0)$) or $\theta_i(\sigma) = 0$ (*i.e.* $\sigma \in \mathsf{Ker}(\theta_i)$), *i.e.* to $\gamma^i \in G_1$ or $\sigma \in G_{i+1}$. □

Corollary 4.3.20. Assume G is abelian. If $\#(G_0/G_1) \nmid i$, we have $G_i = G_{i+1}$.

Proof. Fix $\gamma \in G_0$ mapping to a generator of G_0/G_1. If $\sigma \in G_i$, we have $\gamma\sigma\gamma^{-1}\sigma^{-1} = \mathsf{Id}_L \in G_{i+1}$, so that $\gamma^i \in G_1$ or $\sigma \in G_{i+1}$ by corollary 4.3.19: as $\gamma^i \notin G_1$ since $\#(G_0/G_1) \nmid i$, we must have $\sigma \in G_{i+1}$, *i.e.* $G_i = G_{i+1}$. □

Proposition 4.3.21. (1) Integers $i \in \mathbf{Z}_{\geqslant 1}$ such that $G_i \neq G_{i+1}$ are congruent modulo $p = \mathsf{char}(\kappa_L)$.
(2) Let $i, j \in \mathbf{Z}_{\geqslant 1}$, $\gamma \in G_i$ and $\sigma \in G_j$. Then $\gamma\sigma\gamma^{-1}\sigma^{-1} \in G_{i+j+1}$.

Lemma 4.3.22. Let $i, j \in \mathbf{Z}_{\geqslant 1}$, $\gamma \in G_i$ and $\sigma \in G_j$. Then $\gamma\sigma\gamma^{-1}\sigma^{-1} \in G_{i+j}$ and

$$\theta_{i+j}(\gamma\sigma\gamma^{-1}\sigma^{-1}) = (j-i)\theta_i(\gamma)\theta_j(\sigma).$$

Proof. Write $\gamma(\pi) = \pi(1+a)$ and $\sigma(\pi) = \pi(1+b)$ with $a = x\pi^i \in \mathfrak{m}_L^i$ and $b = y\pi^j \in \mathfrak{m}_L^j$, where $x, y \in \mathcal{O}_L$. We get $(\gamma\sigma)(\pi) = \pi(1+a)(1+\gamma(b)) = \pi(1+a+\gamma(b)+a\gamma(b))$. As $\gamma(b) = \gamma(y)\gamma(\pi)^j = \gamma(y)\pi^j(1+a)^j$, $\gamma(y) \equiv y \mod \mathfrak{m}_L^{i+1}$ and $(1+a)^j \equiv 1+ja \mod \mathfrak{m}_L^{i+1}$ (since $i > 0$), we have $\gamma(b) \equiv y\pi^j(1+ja) \mod \mathfrak{m}_L^{i+j+1}$, *i.e.* $\gamma(b) \equiv b + jab \mod \mathfrak{m}_L^{i+j+1}$. This implies that $(\gamma\sigma)(\pi) \equiv \pi(1+c)$ with $c \equiv a+b+(j+1)ab \mod \mathfrak{m}_L^{i+j+1}$. Similarly, we have $(\sigma\gamma)(\pi) = \pi(1+d)$ with $d \equiv a+b+(i+1)ab \mod \mathfrak{m}_L^{i+j+1}$.
Put $\pi' = \sigma\gamma(\pi)$: this is a uniformizer of L, and

$$(\gamma\sigma\gamma^{-1}\sigma^{-1})(\pi') = (\gamma\sigma)(\pi) = \pi(1+c) = \pi'(1+c)(1+d)^{-1} = \pi'(1+e)$$

where $e = (1+c)(1+d)^{-1} \equiv 1+c-d \mod \mathfrak{m}_L^{i+j+1}$, *i.e.* $e \equiv (j-i)ab \mod \mathfrak{m}_L^{i+j+1}$. This shows that $\frac{(\gamma\sigma\gamma^{-1}\sigma^{-1})(\pi')}{\pi'} - 1 \in \mathfrak{m}_K^{i+j}$ (since $a \in \mathfrak{m}_L^i$ and $b \in \mathfrak{m}_L^j$), and that $\theta_{i+j}(\gamma\sigma\gamma^{-1}\sigma^{-1})$ is the image of $(j-i)ab$ in $\mathfrak{m}_L^{i+1}/\mathfrak{m}_L^{i+j+1}$, *i.e.* $\theta_{i+j}(\gamma\sigma\gamma^{-1}\sigma^{-1}) = (j-i)\theta_i(\gamma)\theta_j(\sigma)$. □

Proof of proposition 4.3.21. (1) If $G_1 = \{\mathsf{Id}_L\}$, there is nothing to do: assume that $G_1 \neq \{\mathsf{Id}_L\}$, so that $\mathsf{char}(\kappa_L) = p > 0$. Let $j \in \mathbf{Z}_{>0}$ be the integer such that $G_j \neq \{\mathsf{Id}_L\}$ and $G_{j+1} = \{\mathsf{Id}_L\}$. Let $i \in \mathbf{Z}_{>0}$ be such that $G_i \neq G_{i+1}$. Let $\gamma \in G_i \backslash G_{i+1}$ and $\sigma \in G_j \backslash \{\mathsf{Id}_L\}$. By lemma 4.3.22, we have $\gamma\sigma\gamma^{-1}\sigma^{-1} \in G_{i+j} = \{\mathsf{Id}_L\}$, so that $\theta_{i+j}(\gamma\sigma\gamma^{-1}\sigma^{-1}) = 0$. By lemma 4.3.22 again, this implies that $(j-i)\theta_i(\gamma)\theta_j(\sigma) = 0$ in the one dimensional κ_L-vector space $\mathfrak{m}_L^{i+j}/\mathfrak{m}_L^{i+j+1}$. As $\theta_i(\gamma) \in (\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}) \backslash \{0\}$ and $\theta_j(\sigma) \in (\mathfrak{m}_L^j/\mathfrak{m}_L^{j+1}) \backslash \{0\}$, the image of $\theta_i(\gamma)\theta_j(\sigma)$ in nonzero in $\mathfrak{m}_L^{i+1}/\mathfrak{m}_L^{i+j+1}$, implying that $j - i = 0$ in κ_L, *i.e.* $p \mid j - i$.
(2) If $\gamma \in G_{i+1}$ or $\sigma \in G_{j+1}$, we have $\gamma\sigma\gamma^{-1}\sigma^{-1} \in G_{i+j+1}$ by lemma 4.3.22. Otherwise, we have $G_i \neq G_{i+1}$ and $G_j \neq G_{j+1}$, so that $j \equiv i \mod p\mathbf{Z}$: this implies that $\theta_{i+j}(\gamma\sigma\gamma^{-1}\sigma^{-1}) = (j-i)\theta_i(\gamma)\theta_j(\sigma) = 0$, whence $\gamma\sigma\gamma^{-1}\sigma^{-1} \in G_{i+j+1}$. □

4.3.23. *Upper numbering and Herbrand's theorem.*

Notation. If $t \in [-1, +\infty[$, we put

$$G_t = G_{\lceil t \rceil}$$

so that $\gamma \in G_t \Leftrightarrow i_G(\gamma) \geqslant t+1$. Put

$$\varphi_{L/K}(x) = \int_0^x \frac{\mathrm{d}t}{[G_0 : G_t]}$$

(where $[G_0 : G_t] = 1$ for $-1 < t \leqslant 0$, so that $\varphi_{L/K}(x) = x$ for all $x \in [-1, 0]$).

Proposition 4.3.24. The map $\varphi_{L/K}$ is a continuous, piecewise linear, increasing and concave map, such that $\varphi_{L/K}(0) = 0$. Moreover, we have $\varphi'_{L/K,l}(t) = \varphi'_{L/K,r}(t) = \frac{1}{[G_0:G_t]}$ if $t \notin \mathbf{Z}$, but $\varphi'_{L/K,l}(t) = \frac{1}{[G_0:G_t]}$ and $\varphi'_{L/K,r}(t) = \frac{1}{[G_0:G_{t+1}]}$ if $t \in \mathbf{Z}$.

Remark 4.3.25. If $i \in \mathbf{Z}_{\geqslant 0}$ and $i \leqslant x \leqslant i+1$, we have $\varphi_{L/K}(x) = \sum\limits_{k=0}^{i-1} \frac{1}{[G_0:G_{k+1}]} + \frac{x-i}{[G_0:G_{i+1}]}$ *i.e.*

$$\varphi_{L/K}(x) = \tfrac{1}{\#G_0}\big(\#G_1 + \cdots + \#G_i + (x-i)\#G_{i+1}\big).$$

Definition 4.3.26. The map $\varphi_{L/K}$ induces an homeomorphism from $[-1, +\infty[$ onto itself: we denote by $\psi_{L/K} \colon [-1, +\infty[\to [-1, +\infty[$ the inverse map. It is called the *Hasse-Herbrand map.*

Proposition 4.3.27. The map $\psi_{L/K}$ is a continuous, piecewise linear, increasing and convex map, such that $\psi_{L/K}(0) = 0$. The slopes of the linear pieces of the graph of $\psi_{L/K}$ are integers. Moreover, we have $\psi_{L/K}(\mathbf{Z}_{\geqslant 0}) \subset \mathbf{Z}_{\geqslant 0}$.

Proof. The only non trivial statement is the last one: let $y \in \mathbf{Z}_{\geqslant 0}$ and $i = \lfloor \psi_{L/K}(y) \rfloor$. By remark 4.3.25, we have $\#G_0 y = \#G_1 + \cdots + \#G_i + (\psi_{L/K}(y) - i)\#G_{i+1}$, so that $\psi_{L/K}(y) = i + [G_0 : G_{i+1}]y - \sum\limits_{k=1}^{i} [G_k : G_{i+1}] \in \mathbf{Z}$ (since $G_{i+1} \leqslant G_k$ for all $k \in \{0, \ldots, i\}$). □

Definition 4.3.28. (Ramification groups with upper numbering). If $y \in [-1, +\infty[$, we put

$$G^y = G_{\psi_{L/K}(y)}.$$

Remark 4.3.29. By definition, we have $G_x = G^{\varphi_{L/K}(x)}$ for all $x \in [-1, +\infty[$.

Example 4.3.30. We have $G^{-1} = G$, $G^0 = G_0$ and $G^y = \{\mathsf{Id}_L\}$ if $y \gg 0$.

The following result shows that the upper numbering is compatible passing to the quotient (*cf* remark 4.3.8).

Theorem 4.3.31. Let $H \trianglelefteq G$ be a normal subgroup. We have $(G/H)^y = G^y H/H$ for all $y \in [-1, +\infty[$.

Proposition 4.3.32. (Transitivity of Hasse-Herbrand map). If $M = L^H$, we have

$$\varphi_{L/K} = \varphi_{M/K} \circ \varphi_{L/M} \text{ and } \psi_{L/K} = \psi_{L/M} \circ \psi_{M/K}.$$

Lemma 4.3.33. If $x \in [-1, +\infty[$, we have $\varphi_{L/K}(x) + 1 = \frac{1}{\#G_0} \sum\limits_{\gamma \in G} \inf\{i_G(\gamma), x+1\}$.

Proof. Both sides are continuous, piecewise linear, and equal to 0 when $x = -1$: it is enough to show the equality of derivatives on intervals of the form $]i, i+1[$. If $i < x < i+1$, the derivative of the LHS is $\frac{1}{[G_0:G_{i+1}]}$, and that of the RHS is $\frac{1}{\#G_0} \sum\limits_{\substack{\gamma\in G\\ i_G(\gamma)>x+1}} 1 = \frac{\#\{\gamma\in G\,;\, i_G(\gamma)\geqslant i+2\}}{\#G_0} = \frac{\#G_{i+1}}{\#G_0} = \frac{1}{[G_0:G_{i+1}]}$. □

Lemma 4.3.34. Let $\sigma \in G/H$ and $j(\sigma) = \sup\limits_{\substack{s\in G\\ s\mapsto\sigma}} i_G(s)$. Then $i_{G/H}(\sigma) - 1 = \varphi_{L/M}(j(\sigma) - 1)$.

Proof. Let $s \in G$ be such that $i_G(s) = j(\sigma)$. If $\eta \in H_{j(\sigma)-1} = H \cap G_{j(\sigma)-1}$, we have $i_G(\eta) \geqslant j(\sigma)$, so that $i_G(s\eta) \geqslant j(\sigma)$ (simply because $G_{j(\sigma)-1}$ is a group), whence $i_G(s\eta) = j(\sigma)$ (by definition of $j(\sigma)$). If $\eta \in H \backslash H_{j(\sigma)-1}$, we have $i_G(\eta) < j(\sigma)$, so[39] $i_G(s\eta) = i_G(\eta)$. In any case, we have $i_G(s\eta) = \inf\{i_G(\eta), j(\sigma)\}$. By proposition 4.3.6, this implies that

$$i_{G/H}(\sigma) = \frac{1}{e_{L/M}} \sum_{\substack{\gamma\in G\\ \gamma\mapsto\sigma}} i_G(\gamma) = \frac{1}{\#H_0} \sum_{\eta\in H} \inf\{i_G(\eta), j(\sigma)\} = \varphi_{L/M}(j(\sigma)-1) + 1$$

by lemma 4.3.33 applied to the extension L/M. □

Lemma 4.3.35. (Herbrand's theorem). We have $G_xH/H = (G/H)_{\varphi_{L/M}(x)}$ for all $x \in [-1, +\infty[$.

Proof. We have the equivalences:

$$\sigma \in G_xH/H \Leftrightarrow j(\sigma) \geqslant x+1 \Leftrightarrow \varphi_{L/M}(j(\sigma)-1) \geqslant \varphi_{L/M}(x) \Leftrightarrow i_{G/H}(\sigma) - 1 \geqslant \varphi_{L/M}(x) \Leftrightarrow \sigma \in (G/H)_{\varphi_{L/M}(x)}$$

proving the equality. □

Proof of proposition 4.3.32. The second equality follows from the first. Both maps $\varphi_{L/K}$ and $\varphi_{M/K} \circ \varphi_{L/M}$ are continuous, piecewise linear and vanish at 0: it is enough to show that their derivatives on intervals of the form $]i, i+1[$ are the same for all $i \in \mathbf{Z}_{\geqslant -1}$. That of $\varphi_{M/K} \circ \varphi_{L/M}$ at $x \in]i, i+1[$ is

$$\begin{aligned}\varphi'_{M/K}(\varphi_{L/M}(x))\varphi'_{L/M}(x) &= \frac{1}{[(G/H)_0:(G/H)_{\varphi_{L/M}(x)}]} \frac{1}{[H_0:H_x]}\\ &= \frac{1}{[G_0H/H:G_xH/H]} \frac{1}{[H_0:H_x]}\\ &= \frac{\#(G_xH)\#H_x}{\#(G_0H)\#H_0} = \frac{1}{[G_0:G_x]} = \varphi'_{L/K}(x)\end{aligned}$$

since $\#(G_xH)\#H_x = \#(G_xH)\#(G_x \cap H) = \#G_x\#H$ and similarly $\#(G_0H)\#H_0 = \#G_0\#H$. □

Proof of theorem 4.3.31. We have $(G/H)^y = (G/H)_x$ with $x = \psi_{M/K}(y)$. As $(G/H)_x = G_{\psi_{L/M}(x)}H/H$ by lemma 4.3.35, this gives $(G/H)^y = G_{\psi_{L/K}(y)}H/H = G^yH/H$ since $\psi_{L/M}(x) = \psi_{L/M}(\psi_{M/K}(y)) = \psi_{L/K}(y)$ by proposition 4.3.32. □

Definition 4.3.36. A *jump* in the filtration $(G^y)_{y\geqslant -1}$ is an element $y \in [-1, +\infty[$ such that $G^y \neq G^{y+\varepsilon}$ for all $\varepsilon \in \mathbf{R}_{>0}$.

A fundamental theorem of ramification is the following:

Theorem 4.3.37. (Hasse-Arf). Assume that G is abelian. The jumps of the filtration $(G^y)_{y\geqslant -1}$ are integers. Equivalently, if $i \in \mathbf{Z}_{\geqslant -1}$ is such that $G_i \neq G_{i+1}$, then $\varphi_{L/K}(i)$ is an integer.

4.4. Exercises.

Exercise 4.4.1. Let p be a prime number and A a ring of characteristic p.
(1) Show that $\mathsf{W}(A)$ is an integral domain if and only if A is an integral domain.
(2) Show that $\mathsf{W}(A)$ is reduced if and only if A is reduced.
(3) Show that A is perfect if and only if $\mathsf{W}(A)/p\,\mathsf{W}(A)$ is reduced.

Exercise 4.4.2. Let A be a ring of characteristic p. Show that the V-adic and the p-adic topologies coincide if and only if the map $A \to A$; $a \mapsto a^p$ is surjective.

Exercise 4.4.3. Let k be a field of characteristic p. Show that $\mathsf{W}(k)$ is noetherian if and only if k is perfect [hint: compute $\dim_k(V(\mathsf{W}(k))/V(\mathsf{W}(k))^2)$].

[39] Because $v_L(s\eta(\alpha) - \alpha)) = v_L((s - \mathsf{Id}_L)(\eta(\alpha)) + (\eta - \mathsf{Id}_L)(\alpha)) = \min\{v_L((s - \mathsf{Id}_L)(\eta(\alpha)), v_L(\eta - \mathsf{Id}_L)(\alpha)) = i_G(\eta)$ since $v_L(\eta(\alpha) - \alpha) = i_G(\eta) < j(\sigma) = v_L((s - \mathsf{Id}_L)(\eta(\alpha)))$, for $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ (note that for such an α, we have $\mathcal{O}_L = \eta(\mathcal{O}_L) = \eta(\mathcal{O}_K[\alpha]) = \mathcal{O}_K[\eta(\alpha)]$).

Exercise 4.4.4. Let A be a ring and p a prime number which is not a zero divisor in A. Let $\sigma\colon A \to A$ be an endomorphism such that $\sigma(a) \equiv a^p \mod pA$ for all $a \in A$.
(1) Show that there exists a unique ring homomorphism $s_\sigma\colon A \to \mathsf{W}(A)$ such that $s_\sigma \circ \sigma = F_A \circ s_\sigma$ and $\Phi_0 \circ s_\sigma = \mathsf{Id}_A$.
(2) Let B be a ring such that p is not a zero divisor in B, and $\sigma'\colon B \to B$ an endomorphism such that $\sigma'(b) \equiv b^p \mod pB$ for all $b \in B$, and $u\colon A \to B$ a ring homomorphism such that $u \circ \sigma = \sigma' \circ u$. Show that $\mathsf{W}(u) \circ s_\sigma = s_{\sigma'} \circ u$.
(3) Let $t_\sigma\colon A \to \mathsf{W}(A/pA)$ be the composite of s_σ and the natural ring homomorphism $\mathsf{W}(A) \to \mathsf{W}(A/pA)$. Show that t_σ induces a ring homomorphism $t_{\sigma,n}\colon A/p^nA \to \mathsf{W}_n(A/pA)$ for all $n \in \mathbf{Z}_{>0}$.
(4) Show that $t_{\sigma,n}$ is an isomorphism when A/pA is perfect.
(5) Show that if A/pA is perfect and A is separated and complete for the p-adic topology, then t_σ is an isomorphism.

Exercise 4.4.5. Let A be a ring and p a prime number which is not a zero divisor in A.
(1) Show there exists a unique ring homomorphism $s_A\colon \mathsf{W}(A) \to \mathsf{W}(\mathsf{W}(A))$ such that $s_A \circ F_A = F_{\mathsf{W}(A)} \circ s_A$ and $\Phi_0 \circ s_A = \mathsf{Id}_{W(A)}$. Show that it is the unique ring homomorphism such that $\Phi_n \circ s_\sigma = F_A^n$ for all $n \in \mathbf{Z}_{\geqslant 0}$.
(2) Let $\mathcal{A} = \mathbf{Z}[X_n]_{n\in\mathbf{Z}_{\geqslant 0}}$ and $\mathbf{X} = (X_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in \mathsf{W}(\mathcal{A})$. Write $s_{\mathcal{A}}(\mathbf{X}) = (s_n(\mathbf{X}))_{n\in\mathbf{Z}_{\geqslant 0}}$, where $s_n(\mathbf{X}) \in \mathsf{W}(\mathcal{A})$. Show that $s_A(\underline{a}) = (s_n(\underline{a}))_{n\in\mathbf{Z}_{\geqslant 0}}$ for all $\underline{a} = (a_0, a_1, \ldots) \in \mathsf{W}(A)$.
(3) For all ring homomorphism $u\colon A \to B$, show that $s_B \circ \mathsf{W}(u) = \mathsf{W}(\mathsf{W}(u)) \circ s_A$.
(4) Show that the maps $\mathsf{W}(s_A) \circ s_A$ and $s_{\mathsf{W}(A)} \circ s_A$ from $W(A)$ to $\mathsf{W}(\mathsf{W}(\mathsf{W}(A)))$ are equal.

Exercise 4.4.6. Let K be a local field of characteristic $p > 0$. Show that it has only one coefficient field.

Exercise 4.4.7. Let $(K, |.|)$ be a local field, $\overline{K}$ an algebraic closure of K, and k/κ_K a finite field extension. Denote by L the unique subextension of $\overline{K}/K$ that is unramified and such that $\kappa_L = k$. Show that

$$L \simeq \begin{cases} k \otimes_{\kappa_K} K & \text{if } \mathsf{char}(K) = \mathsf{char}(\kappa_K) \\ \mathsf{W}(k) \otimes_{\mathsf{W}(\kappa_K)} K & \text{if } \mathsf{char}(K) \neq \mathsf{char}(\kappa_K) \end{cases}$$

Exercise 4.4.8. Let $\mathbf{Q}_p^{\mathrm{ur}}$ be the maximal unramified extension of $\mathbf{Q}_p$ in $\overline{\mathbf{Q}}_p$. Show that the completion of $\mathbf{Q}_p^{\mathrm{ur}}$ for $|.|_p$ is $\mathsf{W}(\overline{\mathbf{F}}_p)[p^{-1}]$.

Exercise 4.4.9. Let A be the localization of the polynomial ring $\mathbf{R}[X]$ with respect to the ideal $\mathfrak{p} = \langle X^2+1\rangle$.
(1) Show that A is a DVR but that there is no section $\kappa_A \to A$ of the projection.
(2) The completion $\widehat{A}$ of the DVR A has a field of coefficients: explicit an element in $\widehat{A}$ whose square is -1.

Exercise 4.4.10. (Cohen rings). Let p be a prime number. A *p-ring* is a DVR of characteristic 0 whose maximal ideal is generated by p.
(1) Let A be a DVR, $\pi \in A$ a uniformizer, and k a field extension of $\kappa := A/\pi A$. Show that there exists a DVR B that contains A and such that $B/\pi B = k$ [hint: lift first a transcendance basis of k over κ and use Zorn's lemma].
(2) (Kedlaya) Let $\mathscr{C}$ be the category of complete DVRs that are unramified over A, in which morphisms are unramified morphisms of rings (*i.e.* morphisms which induce isomorphisms on value groups). If $R, S \in \mathscr{C}$ have residue fields κ_R and κ_S respectively, and $\varphi\colon \kappa_R \to \kappa_S$ is a morphism, we say the morphism $f\colon R \to S$ is compatible (with φ) if the diagram

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d] & S \arrow[d] \\ \kappa_R \arrow[r, "\varphi"] & \kappa_S \end{tikzcd}$$

commutes. Show that if $R \in \mathscr{C}$ and $\kappa_R \to k$ is a separable field extension, there exists $S \in \mathscr{C}$ with residue field k and a compatible morphism $R \to S$. Show moreover that if $R, S, T \in \mathscr{C}$ are such that there are morphisms $\kappa_R \to \kappa_S \to \kappa_T$ and $f\colon R \to S$ and $h\colon R \to T$ are compatible morphisms, there exists a unique compatible morphism $g\colon S \to T$ such that $h = g \circ f$.

Remark 4.4.11. This implies in particular that if $f\colon R \to S$ is a compatible morphism in $\mathscr{C}$ and κ_S/κ_R is Galois, then the group of f-equivariant automorphisms of S is isomorphic to $\mathsf{Gal}(\kappa_S/\kappa_R)$.

(3) Show that if k is a field of characteristic p, there exists a complete p-ring having k as residue field (such a DVR is called a *Cohen ring* for k).
(4) Construct a Cohen ring for $\mathbf{F}_p(\!(T)\!)$.
(5) Show that if k is perfect, then any Cohen ring for k is uniquely isomorphic to $\mathsf{W}(k)$.

Exercise 4.4.12. Let p be a prime. Can you find a Galois extension of $\mathbf{Q}_p$ whose Galois group is isomorphic to $\mathfrak{S}_5$?

Exercise 4.4.13. Let p be a prime number and $d \in \mathbf{Z}$. Assume that d is not a square in $\mathbf{Q}_p$ and put $K = \mathbf{Q}_p(\sqrt{d})$. Compute the ramification groups of $K/\mathbf{Q}_p$ [hint: treat the cases p odd and $p = 2$ separately].

Exercise 4.4.14. Let L/K be a finite Galois extension of local fields of characteristic 0, with residue field of characteristic $p > 0$. Let $G = \mathsf{Gal}(L/K)$ be its Galois group, and π a uniformizer of L.
(1) Let $i \in \mathbf{Z}_{\geqslant 0}$ and $g \in G_i$. Write $g(\pi) = \pi(1+a)$ with $a \in \mathfrak{m}_L^i$. Let $\varphi = g - \mathsf{Id}_L \colon L \to L$. Show that $\varphi(x) \equiv jax \mod \mathfrak{m}_L^{j+i+1}$ for all $j \in \mathbf{Z}_{\geqslant 0}$ and $x \in \mathfrak{m}_L^j$.
(2) Let $\psi = g^p - \mathsf{Id}_L \colon L \to L$. Show that

$$\psi(x) \equiv \begin{cases} pjax \mod \mathfrak{m}_L^{j+i+e_L+1} & \text{if } i > \frac{e_L}{p-1} \\ pjax + j(1-i^{p-1})a^p x \mod \mathfrak{m}_L^{j+i+e_L+1} & \text{if } i = \frac{e_L}{p-1} \\ j(1-i^{p-1})a^p x \mod \mathfrak{m}_L^{j+pi+1} & \text{if } i < \frac{e_L}{p-1} \end{cases}$$

(3) Show that if $i > \frac{e_L}{p-1}$ and $g \notin G_{i+1}$, then $g^p \in G_{i+e_L} \backslash G_{i+e_L+1}$. Conclude that $i > \frac{e_L}{p-1} \Rightarrow G_i = \{\mathsf{Id}_L\}$.
(4) Similarly, show that if $i = \frac{e_L}{p-1}$, the group G_i is either trivial or cyclic of order p, this last case being possible if and only if $p \mid i$.
(5) Assume that $i < \frac{e_L}{p-1}$. Show that if $p \nmid i$, then $g^p \in G_{pi+1}$. If $p \mid i$, show that $g^p \in G_{pi}$ and $\theta_{pi}(g^p) = \theta_i(g)^p$. Conclude that if $p \mid i$, the group G_i/G_{i+1} is either trivial, or cyclic of order p, this last case being possible if and only if $p^h i = \frac{e_L}{p-1}$ for some $h \in \mathbf{Z}_{>0}$.
(6) Show that if the integers $i \in \mathbf{Z}_{>0}$ such that $G_i \neq G_{i+1}$ all are divisible by p, then they are of the form $p^k i_0$ with $k \in \{1, \ldots, h\}$ where $p^h i_0 = \frac{e_L}{p-1}$, and G_1 is cyclic of order p^h.

Exercise 4.4.15. Let K be a field of characteristic 0, with residue field of characteristic $p > 0$. Assume that K contains the p-th roots of unity. Let $\overline{K}$ be an algebraic closure of K and $x \in \overline{K}$ such that $x^p = \pi$ is a uniformizer of K. Put $L = K(x)$. Show that L/K is a cyclic extension of degree p. If $G = \mathsf{Gal}(L/K)$, show that $G_i = G$ and $G_{i+1} = \{\mathsf{Id}_L\}$ for $i = \frac{pe_K}{p-1}$.

Exercise 4.4.16. Let K be a local field of characteristic 0, $\overline{K}$ an algebraic closure of K, and $n \in \mathbf{Z}_{>0}$ such that $n < \frac{pe_K}{p-1}$ and $p \nmid n$, where $p = \mathsf{char}(\kappa_K) > 0$. Let $y \in K$ be such that $v_K(y) = -n$ and $x \in \overline{K}$ such that $x^p - x = y$. Put $L = K(x)$.
(1) Show that L/K is a cyclic extension of degree p.
(2) Let $G = \mathsf{Gal}(L/K)$. Show that $G_n = G$ and $G_{n+1} = \{\mathsf{Id}_L\}$.

Exercise 4.4.17. Let p be a prime number, $\zeta_{p^2} \in \overline{\mathbf{Q}}_p$ a primitive p^2-th root of unity and $\zeta_p = \zeta_{p^2}^p$. Put $F = \mathbf{Q}_p(\zeta_p)$, $K = \mathbf{Q}_p(\zeta_{p^2})$, $L = K(p^{1/p})$ and $K_i = \mathbf{Q}_p(\zeta_p, p^{1/p}\zeta_{p^2}^i)$ for $i \in \{0, \ldots, p-1\}$.
(1) Explain why L/F is Galois.
(2) Show that there is an injective group homomorphism $(a, b) \colon \mathsf{Gal}(L/F) \to (\mathbf{Z}/p\mathbf{Z})^2$.
(3) Show that the extensions K/F and K_i/F are Galois (for $i \in \{1, \ldots, p\}$), and describe their ramification filtration (with lower numbering) [hint: show that if $\pi = \zeta_p - 1 \in F$ then $\varpi_i := \frac{\pi}{\zeta_{p^2}^i p^{1/p}} \in K_i$ is a uniformizer of K_i].
(4) Deduce that $K_i \neq K$ for all $i \in \{1, \ldots, p\}$, and that $[L : F] = p^2$.
(5) Using these extensions, show that the lower numbering is not compatible with quotients.

Exercise 4.4.18. Let $p > 3$ be a prime and K a splitting field of $P(X) = X^3 + pX + p \in \mathbf{Q}_p[X]$.
(1) Show that $G := \mathsf{Gal}(K/\mathbf{Q}_p) \simeq \begin{cases} \mathfrak{A}_3 & \text{if } \left(\frac{-3}{p}\right) = 1 \\ \mathfrak{S}_3 & \text{if } \left(\frac{-3}{p}\right) = -1 \end{cases}$ [hint: the discriminant $-4p^3 - 27p^2$ of P is δ^2 with $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3)$ where $\alpha_1, \alpha_2, \alpha_3 \in K$ are the roots of P].
(2) Compute the ramification filtration on G.

Exercise 4.4.19. Let L/K be a totally ramified Galois extension of local fields of characteristic 0. Assume that its Galois group $G \simeq \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group (so that $C := \mathsf{Z}(G) \simeq \{\pm 1\}$), and that $G_4 = \{\mathsf{Id}_L\}$. Show that $G = G_0 = G_1$, and $G_2 = G_3 = C$. What is the different of L/K? Show that

$$G^y = \begin{cases} G & \text{if } y \leqslant 1 \\ C & \text{if } 1 < y \leqslant \frac{3}{2} \\ \{\mathsf{Id}_L\} & \text{if } \frac{3}{2} < y \end{cases}$$

Exercise 4.4.20. Let p be a prime number, $\overline{\mathbf{Q}}_p$ an algebraic closure of $\mathbf{Q}_p$. If $n \in \mathbf{Z}_{>0}$, let $\zeta \in \overline{\mathbf{Q}}_p$ be a primitive p^n-th root of unity, and $K_n = \mathbf{Q}_p(\zeta)$.
(1) Show that $K_n/\mathbf{Q}_p$ is totally ramified of degree $p^{n-1}(p-1)$, whose ring of integers is $\mathbf{Z}_p[\zeta]$, of which a uniformizer is $\zeta - 1$.
(2) Show that $K_n/\mathbf{Q}_p$ is Galois, and that there is an isomorphism $G := \mathsf{Gal}(K_n/\mathbf{Q}_p) \simeq (\mathbf{Z}/p^n\mathbf{Z})^\times$. If $m \in \{1, \ldots, n-1\}$, what is the image of $\mathsf{Gal}(K_n/K_m)$ under this isomorphism?
(3) Show that the ramification groups of $K_n/\mathbf{Q}_p$ are given by

$$G_i = \begin{cases} G & \text{if } i = 0 \\ \mathsf{Gal}(K_n/K_m) & \text{if } p^{m-1} \leqslant i < p^m \text{ for some } m \in \{1, \ldots, n-1\} \\ \{\mathsf{Id}_{K_n}\} & \text{if } p^{n-1} \leqslant i \end{cases}$$

(4) Compute $\mathfrak{D}_{K_n/\mathbf{Q}_p}$.
(5) Describe the upper ramification groups.

Exercise 4.4.21. Assume $p > 2$ and let $K/\mathbf{Q}_p$ be a totally ramified Galois extension of degree p. Denote by π a uniformizer of K and v_K its normalized valuation. Let $E(X) = X^p + a_{p-1}X^{p-1} + \cdots + a_0 \in \mathbf{Z}_p$ be the minimal polynomial of π over $\mathbf{Q}_p$. Recall that $v_K(\mathfrak{D}_{K/\mathbf{Q}_p}) = \min\{2p-1, v_K(a_i) + i - 1\}_{1 \leqslant i < p}$ (where $\mathfrak{D}_{K/\mathbf{Q}_p}$ denotes the different ideal of $K/\mathbf{Q}_p$).
(1) Show that $p - 1 \mid v_K(\mathfrak{D}_{K/\mathbf{Q}_p})$ [hint: use the ramification filtration].
(2) Deduce that $v_K(\mathfrak{D}_{K/\mathbf{Q}_p}) = 2p - 2$.
(3) Compute $\mathsf{Gal}(K/\mathbf{Q}_p)_x$ for $x \in [-1, +\infty[$.
(4) Deduce $\mathsf{Gal}(K/\mathbf{Q}_p)^y$ for $y \in [-1, +\infty[$.
(5) Assume $L/\mathbf{Q}_p$ is a totally ramified Galois extension such that $\mathsf{Gal}(L/\mathbf{Q}_p) \simeq (\mathbf{Z}/p\mathbf{Z})^2$.
(a) Show that $L = K_1K_2$ where $K_i/\mathbf{Q}_p$ is totally ramified Galois of degree p for $i \in \{1, 2\}$.
(b) Show that $\mathsf{Gal}(L/\mathbf{Q}_p)^y \hookrightarrow \mathsf{Gal}(K_1/\mathbf{Q}_p)^y \times \mathsf{Gal}(K_2/\mathbf{Q}_p)^y$ for all $y \in [-1, +\infty[$.
(c) Compute $\mathsf{Gal}(L/\mathbf{Q}_p)^y$ for all $y \in [-1, +\infty[$.
(d) Deduce $\mathsf{Gal}(L/\mathbf{Q}_p)_1/\mathsf{Gal}(L/\mathbf{Q}_p)_2$.
(e) Derive a contradiction and conclude that no such L exists.

Exercise 4.4.22. Unless otherwise stated, ramification subgroups of a finite Galois extension L/K will be considered with the lower numbering. A *jump* of the extension L/K is an integer i such that $\mathsf{Gal}(L/K)_i \neq \mathsf{Gal}(L/K)_{i+1}$.
Let L/K and K/F be nontrivial finite extensions of local fields.
(1) Assume that L/F and K/F are Galois. Let $i_1 < \cdots < i_n$ be the jumps of the ramification filtration of L/K. Assume that the ramification filtration of K/F has a unique jump i_0, and that $i_0 < i_1$. Show that

$$\mathsf{Gal}(L/F)_i = \begin{cases} \mathsf{Gal}(L/F) & \text{if } i \leqslant i_0 \\ \mathsf{Gal}(L/K)_i & \text{if } i > i_0 \end{cases}$$

and deduce that the jumps of the ramification filtration of L/F are $i_0, i_1, \ldots, i_n$ [hint: Herbrand's theorem].
Assume from now on that F has mixed characteristics $(0, p)$, that $K = F(\zeta)$ where ζ is a primitive p-th root of unity, and that $L = K(\alpha)$, where $a := \alpha^p \in K$ and $\alpha \notin K$.
(2) Show that the extension K/F is cyclic of degree dividing $p - 1$, and that $v_K(\zeta - 1) = \frac{e_K}{p-1} \in \mathbf{Z}_{>0}$ (where e_K is the absolute ramification index of K).
(3) Explain why K/F has at most two jumps, and exactly one when it is totally ramified.
We henceforth assume that K/F is totally ramified. Denote by v_K (resp. v_L) the normalized valuation on K (resp. on L).
(4) Show that L/K is a cyclic extension of degree p. When $a \in F$, show that L/F is Galois and describe the structure of $\mathsf{Gal}(L/F)$.

(5) Assume that $p \nmid v_K(a)$. Show that L/K is totally ramified, and that $v_L(\mathfrak{D}_{L/K}) = pe_K + p - 1$ [hint: first reduce to the case where $v_K(a) = 1$]. Deduce the jumps of L/K. If $a \in F$, what are the jumps of L/F? Under which condition on e_F are the jumps in the upper numbering integers?
Assume from now on that $p \mid v_K(a)$ and put $E = \big\{i \in \mathbf{Z}_{>0}\,;\,(\exists x \in K^\times)\, ax^{-p} \in U_K^{(i)}\big\}$.
(6) (i) Show that $1 \in E$.
(ii) Assume that $a \in U_K^{(i)}$ with $i > \frac{pe_K}{p-1}$. Show that the polynomial $Q(X) = \frac{(1+(\zeta-1)X)^p - a}{(\zeta-1)^p}$ belongs to $\mathcal{O}_K[X]$, and use Newton's lemma to show that it has a root in $\mathcal{O}_K$, contradicting the hypothesis.
The set E is thus non empty, and included in $\big\{1, \ldots, \frac{pe_K}{p-1}\big\}$. Put $c = \max E$: replacing a by ax^{-p} for some appropriate $x \in K^\times$, we may assume that $a \in U_K^{(c)}$.
(7) Show that there exists $A(X) \in \mathbf{Z}[X]$ such that $(X-1)^p = X^p - 1 + p(X-1)A(X)$ and $A(1) = -1$.
(8) Assume that $c = \frac{pe_K}{p-1}$ and put $z = \frac{\alpha - 1}{\zeta - 1} \in L$.

- (i) Show that $v_L(z) = 0$ [hint: use question (7)].
- (ii) Compute the minimal polynomial P of z over K, and show that its image $\overline{P}$ in $\kappa_K[X]$ is of the form $\overline{P}(X) = X^p - X - \lambda$. Explain why $\overline{P}$ is irreducible, and deduce that K/F is unramified.
- (iii) If $a \in F$, what are the jumps of L/F in that case?

(9) Assume that $c \leqslant \frac{pe_K}{p-1} - 1$.

- (i) Show that $p \nmid c$ [hint: assume the contrary and deduce a contradiction with the definition of c.]
- (ii) Compute $v_L(\alpha - 1)$ [hint: use question (7)], and deduce that L/K is totally ramified.
- (iii) Constuct a uniformizer π_L of L, and determine the jump of L/K [hint: consider the action of a generator of $\mathsf{Gal}(L/K)$ on π_L.]
- (iv) Deduce that $v_L(\mathfrak{D}_{L/K}) = (p-1)\big(\frac{pe_K}{p-1} - c + 1\big)$. When $a \in F$, what are the jumps of L/F in this case?

Exercise 4.4.23. Let $(K, |.|)$ be a complete discretely valued field of characteristic 0, with perfect residue field κ_K of characteristic p. We denote by v the normalized valuation on K and by $e_K = v(p)$ its absolute ramification index. Let $n \in \mathbf{Z}_{>0}$ be such that $\mathbf{F}_{p^n} \subset \kappa_K$ and $\alpha \in K$ such that $v(\alpha) > -\frac{p^n e_K}{p^n - 1}$. Put $P(X) = X^{p^n} - X - \alpha \in K[X]$, let $\lambda \in \overline{K}$ be a root of P and $L = K(\lambda)$. We still denote by v its extension to L.
(1) Recall why there is a unique multiplicative map $[.]\colon \mathbf{F}_{p^n} \to \mathcal{O}_K$ such that $\pi \circ [.] = \mathsf{Id}_{\mathbf{F}_{p^n}}$, where $\pi\colon \mathcal{O}_K \to \kappa_K$ is the projection.
Put $Q(X) = P(X + \lambda) \in L[X]$.
(2) Assume $v(\alpha) < 0$. Show that $v(\lambda) = \frac{v(\alpha)}{p^n}$. Deduce that $Q(X) \in \mathcal{O}_L[X]$ and compute the image $\overline{Q}(X)$ of $Q(X)$ in $\kappa_L[X]$.
(3) For $x \in \mathbf{F}_{p^n}$, compute the images of $Q([x])$ and $Q'([x])$ in κ_L. Deduce that P is split in L.
What precedes shows that L/K is Galois: put $G = \mathsf{Gal}(L/K)$.
(4) Show that if $\sigma \in G\backslash\{\mathsf{Id}_L\}$, we have $|\sigma(\lambda) - \lambda| = 1$.
(5) Assume now that $p \nmid v(\alpha)$ and $v(\alpha) < 0$.

- (a) Show that L/K is totally ramified, and give a uniformizer π_L in terms of a uniformizer π_K of K and λ [hint: use the fact that $\mathsf{gcd}(p^n, v(\alpha)) = 1$].
- (b) Show that the ramification filtration with lower numbering is given by
$$G_i = \begin{cases} G & \text{if } i \leqslant -v(\alpha) \\ \{\mathsf{Id}_L\} & \text{if } i > -v(\alpha) \end{cases}.$$
- (c) Compute the different $\mathfrak{D}_{L/K}$ and the discriminant $\mathfrak{d}_{L/K}$.

(6) Show that if $\alpha_1 \in K$ satisfies $|\alpha - \alpha_1| < 1$ and λ_1 is a root of $P_1(X) = X^{p^n} - X - \alpha_1$, then $K(\lambda) = K(\lambda_1)$.
(7) Assume now that $\alpha_1, \alpha_2 \in K$ are such that $v(\alpha_1), v(\alpha_2) > -e_K$ and $|\alpha - \alpha_1 - \alpha_2| < 1$. Show that $L = K(\lambda)$ lies in the compositum of $K(\lambda_1)K(\lambda_2)$.

Exercise 4.4.24. Let p be a prime number and $n \in \mathbf{Z}_{>0}$. Write $n = p^r m$ with $r \in \mathbf{Z}_{\geqslant 0}$ and $m \in \mathbf{Z}_{>0}$ such that $p \nmid m$. Fix an algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$. In what follows, ζ_n will denote a (any) primitive n-th root of unity, and $K_n = \mathbf{Q}_p(\zeta_n)$. Let $\Phi_n(X) \in \mathbf{Z}[X]$ be the n-th cyclotomic polynomial.
(1) Explain why $K_n/\mathbf{Q}_p$ is Galois and show that $\mathsf{Gal}(K_n/\mathbf{Q}_p)$ injects canonically in $(\mathbf{Z}/n\mathbf{Z})^\times$.
(2) Show that the extension of $\mathbf{F}_p$ generated by the primitive m-th roots of unity is $\mathbf{F}_{p^f}$ where f is the order of p in $(\mathbf{Z}/m\mathbf{Z})^\times$. Explain why the irreducible factors of the image of Φ_m in $\mathbf{F}_p[X]$ all are of degree f.

(3) Show that K_m is the unramified extension of degree f of $\mathbf{Q}_p$ [hint: use Newton's lemma to show that its residue field is $\mathbf{F}_{p^f}$].
(4) Show that $\Phi_{p^r}(1+X)$ is an Eisenstein polynomial in $K_m[X]$. Deduce that K_m is the maximal unramified subextension of $K_n/\mathbf{Q}_p$ [hint: show that $K_n = K_m(\zeta_{p^r})$]. What is the degree of the extension $[K_n : \mathbf{Q}_p]$?
(5) Deduce that the ring of integers of K_n is $\mathbf{Z}_p[\zeta_n]$. Show that $\zeta_{p^r} - 1$ is a uniformizer of K_n. Is $\zeta_n - 1$ a uniformizer?
(6) Compute the different and the discriminant of $K_n/\mathbf{Q}_p$.
(7) Determine the ramification filtration of $\mathsf{Gal}(K_n/\mathbf{Q}_p)$ with lower and upper numbering.
(8) Retrieve the result of question (6) using the ramification filtration.
(9) Show that there exists $\pi_0 \in K_p$ such that $\pi_0^{p-1} = -p$.
(10) Is there necessarily an element $\pi_1 \in K_p$ such that $\pi_1^{p-1} = p$?

5. Infinite extensions

5.1. **Infinite Galois theory.** Let K be a field. If L/K is a finite Galois extension, Galois theory provides a dictionary between subextensions of L/K and subgroups of $\mathsf{Gal}(L/K) = \mathsf{Aut}_{K\text{-alg}}(L)$. More precisely, there is a decreasing bijection

$$\begin{aligned}\{\text{subextensions of } L/K\} &\to \{\text{subgroups of } \mathsf{Gal}(L/K)\}\\ F &\mapsto \mathsf{Gal}(L/F)\end{aligned}$$

(the inverse bijection is $H \mapsto L^H$). We extend this to (possibly) infinite Galois extensions: let L/K be an algebraic, separable and normal extension, and put

$$\mathsf{Gal}(L/K) = \mathsf{Aut}_{K\text{-alg}}(L)$$

Remark 5.1.1. An important example, is when $L = \overline{K}$ is a separable closure of K. The group $\mathsf{Gal}(\overline{K}/K)$ is called "the" *absolute Galois group* of K.

Denote by $\mathcal{I}_{L/K}$ the set of *finite and normal* subextensions of L/K. Endowed with the inclusion relation, this is a directed set (an upper bound of two extensions being their compositum). For $F_1 \subset F_2 \in \mathcal{I}_{L/K}$, the restriction provides group homomorphisms $\mathsf{Gal}(L/K) \to \mathsf{Gal}(F_2/K) \to \mathsf{Gal}(F_1/K)$: the family $(\mathsf{Gal}(F/K))_{F\in\mathcal{I}_{L/K}}$ (endowed with the restriction maps) is an inverse system, and there is a group homomorphism

$$\psi\colon \mathsf{Gal}(L/K) \to \varprojlim_{F\in\mathcal{I}_{L/K}} \mathsf{Gal}(F/K)$$

Lemma 5.1.2. The previous morphism is an isomorphism.

Proof. If $g \in \mathsf{Ker}(\psi)$, then $g_{|F} = \mathsf{Id}_F$ for every $F \in \mathcal{I}_{L/K}$. As $L = \bigcup\limits_{F\in\mathcal{I}_{L/K}} F$ (because L/K is algebraic), this implies that $g = \mathsf{Id}_L$, so that ψ is injective. Let $(g_F)_{F\in\mathcal{I}_{L/K}} \in \varprojlim\limits_{F\in\mathcal{I}_{L/K}} \mathsf{Gal}(F/K)$. If $x \in L$ and $F_1, F_2 \in \mathcal{I}_{L/K}$ are such that $x \in F_1 \cap F_2$, let F be the compositum of F_1 and F_2. As $(g_F)_{|F_1} = g_{F_1}$ and $(g_F)_{|F_2} = g_{F_2}$, we have $g_{F_1}(x) = g_F(x) = g_{F_2}(x)$, so $g_F(x)$ does not depend on the choice of $F \in \mathcal{I}_{L/K}$ such that $x \in F$. So we can define $g\colon L \to L$ by $g(x) = g_F(x)$ for any $F \in \mathcal{I}_{L/K}$ such that $x \in F$. We have $g_{|F} = g_F$ for all $F \in \mathcal{I}_{L/K}$, so $g \in \mathsf{Gal}(L/K)$, and $\psi(g) = (g_F)_{F\in\mathcal{I}_{L/K}}$, which proves the surjectivity of ψ. □

Definition 5.1.3. Via the previous isomorphism, the group $\mathsf{Gal}(L/K)$ is endowed with a topology (called the *Krull topology*) for which it is profinite (in particular it is compact). If $g \in \mathsf{Gal}(L/K)$, a basis of neighborhoods of g is $\{g\,\mathsf{Gal}(L/F)\}_{F\in\mathcal{I}_{L/K}}$ (*i.e.* $g_1, g_2 \in \mathsf{Gal}(L/K)$ are close if they agree on a big finite subextension of L/K).

Theorem 5.1.4. The map $F \mapsto \mathsf{Gal}(L/F)$ is a bijection between the set of subextensions of L/K and that of *closed* subgroups of $\mathsf{Gal}(L/K)$. The open subgroups correspond to finite subextensions of L/K. The inverse bijection is $H \mapsto L^H$.

Proof. • If F is a finite subextension of L/K, the subgroup $\mathsf{Gal}(L/F) \leqslant \mathsf{Gal}(L/K)$ is open[(40)], hence closed. Now if F/K is any (*i.e.* not necessarily finite) subextension of L/K, then $\mathsf{Gal}(L/F) = \bigcap\limits_{\substack{M\subset F\\ [M:K]<\infty}} \mathsf{Gal}(L/M)$ (because $F = \bigcup\limits_{\substack{M\subset F\\ [M:K]<\infty}} M$), so $\mathsf{Gal}(L/F)$ is a closed subgroup as the intersection of closed subgroups. This shows that the map is well defined.

• Let F be a subextension of L/K. If $x \in L$, there exists a finite and normal subextension N/F of L/F such that $x \in N$. If x fixed by $\mathsf{Gal}(L/F)$, it is fixed by $\mathsf{Gal}(N/F)$, hence $x \in F$ (by classical Galois theory). This implies that $L^{\mathsf{Gal}(L/F)} = F$, so the map $F \mapsto \mathsf{Gal}(L/F)$ is injective.

• It remains to show that if $H \leqslant \mathsf{Gal}(L/K)$ is a closed subgroup, then $H = \mathsf{Gal}(L/F)$ with $F := L^H$. One has $H \leqslant \mathsf{Gal}(L/F)$. To show the equality, is is enough to show that H is dense in $\mathsf{Gal}(L/F)$ (because H is closed). Let $g \in \mathsf{Gal}(L/F)$ and $M \in \mathcal{I}_{L/F}$, so that $g\,\mathsf{Gal}(L/M)$ is an open neighborhood of g in $\mathsf{Gal}(L/F)$. As $F = L^H$, one has $M^{\overline{H}} = F$ as well, where $\overline{H}$ is the image of H in $\mathsf{Gal}(M/F)$. By classical Galois theory, this implies that $\overline{H} = \mathsf{Gal}(M/F)$, so that $H \to \mathsf{Gal}(M/F)$ is surjective: there exists $\sigma \in H$ such that $\sigma_{|M} = g_{|M}$, so that $g^{-1}\sigma \in \mathsf{Gal}(L/M)$, *i.e.* $\sigma \in g\,\mathsf{Gal}(L/M)$: we have $\sigma \in H \cap g\,\mathsf{Gal}(L/M)$ *i.e.* $H \cap g\,\mathsf{Gal}(L/M) \neq \varnothing$, which proves the density.

[(40)] Take $N \subset L$ the normal closure of F, then $N \in \mathcal{I}_{L/K}$, so $\mathsf{Gal}(L/N)$ is open in $\mathsf{Gal}(L/K)$ (by definition of Krull topology): so is $\mathsf{Gal}(L/F) = \bigcup\limits_{g\in\mathsf{Gal}(N/F)} g\,\mathsf{Gal}(L/N)$.

• We have seen that if F/K is finite, then $\mathsf{Gal}(L/F)$ is open in $\mathsf{Gal}(L/K)$. Conversely, if $H = \mathsf{Gal}(L/F)$ is open in $\mathsf{Gal}(L/K)$, one has $[\mathsf{Gal}(L/K) : H] < +\infty$ (because $\mathsf{Gal}(L/K)$ is compact). If $x \in L^H$, then x has at most $[\mathsf{Gal}(L/K) : H]$ conjugates, so $[F : K] \leqslant [\mathsf{Gal}(L/K) : H]$ is finite. □

Proposition 5.1.5. A subextension F/K of L/K is Galois if and only if $\mathsf{Gal}(L/F) \trianglelefteq \mathsf{Gal}(L/K)$. In this case $\mathsf{Gal}(L/K)/\mathsf{Gal}(L/F) \xrightarrow{\sim} \mathsf{Gal}(F/K)$.

Proof. Let $H = \mathsf{Gal}(L/F) \leqslant \mathsf{Gal}(L/K)$. If $g \in \mathsf{Gal}(L/K)$, one has $\mathsf{Gal}(L/g(F)) = gHg^{-1}$. By Galois correspondence, one has $g(F) = F \Leftrightarrow gHg^{-1} = H$, so F/K is Galois if and only if $H \trianglelefteq \mathsf{Gal}(L/K)$. In this case, the restriction induces a surjective group homomorphism $\mathsf{Gal}(L/K) \to \mathsf{Gal}(F/K)$, whose kernel is H. □

Example 5.1.6. Let K be a finite field: $K = \mathbf{F}_q$ with $q = p^n$ (where $p = \mathsf{char}(K)$). Fix $\overline{K}$ an algebraic closure of K. Let $\varphi\colon \overline{K} \to \overline{K}; x \mapsto x^q$ be the *Frobenius* map. For $m \in \mathbf{Z}_{>0}$, let $K_m \simeq \mathbf{F}_{q^m}$ be the unique subextension of $\overline{K}/K$ of degree m. The extension K_m/K is Galois, and $\mathsf{Gal}(K_m/K) \simeq \mathbf{Z}/m\mathbf{Z}$ is cyclic, generated by $\varphi_{|K_m}$. Passing to the limit, the map $\widehat{\mathbf{Z}} \xrightarrow{\sim} \mathsf{Gal}(\overline{K}/K)$; $1 \mapsto \varphi$ is an isomorphism and a homeomorphism.

Remark 5.1.7. (Ramification groups) Assume K is a local field, and L/K a (non necessarily finite) Galois extension. If $y \in [-1, +\infty[$, we can put

$$\mathsf{Gal}(L/K)^y = \varprojlim_{F \in \mathcal{I}_{L/K}} \mathsf{Gal}(F/K)^y$$

(which makes sense since upper numbering is compatible with quotients, *cf* theorem 4.3.31).

5.2. **Dévissage of G_K.** In this section, $(K, |.|)$ denotes a local field of mixed characteristics $(0, p)$ (so that K is an extension of $\mathbf{Q}_p$). Let $v\colon K \to \mathbf{Q} \cup \{+\infty\}$ be the valuation normalized by $v(p) = 1$. Fix $\overline{K}$ an algebraic closure of K and let $G_K = \mathsf{Gal}(\overline{K}/K)$ be "the" absolute Galois group. Recall that $|.|$ extends uniquely to a (non-discrete) absolute value $|.| : \overline{K} \to \mathbf{R}_{\geqslant 0}$ (so that v extends uniquely into a non-discrete valuation $v\colon \overline{K} \to \mathbf{Q} \cup \{\infty\}$), which is G_K-equivariant, *i.e.* $(\forall x \in \overline{K})\,(\forall g \in G_K)\, v(g(x)) = v(x)$ (*cf* corollaries 3.5.7 and 3.5.8). Put $W = \mathsf{W}(k)$ and $F = \mathsf{Frac}(W) = W[\frac{1}{p}]$. One has $F \hookrightarrow K$, and the extension K/F is totally ramified of degree $e_K = [|K^\times| : \mathbf{Z}]$ (we have $v(K) = \frac{1}{e_K}\mathbf{Z} \cup \{\infty\}$).
For every finite and Galois subextension L of $\overline{K}/K$, we have (*cf* §4.1) n exact sequence

$$\{\mathsf{Id}_L\} \to I_{L/K} \to \mathsf{Gal}(L/K) \to \mathsf{Gal}(\kappa_L/\kappa_K) \to \{1\}$$

where $I_{L/K} = \mathsf{Gal}(L/T)$ is the inertia subgroup (here T is the maximal unramified subextension of L/K). As L ranges among the finite and Galois subextension of $\overline{K}/K$, this provides an inverse system of exact sequences. Passing to inverse limit gives an exact sequence:

$$\{\mathsf{Id}_{\overline{K}}\} \to I_K \to G_K \to \mathsf{Gal}(\overline{\kappa}_K/\kappa_K) \to \{1\}$$

(note that $\kappa_{\overline{K}} \simeq \overline{\kappa}_K$ by corollary 3.8.16). Under Galois correspondance, the group I_K corresponds to the composite K^{ur} of all unramified subextensions of $\overline{K}/K$: we call K^{ur} the *maximal unramified subextension* of K. Then $I_K = \mathsf{Gal}(\overline{K}/K^{\mathrm{ur}})$ and $\mathsf{Gal}(K^{\mathrm{ur}}/K) \xrightarrow{\sim} \mathsf{Gal}(\overline{\kappa}_K/\kappa_K)$.

Remark 5.2.1. When K in a finite extension of $\mathbf{Q}_p$, the group $\mathsf{Gal}(\overline{\kappa}_K/\kappa_K) \simeq \widehat{\mathbf{Z}}$ is quite explicit (*cf* example 5.1.6). Write $\kappa_K = \mathbf{F}_q$ (where $q = p^{[\kappa_K:\mathbf{F}_p]}$). Then $\kappa_{\overline{K}}$ is an algebraic closure of κ_K: it is obtained by adjoining to κ_K the n-roots of unity for all $n \in \mathbf{Z}_{>0}$ prime to p. Using Newton's lemma, this implies that $K^{\mathrm{ur}} = \bigcup\limits_{p \nmid n} K(\mu_n)$ (where μ_n denotes the group of n-th roots of unity in $\overline{K}$).

Definition 5.2.2. We denote by P_K the pro-p-Sylow subgroup of I_K, *i.e.* the maximal pro-p-subgroup of I_K. This is the closed subgroup of G_K (called the *wild inertia subgroup*). By definition, it corresponds, under Galois correspondance, to the composite K^{tame} of all tamely ramified subextensions of $\overline{K}/K$.

Definition 5.2.3. Let G be a profinite group.
(1) Let B a topological ring endowed with a continuous action of G. A *B-representation* of G is a free B-module of finite rank endowed with a continuous and semi-linear action of G, *i.e.*

$$(\forall g \in G)\ (\forall b \in B)\ (\forall m_1, m_2 \in M)\ g(bm_1 + m_2) = g(b)g(m_1) + g(m_2)$$

With B-linear G-equivariant maps, they form a category denoted by $\mathbf{Rep}_B(G)$.
(2) Let ℓ be a prime number. A *ℓ-adic representation of* G is a $\mathbf{Q}_\ell$-representation (where the action of G on $\mathbf{Q}_\ell$ is trivial). An *integral ℓ-adic representation of* G_K is a $\mathbf{Z}_\ell$-representation of G.

Proposition 5.2.4. Let G be a profinite group and $V \in \mathbf{Rep}_{\mathbf{Q}_\ell}(G)$. There exists an integral ℓ-adic representation $L \subset V$ which is a lattice, *i.e.* such that $V = L \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$.

Proof. Let $L_0 \subset V$ be any lattice (take the $\mathbf{Z}_\ell$-span of a basis). This is an open neighborhood of $0 \in V$: as the action of G is continuous, there exists an open subgroup $H \leqslant G$ such that $(\forall h \in H)\, h(L_0) \subset L_0$. Put $L = \sum\limits_{\tau \in G/H} \tau L_0$. As L_0 is compact (homeomorphic to $\mathbf{Z}_\ell^n$ with $n = \dim_{\mathbf{Q}_\ell}(V)$), so is L. As $L_0 \subset L$, this implies that L is a lattice, which is stable by G by construction. □

If ℓ is a prime number, let $\big(\zeta_{\ell^n}\big)_{n \in \mathbf{N}}$ be a *compatible* sequence of primitive ℓ^n-th roots of unity, which means that $\zeta_0 = 1$, $\zeta_\ell \neq 1$ and $(\forall n \in \mathbf{Z}_{\geqslant 0})\, \zeta_{\ell^{n+1}}^\ell = \zeta_{\ell^n}$.

Definition 5.2.5. (1) For $n \in \mathbf{Z}_{\geqslant 0}$, the extension $K_n := K(\zeta_{\ell^n})/K$ is Galois, and if $g \in \mathsf{Gal}(K_n/K)$, then $g(\zeta_{\ell^n}) = \zeta_{\ell^n}^{\chi_{\ell,n}(g)}$ where $\chi_{\ell,n}(g) \in (\mathbf{Z}/\ell^n\mathbf{Z})^\times$: the map $\chi_{\ell,n}\colon \mathsf{Gal}(K_n/K) \to (\mathbf{Z}/\ell^n\mathbf{Z})^\times$ is an injective group homomorphism. Put $K_\infty = \bigcup\limits_{n=0}^{\infty} K_n$: the subextension K_∞/K of $\overline{K}/K$ is called the (ℓ-adic) *cyclotomic extension*. It is Galois, and as n varies, the morphisms $\chi_{\ell,n}$ are compatible: passing to the inverse limit, one gets an injective group homomorphism

$$\chi_\ell\colon \mathsf{Gal}(K_\infty/K) \to \mathbf{Z}_\ell^\times$$

called the (ℓ-adic) *cyclotomic character*. Note that the image of χ_ℓ has finite index in $\mathbf{Z}_\ell^\times$.
The composite $G_K \to \mathsf{Gal}(K_\infty/K) \xrightarrow{\chi_\ell} \mathbf{Z}_\ell^\times$ is also denoted by χ_ℓ and called the cyclotomic character as well.
(2) The character χ_p provides a continuous action of G_K on $\mathbf{Z}_p$ (given by the multiplication by χ_p), in particular a p-adic representation of G_K. We denote by $\mathbf{Z}_p(1)$ this G_K-module: one has $\mathbf{Z}_p(1) = \varprojlim\limits_n \mu_{p^n}(\overline{K})$ (taken additively). If $i \in \mathbf{Z}$, we put $\mathbf{Z}_p(i) = \mathbf{Z}_p(1)^{\otimes i}$: this is nothing but $\mathbf{Z}_p$ endowed with the action of G_K given by the multiplication by χ_p^i. If M is any (topological) $\mathbf{Z}_p$-module with a continuous action of G_K, and $i \in \mathbf{Z}$, we put $M(i) = M \otimes_{\mathbf{Z}_p} \mathbf{Z}_p(i)$ (as G_K-modules). This is called a *Tate twist.*

Let π be a uniformizer of K. It is a uniformizer of K^{ur}. For $n \in \mathbf{Z}_{>0}$ prime to p, let $\pi_n = \sqrt[n]{\pi} \in \overline{K}$ be a n-th root of π. We may assume that the family $(\pi_n)_{p \nmid n}$ is compatible, *i.e.* $(\forall m, n \in \mathbf{N}_{>0})\, p \nmid nm \Rightarrow \pi_{nm}^m = \pi_n$. As $X^n - \pi \in K^{\mathrm{ur}}[X]$ is an Eisenstein polynomial, the extensions $K(\pi_n)/K$ and $K^{\mathrm{ur}}(\pi_n)/K^{\mathrm{ur}}$ have degree n. They are totally tamely ramified. In particular, $\bigcup\limits_{p \nmid n} K^{\mathrm{ur}}(\pi_n) \subset K^{\mathrm{tame}}$.

Proposition 5.2.6. We have $K^{\mathrm{tame}} = \bigcup\limits_{p \nmid n} K^{\mathrm{ur}}(\pi_n)$.

Proof. We have to show that if L is a finite tamely ramified subextension of $\overline{K}/K$, there exists a finite unramified subextension T of $\overline{K}/K$ and $n \in \mathbf{Z}_{>0}$ prime to p such that $L \subset T(\pi_n)$. Let T be the maximal unramified extension of L/K. As L/T is totally tamely ramified, one has $L = T(\varpi)$, where ϖ is a uniformizer of L such that ϖ^e is a uniformizer of T (where $e = [L : T]$ is prime to p, *cf* theorem 3.8.28): there exists $\alpha \in \mathcal{O}_T^\times$ such that ϖ is a root of the Eisenstein polynomial $E(X) = X^e - \pi\alpha \in \mathcal{O}_T[X]$. Let $\overline{u} \in \overline{\kappa}_K$ be a root of the reduction of $X^e - \overline{\alpha} \in \kappa_T[X]$ (where $\overline{\alpha}$ denotes the image of α in κ_T). As it is separable (because $e\alpha \in \mathcal{O}_T^\times$ since $p \nmid e$), one can lift $\overline{u}$ to a root $u \in \mathcal{O}_{K^{\mathrm{ur}}}$ of $X^e - \alpha \in \mathcal{O}_T[X]$ (by Newton's lemma). Replacing L by $L(u)$ (which is licit since $T(u)/T$ is unramified), we may assume that $u \in T$. We have $\varpi^e = (u\pi_e)^e$, so that $\varpi = \zeta u \pi_e$ for some e-th root of unity ζ. Replacing L by $L(\zeta)$ (which is licit since $T(\zeta)/T$ is unramified), we may assume that $\zeta \in T$, so that $\pi_e = \frac{\varpi}{\zeta u} \in L$, hence $T(\pi_e) \subset L$. As $[T(\pi_e) : T] = e = [L : T]$, this implies that $L = T(\pi_e)$. □

If $\ell \neq p$ is a prime number and $n \in \mathbf{Z}_{>0}$, the conjugates of π_{ℓ^n} are $\zeta_{\ell^n}^k \pi_{\ell^n}$ with $k \in \mathbf{Z}/\ell^n\mathbf{Z}$: if $g \in G_K$, one has $g(\pi_{\ell^n}) = \zeta_{\ell^n}^{t_\ell(g)} \pi_{\ell^n}$, where $t_\ell\colon I_K \to \mathbf{Z}/\ell^n\mathbf{Z}$ is a surjective group homomorphism. These are compatible as n varies, giving rise to a surjective group homomorphism

$$t_\ell\colon I_K \to \mathbf{Z}_\ell(1)$$

Remark 5.2.7. The Tate twist (which is relative to the ℓ-adic cyclotomic character) denotes the fact that t_ℓ is a *cocycle.* This means the following. Let $g \in I_K$ and $\gamma \in G_K$. As I_K is normal in G_K, we have $\gamma g \gamma^{-1} \in I_K$, and $(\gamma g \gamma^{-1})(\pi_{\ell^n}) = \zeta_{\ell^n}^{\chi(\gamma)(t_\ell(\gamma^{-1}) + t_\ell(g)) + t_\ell(\gamma)} \pi_{\ell^n}$ so that $t_\ell(\gamma g \gamma^{-1}) = \chi(\gamma) t_\ell(g) + \chi(\gamma) t_\ell(\gamma^{-1}) + t_\ell(\gamma)$. With $g = \mathsf{Id}_{\overline{K}}$ (in which case $t_\ell(g) = 0$), this shows that $\chi(\gamma) t_\ell(\gamma^{-1}) + t_\ell(\gamma) = 0$ for all $\gamma \in G_K$, so that the previous equality gives

$$t_\ell(\gamma g \gamma^{-1}) = \chi(\gamma) t_\ell(g).$$

Proposition 5.2.8. The sequence

$$\{\mathsf{Id}_{\overline{K}}\} \to P_K \to I_K \xrightarrow{(t_\ell)_\ell} \prod_{\ell \neq p} \mathbf{Z}_\ell(1) \to \{0\}$$

is exact.

Proof. By definition, one has $I_K/P_K \xrightarrow{\sim} \mathsf{Gal}(K^{\mathrm{tame}}/K^{\mathrm{ur}})$, and the fact that $\mathsf{Gal}(K^{\mathrm{tame}}/K^{\mathrm{ur}}) \xrightarrow{\sim} \prod\limits_{\ell\neq p} \mathbf{Z}_\ell(1)$ through $(t_\ell)_\ell$ follows from proposition 5.2.6. □

Theorem 5.2.9. (Grothendieck's monodromy theorem), *cf* [23, Appendix]) Let $\ell \neq p$ be a prime integer, and V an ℓ-adic representation of G_K. Assume that $K(\mu_{\ell^\infty})/K$ is infinite. Then V is *quasi-unipotent*, *i.e.* there exists a unique nilpotent endomorphism $N\colon V(1) \to V$ and an open subgroup $I \subseteq I_K$ such that

$$(\forall g \in I)(\forall v \in V)\ g(v) = \exp(t_\ell(g)N)(v)$$

Proof. By proposition 5.2.4, V contains a G_K-stable lattice L: the representation is thus given by a continuous group homomorphism $\rho\colon G_K \to \mathsf{GL}(L) \simeq \mathsf{GL}_n(\mathbf{Z}_\ell)$ where $n = \dim_{\mathbf{Q}_\ell}(V)$. The subgroup $\mathsf{Id}_L + \ell^2 \mathsf{End}(L) \subset \mathsf{GL}(L)$ is open and normal: let $I = \rho^{-1}\big(\mathsf{Id}_L + \ell^2\mathsf{End}(L)\big) \cap I_K$. This is an open subgroup of I_K and a normal subgroup of G_K. Let $\rho_{|I}\colon I \to \mathsf{Id}_L + \ell^2\mathsf{End}(L)$ be the group homomorphism induced by ρ. As $\mathsf{Id}_L + \ell^2\mathsf{End}(L)$ is a pro-ℓ-group and $\mathsf{Ker}(t_\ell)$ is an inverse limit of groups of order prime to p, the morphism ρ is trivial on $I \cap \mathsf{Ker}(t_\ell)$, *i.e.* $\rho_{|I}$ factors through $I/(I \cap \mathsf{Ker}(t_\ell))$.

If $g \in I$, then $\rho(g) \in \mathsf{Id}_L + \ell^2\mathsf{End}(L)$, so the series $\log(\rho(g)) = -\sum\limits_{i=1}^{\infty} \frac{1}{i}\big(\mathsf{Id}_L - \rho(g)\big)^i$ converges in $\ell^2\mathsf{End}(L)$ (for the ℓ-adic topology). Also, since $\log(\rho(g)) \in \ell^2\mathsf{End}(L)$, one has $\rho(g) = \exp(\log(\rho(g)))$. This provides a continuous group homomorphism $\log(\rho)\colon I \to \ell^2\mathsf{End}(L)$ that factors through $I/(I \cap \mathsf{Ker}(t_\ell))$, *i.e.* by t_ℓ: there exists a unique $N\colon V(1) \to V$ such that $(\forall g \in I)\ \log(\rho(g)) = t_\ell(g)N$. It remains to see that N is nilpotent.

Denote by $\chi_\ell\colon G_K \to \mathbf{Z}_\ell^\times$ be the ℓ-adic cyclotomic character. As $K(\mu_{\ell^\infty})/K$ is infinite, the image of χ_ℓ is infinite. If $\gamma \in G_K$ and $g \in I$, one has $\gamma^{-1}g\gamma \in I$ (because I is normal in G_K), and[41] $t_\ell(\gamma^{-1}g\gamma) = \chi_\ell(\gamma)t_\ell(g)$. We have $\rho(\gamma^{-1}g\gamma) = \rho(\gamma)^{-1}\rho(g)\rho(\gamma)$, taking the logarithm we get $t_\ell(\gamma^{-1}g\gamma)N = t_\ell(g)\rho(\gamma)^{-1}N\rho(\gamma)$ hence

$$\rho(\gamma)^{-1}N\rho(\gamma) = \chi_\ell(\gamma)N$$

This implies that the spectrum of N is stable by multiplication by $\mathsf{Im}(\chi_\ell)$. As $\mathsf{Im}(\chi_\ell)$ infinite and the spectrum of N is finite, the latter has to be reduced to $\{0\}$, and N is nilpotent. □

Remark 5.2.10. As $\ell \neq p$, one has $\mu_{\ell^\infty}(\overline{K}) = \mu_{\ell^\infty}(\overline{k}_K)$, so the condition in the theorem is automatically fulfilled when k is finite.

5.3. **The completion of a separable closure of a local field.** Let $(F, |.|)$ be a complete non archimedean valued field. Fix $\overline{F}$ an algebraic closure of F. The absolute value $|.|$ extends uniquely into an absolute value $|.|$ on $\overline{F}$ (*cf* corollary 3.5.7).

Lemma 5.3.1. (Krasner[42]). Let $\alpha, \beta \in \overline{F}$ be such that α is separable over F and:

$$|\alpha - \beta| < \min_{\alpha' \in \mathsf{C}(\alpha)\setminus\{\alpha\}} |\alpha - \alpha'|$$

where $\mathsf{C}(\alpha)$ is the set of conjugates of α over F. Then $F(\alpha) \subset F(\beta)$.

Proof. Put $\gamma = \beta - \alpha$ and $F' = F(\beta)$: we have $F'(\gamma) = F'(\alpha)$ so $F'(\gamma)/F'$ is separable. Let γ' be a conjugate of γ over F'. If $\gamma' \neq \gamma$, we can write $\gamma' = \beta - \alpha'$ with $\alpha' \in \mathsf{C}(\alpha)\setminus\{\alpha\}$. As γ' and γ are conjugate over F', we have $|\gamma'| = |\gamma|$, so that

$$|\alpha - \alpha'| = |\gamma' - \gamma| \leqslant |\gamma| = |\beta - \alpha|$$

which contradicts the hypothesis. This implies that γ has only one conjugate over F', *i.e.* $\gamma \in F'$, whence $\alpha \in F' = F(\beta)$. □

Lemma 5.3.2. If $|.|$ is not trivial, then an infinite and separable subextension of $\overline{F}/F$ is never complete.

[41] This is the precise meaning of remark 5.2.7.

[42] This result is in fact due to Ostrowski.

Proof. Let K be an infinite subextension of $\overline{F}/F$. Assume that $(K,|.|)$ is complete, and that K/F is separable. Choose a sequence $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ of elements in K that are all linearly independent over F. As $|.|$ is not trivial, there exists a sequence $(a_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ of elements in F such that the sequence $(|a_nx_n|)_{n\in\mathbf{Z}_{\geqslant 0}}$ is strictly decreasing and converges to 0. As K is complete, the series $s=\sum\limits_{n=0}^{\infty}a_nx_n$ converges in K. For $n\in\mathbf{Z}_{>0}$, put $s_n=\sum\limits_{i=0}^{n-1}a_ix_i$: the elements $\{s_n\}_{n\in\mathbf{Z}_{>0}}$ are all linearly independent over F. For $n\in\mathbf{Z}_{>0}$, let d_n be the smallest distance between s_n and its conjugates. a_0 being chosen arbitrarily, we can construct the sequence $(a_n)_{n\in\mathbf{Z}_{\geqslant 0}}$ inductively so that $|a_nx_n|<d_n$ for all $n\in\mathbf{Z}_{>0}$. As $(|a_nx_n|)_{n\in\mathbf{Z}_{\geqslant 0}}$ is strictly decreasing, we have $|s-s_n|=|a_nx_n|<d_n$. By Krasner's lemma, this implies that $s_n\in F(s)$. As $(s_n)_{n\in\mathbf{Z}_{>0}}$ is linearly independent, this implies that $[F(s):F]=\infty$, which contradicts the fact that $s\in K$ is algebraic over F. □

Remark 5.3.3. In the lemma 5.3.2, the separability condition is really necessary: let $K=\mathbf{F}_p(x_i)_{i\in\mathbf{Z}_{\geqslant 0}}$ be the field of rational fractions in the indeterminates $(x_i)_{i\in\mathbf{Z}_{\geqslant 0}}$ with coefficients in $\mathbf{F}_p$, and $F=K(\!(T)\!)$ the field of formal Laurent series with coefficients in K. Endowed with the T-adic absolute value $|.|$, the field F is complete. Then $F^{1/p}=K^{1/p}(\!(T^{1/p})\!)$ is a totally inseparable algebraic extension of F. The absolute value $|.|$ extends uniquely to $F^{1/p}$ (*cf* theorem 3.5.6), and the Frobenius map $\varphi\colon F^{1/p}\to F$ is a field isomorphism. As $|\varphi(f)|=|f|^p$ for all $f\in F^{1/p}$, the Frobenius map is also an homeomorphism, so that $F^{1/p}$ is also complete. On the other hand, the extension $F^{1/p}/F$ is infinite, because $K^{1/p}/K$ is (this can be seen as follows: for all $i\in\mathbf{Z}_{\geqslant 0}$, we have $x_i\notin\mathbf{F}_p(x_0,\ldots,x_{i-1},x_i^p,x_{i+1}^p,\ldots)$, so that

$$[\mathbf{F}_p(x_0^{1/p},\ldots,x_i^{1/p},x_{i+1},\ldots):\mathbf{F}_p(x_0^{1/p},\ldots,x_{i-1}^{1/p},x_i,x_{i+1},\ldots)]=p,$$

whence $[\mathbf{F}_p(x_0^{1/p},\ldots,x_i^{1/p},x_{i+1},\ldots):K]=p^{i+1}$ by induction).

From now on, $(K,|.|)$ denote a complete non archimedean valued field. We assume that $|.|$ is not trivial.

Proposition 5.3.4. $\kappa_{\overline{K}}$ is an algebraic closure of κ_K and $\left|\overline{K}^\times\right|=\{r\in\mathbf{R}_{>0}\,;\,(\exists n\in\mathbf{Z}_{>0})\,r^n\in|K^\times|\}=\rho^{\mathbf{Q}}$ for any element $\rho\in|K^\times|\backslash\{1\}$.

Proof. • Let $x\in\kappa_{\overline{K}}$: there exists $\widehat{x}\in\mathcal{O}_{\overline{K}}$ such that $\widehat{x}$ maps to x in $\kappa_{\overline{K}}=\mathcal{O}_{\overline{K}}/\mathfrak{m}_{\overline{K}}$. There exists a finite subextension L/K of $\overline{K}/K$ such that $\widehat{x}\in L$, *i.e.* $\widehat{x}\in\mathcal{O}_L$. Reducing modulo $\mathfrak{m}_L$ shows that $x\in\kappa_L$ is algebraic over κ_K.

• Let $P(X)\in\kappa_K[X]$ be a monic irreducible polynomial, and $\widehat{P}(X)\in\mathcal{O}_K[X]$ a monic lift of P. Then $\widehat{P}$ has a root $\alpha\in\overline{K}$, and $\alpha\in\mathcal{O}_{\overline{K}}$ (*cf* corollary 3.5.10): if $\overline{\alpha}$ denotes the image of α in $\kappa_{\overline{K}}$, we have $P(\overline{\alpha})=0$, hence P has a root in $\kappa_{\overline{K}}$, proving that $\kappa_{\overline{K}}$ is an algebraic closure of κ_K.

• Let L/K be a finite subextension of $\overline{K}/K$. We have $|L^\times|=|K^\times|^{1/e}$ where e is the ramification index of L/K. This implies that $|L^\times|\subset\{r\in\mathbf{R}_{>0}\,;\,(\exists n\in\mathbf{Z}_{>0})\,r^n\in|K^\times|\}$. As this holds for all subextension L/K of $\overline{K}/K$, we have $\left|\overline{K}^\times\right|\subset\{r\in\mathbf{R}_{>0}\,;\,(\exists n\in\mathbf{Z}_{>0})\,r^n\in|K^\times|\}$.

• Conversely, let $r\in\mathbf{R}_{>0}$ and $n\in\mathbf{Z}_{\geqslant 0}$ be such that $r^n\in|K^\times|$: there exists $m\in\mathbf{Z}$ such that $|\pi_K|^m=r^n$, where π_K is a uniformizer on K. Then $P(X)=X^n-\pi_K\in\mathcal{O}_K[X]$ is an Eisenstein polynomial: if $\alpha\in\overline{K}$ is a root of P, then $|\alpha|=|\pi_K|^{1/n}$, so that $r^n=|\alpha|^{nm}$, hence $r=|\alpha^m|\in\left|\overline{K}^\times\right|$. □

Corollary 5.3.5. The field $\kappa_{\overline{K}}$ is infinite, and $\left|\overline{K}^\times\right|$ is dense in $\mathbf{R}_{>0}$.

Notation. We denote by C the completion of $\overline{K}$ with respect to its absolute value $|.|$. The latter extends to C: we still denote by $|.|$ this extension.

Proposition 5.3.6. The field C is algebraically closed.

Proof. Let L be a finite extension of C. Replacing L by its normal closure over C, we may assume that L/C is normal. Denote by $|.|$ the unique extension of $|.|$ to L. Let $\alpha\in L$ and $P(X)=X^n+a_1X^{n-1}+\cdots+a_n\in C[X]$ its minimal polynomial over C. Let $\varepsilon\in\mathbf{R}_{>0}$: as $\overline{K}$ is dense in C, we can choose $b_1,\ldots,b_n\in\overline{K}$ such that $|b_i-a_i|\,|\alpha|^{n-i}<\varepsilon^n$ for all $i\in\{1,\ldots,n\}$. Put $Q(X)=X^n+b_1X^{n-1}+\cdots+b_n\in\overline{K}[X]$: we have $Q(\alpha)=Q(\alpha)-P(\alpha)=\sum\limits_{i=1}^{n}(b_i-a_i)\alpha^{n-i}$, so that $|Q(\alpha)|\leqslant\max\limits_{1\leqslant i\leqslant n}|b_i-a_i|\,|\alpha|^{n-i}<\varepsilon^n$. On the other hand, let $\beta_1,\ldots,\beta_n\in\overline{K}$ be the roots of $Q(X)$. As $Q(\alpha)=\prod\limits_{i=1}^{n}(\alpha-\beta_i)$, we have $\prod\limits_{i=1}^{n}|\alpha-\beta_i|<\varepsilon^n$, so there exists $i\in\{1,\ldots,n\}$ such that $\beta:=\beta_i\in\overline{K}$ satisfies $|\alpha-\beta|<\varepsilon$. We can thus construct a sequence $(x_k)_{k\in\mathbf{Z}_{>0}}$ in $\overline{K}$ such that $|\alpha-x_k|<2^{-k}$ for all $k\in\mathbf{Z}_{>0}$. This implies that $\alpha=\lim\limits_{k\to\infty}x_k\in C$. In particular, we must have $L=C$. □

Definition 5.3.7. The completion of "the" algebraic closure of $\mathbf{Q}_p$ is denoted by $\mathbf{C}_p$.

5.3.8. *The Galois action on C.* The content of this part is taken from [2]. Recall that $(K, |.|)$ is a complete non archimedean valued fied such that $|.|$ is non trivial. Let $\overline{K}$ be a separable closure of K, and $(C, |.|)$ the completion of $(\overline{K}, |.|)$. As the group $G_K := \mathsf{Gal}(\overline{K}/K)$ acts by isometries on $\overline{K}$, the action of G_K extends to C by continuity. Let $\sqrt{K}$ denote the *perfect closure* of K, *i.e.*

$$\sqrt{K} = \begin{cases} K & \text{if } \mathsf{char}(K) = 0 \\ K^{p^{-\infty}} & \text{if } \mathsf{char}(K) = p > 0 \end{cases}$$

Theorem 5.3.9. We have $C^{G_K} = \widehat{\sqrt{K}}$, *i.e.* the field of elements in C that are invariant under G_K is the completion of the perfect closure of K.

We will need a few lemmas.

Lemma 5.3.10. Let p be a prime number and $n \in \mathbf{Z}_{\geqslant 1}$. If $k \in \{0, \ldots, v_p(n)\}$, then $v_p\big(\binom{n}{p^k}\big) = v_p(n) - k$.

Proof. Let $s(n)$ be the sum of the digits of the p-adic development of n. Then $v_p(n!) = \frac{n-s(n)}{p-1}$. This implies that $v_p\big(\binom{n}{p^k}\big) = \frac{n-s(n)-(p^k-1+n-p^k-s(n-p^k))}{p-1} = \frac{s(n-p^k)+1-s(n)}{p-1}$. Put $v = v_p(n)$ and write $n = p^v m$ with $p \nmid m$: we have $s(n) = s(m)$ and $n - p^k = p^k(p^{v-k}m - 1)$ so that $s(n - p^k) = s(p^{v-k}m - 1)$. Let $m = a_0 + pa_1 + \cdots + p^r a_r$ with $a_i \in \{0, \ldots, p-1\}$ for $i \in \{0, \ldots, r\}$ be the p-adic development of m. We have $a_0 \neq 0$, and

$$\begin{aligned} p^{v-k}m - 1 &= p^{v-k} - 1 + p^{v-k}(a_0 - 1) + p^{v-k+1}a_1 + \cdots + p^{v-k+r}a_r \\ &= (1 + p + p^2 + \cdots + p^{v-k-1})(p-1) + p^{v-k}(a_0 - 1) + p^{v-k+1}a_1 + \cdots + p^{v-k+r}a_r \end{aligned}$$

so that $s(p^{v-k}m - 1) = (v-k)(p-1) + s(m) - 1$, which implies that $s(n - p^v) + 1 - s(n) = (v-k)(p-1)$ whence $v_p\big(\binom{n}{p^k}\big) = v - k$. □

Lemma 5.3.11. Let $P(X) = \prod\limits_{i=1}^{d}(X - \alpha_i) = \sum\limits_{j=0}^{d} a_j X^j \in C[X]$. Assume that $|\alpha_1| \leqslant \cdots \leqslant |\alpha_d|$. If $j \in \{0, \ldots, d-1\}$, we have $|a_j| \leqslant |\alpha_{j+1} \cdots \alpha_n|$. If $|\alpha_j| < |\alpha_{j+1}|$, we have equality, more precisely

$$\Big|1 - (-1)^{d-j}\tfrac{a_j}{\alpha_{j+1}\cdots\alpha_n}\Big| < 1.$$

Proof. We have $a_j = (-1)^{n-j} \sum\limits_{i_1 < \cdots < i_{d-j}} \alpha_{i_1} \cdots \alpha_{i_{d-j}}$: the ordering of the roots implies the inequalities $\big|\alpha_{i_1} \cdots \alpha_{i_{d-j}}\big| \leqslant |\alpha_{j+1} \cdots \alpha_n|$ proving the first inequality by the triangle inequality. When $|\alpha_j| < |\alpha_{j+1}|$, we have $\big|\alpha_{i_1} \cdots \alpha_{i_{d-j}}\big| < |\alpha_{j+1} \cdots \alpha_n|$ unless $i_k = j + k$ for all $k \in \{1, \ldots, d-j\}$, proving the second part of the lemma in that case. □

Lemma 5.3.12. Let $P(X) \in C[X]$ be of degree $d = p^\delta d_1 = qd_1$ where $p = \max\{1, \mathsf{char}(\kappa_C)\}$, $\delta \in \mathbf{Z}_{\geqslant 0}$ and $\mathsf{gcd}(p, d_1) = 1$. Assume $q < d$ and that a disk $D \subset C$ contains all the roots of P. Then $P^{[q]}$ has a zero in D.

Proof. We may assume that P is monic and that $0 \in D$: this implies that $D = \mathrm{D}(0, r)$ for some $r \in \mathbf{R}_{\geqslant 0}$. Write $P(X) = \prod\limits_{i=1}^{d}(X - \alpha_i) = \sum\limits_{j=0}^{d} a_j X^j$ with $|\alpha_1| \leqslant \cdots \leqslant |\alpha_d| \leqslant r$. By lemma 5.3.11, we have $|a_j| \leqslant r^{d-j}$ for all $j \in \{0, \ldots, d-1\}$. We have

$$P^{[q]}(X) = \sum_{j=q}^{d} \tbinom{j}{q} a_j X^{j-q} = \sum_{k=0}^{d-q} b_k X^k$$

where $b_k = \binom{k+q}{q} a_{k+q}$ for $k \in \{0, \ldots d-q\}$. As P is monic, we have $b_{d-q} = \binom{d}{q}$, so we can write

$$P^{[q]}(X) = \tbinom{d}{q} \prod_{k=1}^{d-q}(X - \beta_k)$$

so that $b_0 = \binom{d}{q} \prod\limits_{k=1}^{d-q}(-\beta_k)$. We have $\Big|\binom{d}{q}\Big| = 1$, because the image of $\binom{d}{q}$ is invertible in κ_C (this is trivial if $\mathsf{char}(\kappa_C) = 0$, and follows from lemma 5.3.10 if $\mathsf{char}(\kappa_C) = p > 0$). This implies that $\prod\limits_{k=1}^{d-q} |\beta_k| \leqslant r^{d-q}$, so that there exists $k_0 \in \{1, \ldots, d-q\}$ such that $|\beta_k| \leqslant r$ *i.e.* $\beta_k \in D$. □

Lemma 5.3.13. Assume that $\mathsf{char}(C) = 0$ and $\mathsf{char}(\kappa_C) = p > 0$. Let $P(X) \in C[X]$ be of degree $d = p^\delta > 1$ having all its zeros in a disk $D = \mathrm{D}(a, r)$. If $q = p^{\delta-1}$, then $P^{[q]}$ has a zero in $\mathrm{D}\big(a, r\,|p|^{-\frac{1}{d-q}}\big)$.

Proof. Again, we may assume that P is monic and that $D = \mathrm{D}(0,r)$. Write $P(X) = \prod\limits_{i=1}^{d}(X-\alpha_i) = \sum\limits_{j=0}^{d} a_j X^j$: as before, we have

$$P^{[q]}(X) = \sum_{j=q}^{d}\tbinom{j}{q}a_j X^{j-q} = \tbinom{d}{q}\prod_{k=1}^{d-q}(X-\beta_k)$$

so that $a_q = \binom{d}{q}\prod\limits_{k=1}^{d-q}(-\beta_k)$. As $v_p\big(\binom{d}{q}\big) = 1$ by lemma 5.3.10, we have $|p|\prod\limits_{k=1}^{d-q}|\beta_k| \leqslant r^{d-q}$, so that there exists $k \in \{1,\dots,d-q\}$ such that $|p|\,|\beta_k|^{d-q} \leqslant r^{d-q}$ *i.e.* $|\beta_k| \leqslant r\,|p|^{-\frac{1}{d-q}}$. □

Definition 5.3.14. If $\alpha \in \overline{K}$, let

$$\Delta_K(\alpha) = \Delta(\alpha) = \sup_{\alpha' \in \mathrm{C}(\alpha)\setminus\{\alpha\}} |\alpha' - \alpha|$$

with the convention that $\Delta(\alpha) = 0$ if $\alpha \in \sqrt{K}$.

Remark 5.3.15. If $\alpha \in \overline{K}$ and $x \in K$, we have $|\alpha' - \alpha| \leqslant \max\{|\alpha' - x|, |\alpha - x|\} = |\alpha - x|$ for all conjugate α' of α (since elements of G_K act by isometries on $\overline{K}$). This implies that $\Delta(\alpha) \leqslant |\alpha - x|$. As this holds for all $x \in K$, this means that $\Delta(\alpha) \leqslant d(\alpha, K)$. The aim of the next few lemmas is to show that $\Delta(\alpha)$ is "close" to $d(\alpha, K)$.

Lemma 5.3.16. Assume that $\mathsf{char}(K) = 0$ and $\mathsf{char}(\kappa_K) = p > 0$. If $\alpha \in \overline{K}$ has degree n over K, then there exists $x \in K$ such that

$$|\alpha - x| \leqslant \Delta(\alpha)\,|p|^{-c(n)}$$

where $c(n) = \sum\limits_{i=1}^{\lambda(n)} \frac{1}{p^i - p^{i-1}}$ and $\lambda(n) = \max\{e \in \mathbf{Z}_{\geqslant 0}\,;\, p^e \leqslant n\}$.

Proof. We proceed by induction on $n \in \mathbf{Z}_{>0}$, the case $n = 1$ being trivial. Let $P(X) \in K[X]$ be the minimal polynomial of α over K. Write $n = p^\delta n_1 = q n_1$ with $p \nmid n_1$. Let D be the disc centered at α with radius $\Delta(\alpha)$.

- If $n_1 > 1$, lemma 5.3.12 implies that $P^{[d]}$ has a root $\beta \in D$, *i.e.* such that $|\alpha - \beta| \leqslant \Delta(\alpha)$. If β' ia a conjugate of β over K, then there exists $\sigma \in G_K$ such that $\sigma(\beta) = \beta'$. This implies that

$$|\beta' - \beta| = |\sigma(\beta) - \beta| = |\sigma(\beta - \alpha) + (\sigma(\alpha) - \alpha) + (\alpha - \beta)| \leqslant \max\{|\alpha - \beta|, |\sigma(\alpha) - \alpha|\} \leqslant \Delta(\alpha)$$

since $|\sigma(\alpha - \beta)| = |\alpha - \beta|$. As this holds for every conjugate β' of β over K, this implies that $\Delta(\beta) \leqslant \Delta(\alpha)$. As $[K(\beta) : K] \leqslant \deg(P^{[q]}) = n - q < n$, the induction hypothesis implies that there exists $x \in K$ such that $|\beta - x| \leqslant \Delta(\beta)\,|p|^{-c(n-q)}$. We have $\lambda(n) \geqslant \lambda(n-q)$, hence $c(n) \geqslant c(n-q)$, thus $|p|^{-c(n-q)} \leqslant |p|^{-c(n)}$ (as $1 < |p|^{-1}$), so $|\beta - x| \leqslant \Delta(\alpha)\,|p|^{-c(n)}$. As $|\alpha - x| \leqslant \max\{|\alpha - \beta|, |\beta - x|\}$, we get $|\alpha - x| \leqslant \Delta(\alpha)\,|p|^{-c(n)}$ (since $|\alpha - \beta| \leqslant \Delta(\alpha)$ and $1 \leqslant |p|^{-c(n)}$).
- If $n_1 = 1$, put $q = p^{\delta-1}$, lemma 5.3.13 shows that $P^{[q]}$ has a root β such that $|\beta - \alpha| \leqslant \Delta(\alpha)\,|p|^{-\frac{1}{d-q}}$. As before, we have $|\beta' - \beta| \leqslant \max\{|\alpha - \beta|, |\sigma(\alpha) - \alpha|\} \leqslant \Delta(\alpha)\,|p|^{-\frac{1}{d-q}}$ for all conjugate β' of β over K, so that $\Delta(\beta) \leqslant \Delta(\alpha)\,|p|^{-\frac{1}{d-q}}$. By the induction hypothesis, there exists $x \in K$ such that $|\beta - x| \leqslant \Delta(\beta)\,|p|^{-c(n-q)}$, *i.e.* $|\beta - x| \leqslant \Delta(\alpha)\,|p|^{-c(n-q)-\frac{1}{n-q}}$. As $n = p^\delta$, we have $n - q = p^{\delta-1}(p-1)$, so $\lambda(n-q) = \delta - 1$, hence $c(n-q) = \sum\limits_{i=1}^{\delta-1}\frac{1}{p^i - p^{i-1}} = c(n) - \frac{1}{n-q}$: this implies that $|\beta - x| \leqslant \Delta(\alpha)\,|p|^{-c(n)}$. As before, we have $|\alpha - x| \leqslant \max\{|\alpha - \beta|, |\beta - x|\}$, so that $|\alpha - x| \leqslant \Delta(\alpha)\,|p|^{-c(n)}$ (because $|\alpha - \beta| \leqslant \Delta(\alpha)\,|p|^{-\frac{1}{d-q}}$ and $|p|^{-\frac{1}{d-q}} \leqslant |p|^{-c(n)}$). □

Proposition 5.3.17. Assume that $\mathsf{char}(K) = 0$ and $\mathsf{char}(\kappa_K) = p > 0$. If $\alpha \in \overline{K}$, there exists $x \in K$ such that $|\alpha - x| \leqslant \Delta(\alpha)\,|p|^{-\frac{p}{(p-1)^2}}$.

Proof. This follows from lemma 5.3.16, since $c(n) \leqslant \sum\limits_{i=1}^{\infty}\frac{1}{p^i - p^{i-1}} = \frac{1}{p-1}\sum\limits_{k=0}^{\infty}\frac{1}{p^k} = \frac{p}{(p-1)^2}$ for all $n \in \mathbf{Z}_{>0}$. □

Lemma 5.3.18. Assume that $\mathsf{char}(K) = p > 0$. If $\alpha \in \overline{K}$ has degree p over K, there exists $\beta \in K^{1/p}$ such that $|\alpha - \beta| \leqslant |\alpha|^{\frac{p-1}{p}}\,\Delta(\alpha)^{\frac{1}{p}}$.

Proof. This is trivial if α is not separable over K: assume that α is separable over K. Let $\alpha_1, \ldots, \alpha_p$ be the conjugates of α over K. For $i \in \{1, \ldots, p\}$, put $\eta_i = \alpha_i - \alpha$. We have

$$\mathsf{N}_{K(\alpha)/K}(\alpha) = \prod_{i=1}^{p} \alpha_i = \prod_{i=1}^{p} (\alpha + \eta_i) = \alpha^p + b_1 \alpha^{p-1} + \cdots + b_p.$$

where b_i is the i-th symmetric function of $\eta_1, \ldots, \eta_p$. As $|\eta_k| \leqslant \Delta(\alpha)$ for all $k \in \{1, \ldots, p\}$, we have $|b_i| \leqslant \Delta(\alpha)^i$ for all $i \in \{1, \ldots, p\}$. Let $\beta \in K^{1/p}$ be such that $\beta^p = \mathsf{N}_{K(\alpha)/K}(\alpha)$: we have

$$(\beta - \alpha)^p = b_1 \alpha^{p-1} + \cdots + b_p$$

so that $|\alpha - \beta| \leqslant \max\limits_{1 \leqslant i \leqslant p} |b_i| \, |\alpha|^{p-i} = \Delta(\alpha) \, |\alpha|^{p-1}$ since $\Delta(\alpha) \leqslant |\alpha|$ (because $|\alpha' - \alpha| \leqslant \max\{|\alpha'|, |\alpha|\} = |\alpha|$ for every conjugate α' of α over K). □

Lemma 5.3.19. Assume that $\mathsf{char}(K) = p > 0$. If $\alpha \in \overline{K}$ has degree p over K and $j \in \mathbf{Z}_{>0}$, there exists $\beta_j \in \sqrt{K}$ such that

$$|\alpha - \beta_j| \leqslant |\alpha|^{(\frac{p-1}{p})^j} \, \Delta(\alpha)^{\frac{1}{p} + \frac{p-1}{p^2} + \cdots + \frac{(p-1)^{j-1}}{p^j}}.$$

Proof. We proceed by induction on $j \in \mathbf{Z}_{>0}$, the case $j = 1$ being lemma 5.3.18. Assume β_j has been constructed. Applying lemma 5.3.18 to $\alpha - \beta_j \in \sqrt{K}$, there exists $\beta_{j+1} \in \sqrt{K}^{1/p} = \sqrt{K}$ such that

$$|\alpha - \beta_{j+1}| \leqslant |\alpha - \beta_j|^{\frac{p-1}{p}} \, \Delta(\alpha - \beta_j)^{\frac{1}{p}}.$$

As $\beta_j \in \sqrt{K}$, the element β_j has only one conjugate, so that $\Delta(\alpha - \beta_j) = \Delta(\alpha)$: we have

$$|\alpha - \beta_{j+1}| \leqslant \left(|\alpha|^{(\frac{p-1}{p})^j} \, \Delta(\alpha)^{\frac{1}{p} + \frac{p-1}{p^2} + \cdots + \frac{(p-1)^{j-1}}{p^j}} \right)^{\frac{p-1}{p}} \Delta(\alpha)^{\frac{1}{p}} = |\alpha|^{(\frac{p-1}{p})^{j+1}} \, \Delta(\alpha)^{\frac{1}{p} + \frac{p-1}{p^2} + \cdots + \frac{(p-1)^j}{p^{j+1}}}.$$

□

Lemma 5.3.20. Assume that $\mathsf{char}(K) = p > 0$. If $\alpha \in \overline{K}$ has degree p over K is such that $|\alpha| \leqslant 1$, and $\ell \in \mathbf{Z}_{>0}$, there exists $\beta \in \sqrt{K}$ such that $|\alpha - \beta| \leqslant \Delta(\alpha)^{1 - \frac{1}{\ell}}$.

Proof. This follows from lemma 5.3.19 and the fact that $\frac{1}{p} + \sum\limits_{j=2}^{\infty} \frac{(p-1)^{j-1}}{p^j} = \frac{1}{p} + \frac{p-1}{p^2} \sum\limits_{k=0}^{\infty} \left(\frac{p-1}{p}\right)^k = 1.$ □

Proposition 5.3.21. Assume that $\mathsf{char}(K) = p$. If $\alpha \in \overline{K}$ is such that $|\alpha| \leqslant 1$ and $\ell \in \mathbf{Z}_{>0}$, there exists $\beta \in \sqrt{K}$ such that $|\alpha - \beta| \leqslant \Delta(\alpha)^{1 - \frac{1}{\ell}}$.

Proof. • Case where K is perfect and every finite extension of K has degree a power of p. Fix a tower of extensions $K = K_0 \subset K_1 \subset \cdots \subset K_n$ such that $\alpha \in K_n$ and $[K_i : K_{i-1}] = p$ for all $i \in \{1, \ldots, n\}$ (take for K_n any finite Galois extension of K containing α, and use the fact that p-groups are solvable). By lemma 5.3.20, there exists $\gamma \in \sqrt{K_{n-1}} = K_{n-1}$ such that $|\alpha - \gamma| \leqslant \Delta_{K_{n-1}}(\alpha)^{1 - \frac{1}{2\ell}} \leqslant \Delta(\alpha)^{1 - \frac{1}{2\ell}}$. If γ' is a conjugate of γ over K, there exists $\sigma \in G_K$ such that $\gamma' = \sigma(\gamma)$, so that

$$|\gamma' - \gamma| \leqslant \max\{|\sigma(\gamma - \alpha)|, |\sigma(\alpha) - \alpha|, |\alpha - \gamma|\} = \max\{\Delta(\alpha), |\alpha - \gamma|\} \leqslant \Delta(\alpha)^{1 - \frac{1}{2\ell}}$$

since $\Delta(\alpha) \leqslant \Delta(\alpha)^{1 - \frac{1}{2\ell}}$ since $\Delta(\alpha) \leqslant 1$ because $\Delta(\alpha) \leqslant |\alpha| \leqslant 1$. As this holds for every conjugate γ' of γ over K, this implies that $\Delta(\gamma) \leqslant \Delta(\alpha)^{1 - \frac{1}{2\ell}}$. By induction on n we can find an element $\beta \in \sqrt{K}$ such that $|\gamma - \beta| \leqslant \Delta(\beta)^{1 - \frac{1}{2\ell}} \leqslant \Delta(\alpha)^{(1 - \frac{1}{2\ell})^2}$, thus $|\alpha - \beta| \leqslant \Delta(\alpha)^{(1 - \frac{1}{2\ell})^2} \leqslant \Delta(\alpha)^{1 - \frac{1}{\ell}}$ (since $\left(1 - \frac{1}{2\ell}\right)^2 \geqslant 1 - \frac{1}{\ell}$ and $\Delta(\alpha) \leqslant 1$).

• Case where K is perfect. Let L be the subfield of $\overline{K}$ fixed by the pro-p-Sylow of G_K: this is the composite of all subextensions of $\overline{K}/K$ that are of degree prime to p. By construction, finite extensions of L have degree a power of p. By the previous case, there exists $\gamma \in \sqrt{L} = L$ such that $|\alpha - \gamma| \leqslant \Delta_L(\alpha)^{1 - \frac{1}{\ell}}$. As before, this implies that $\Delta_K(\gamma) \leqslant \Delta_K(\alpha)^{1 - \frac{1}{\ell}}$.

As $[K(\gamma) : K]$ is prime to p, we may define $\beta = \frac{1}{[K(\gamma):K]} \mathsf{Tr}_{K(\gamma)/K}(\gamma) \in K$. Denote by J be the set of K-embeddings of $K(\gamma)$ into $\overline{K}$: we have $\#J = [K(\gamma) : K]$ since γ is separable over K (because K is perfect). This implies that $\beta - \gamma = \frac{1}{[K(\gamma):K]} \sum\limits_{\sigma \in J} (\sigma(\gamma) - \gamma)$. As $|[K(\gamma) : K]| = 1$ (because $p \nmid [K(\gamma) : K]$), we have $|\beta - \gamma| = \left| \sum\limits_{\sigma \in J} (\sigma(\gamma) - \gamma) \right| \leqslant \max\limits_{\sigma \in J} |\sigma(\gamma) - \gamma| = \Delta_K(\gamma) \leqslant \Delta_K(\alpha)^{1 - \frac{1}{\ell}}$, so that $|\alpha - \beta| \leqslant \Delta_K(\alpha)^{1 - \frac{1}{\ell}}$.

• General case. What precedes (with K replaced by $\sqrt{K}$) implies that there exists $\beta \in \sqrt{K}$ such that $|\alpha - \beta| \leqslant \Delta_{\sqrt{K}}(\alpha)^{1 - \frac{1}{\ell}} \leqslant \Delta_K(\alpha)^{1 - \frac{1}{\ell}}$. □

Proposition 5.3.22. Assume that $\mathsf{char}(\kappa_K) = 0$. If $\alpha \in \overline{K}$, there exists $\beta \in K$ such that $|\alpha - \beta| \leqslant \Delta(\alpha)$.

Proof. Put $\beta = \frac{1}{[K(\alpha):K]} \operatorname{\mathsf{Tr}}_{K(\alpha)/K}(\alpha) \in K$ and let J be the set of K-embeddings of $K(\alpha)$ into $\overline{K}$: we have $\# J = [K(\alpha):K]$ since $\mathsf{char}(K) = 0$ (because $\mathsf{char}(\kappa_K) = 0$). We have $\beta - \alpha = \frac{1}{[K(\alpha):K]} \sum\limits_{\sigma \in J} (\sigma(\alpha) - \alpha)$: as $|[K(\alpha):K]| = 1$ (because $\mathsf{char}(\kappa_K) = 0$ again), we have $|\beta - \alpha| \leqslant \max\limits_{\sigma \in J} |\sigma(\alpha) - \alpha| = \Delta(\alpha)$. □

Proof of theorem 5.3.9. Let $c \in C^{G_K}$. Rescaling via an element of K, we may assume that $|c| \leqslant 1$. If $\lambda \in \left|\overline{K}^\times\right|$ and $\ell \in \mathbf{Z}_{>0}$, there exists $\alpha \in \overline{K}$ such that $|c - \alpha| \leqslant w_K(\lambda, \ell)$ where

$$w_K(\lambda, \ell) = \begin{cases} \lambda & \text{if } \mathsf{char}(\kappa_K) = 0 \\ \lambda \, |p|^{\frac{p}{(p-1)^2}} & \text{if } \mathsf{char}(K) = 0 \text{ if } \mathsf{char}(\kappa_K) = p > 0 \\ \lambda^{(1 - \frac{1}{\ell})^{-1}} & \text{if } \mathsf{char}(K) = p > 0 \end{cases}$$

(by density of $\overline{K}$ in C). If $\sigma \in G_K$, we have

$$|\sigma(\alpha) - \alpha| = |\sigma(\alpha - c) + c - \alpha| \leqslant \max\{|\sigma(\alpha - c)|, |\alpha - c|\} = |c - \alpha| \leqslant w_K(\lambda, \ell)$$

so that $\Delta(\alpha) \leqslant w_K(\lambda, \ell)$. By propositions 5.3.17, 5.3.21 and 5.3.22, there exists $\beta \in \sqrt{K}$ such that $|\alpha - \beta| \leqslant \lambda$. As λ was arbitrary, this implies that $c \in \widehat{\sqrt{K}}$. This implies that $C^{G_K} \subset \widehat{\sqrt{K}}$. The reverse inclusion is obvious. □

Theorem 5.3.23. The separable closure K^{sep} of K in $\overline{K}$ is dense in C, *i.e.* $C = \widehat{K^{\mathrm{sep}}}$.

Proof. This is obvious when $\mathsf{char}(K) = 0$ (since $K^{\mathrm{sep}} = \overline{K}$): we henceforth assume that $\mathsf{char}(K) = p > 0$. Put $L = K^{\mathrm{sep}}$, so that $\overline{K} = \sqrt{L}$. Let $c \in C$: we have to show that c can be approximated by elements of L. We may assume that $|c| \leqslant 1$. As in the proof of theorem 5.3.9, if $\lambda \in \left|\overline{K}^\times\right|$, there exists $\alpha \in \overline{K}$ such that $|c - \alpha| \leqslant \lambda$. There exists a power q of p such that $a = \alpha^q \in L$. Let $b \in K^\times$ (to be chosen later), and $\beta \in L^\times$ a root of smallest absolute value of $P(X) = X^q - bX - a$. We have $P'(X) = b \neq 0$, so P is separable, hence $\beta \in L$. We have $(\beta - \alpha)^q = \beta^q - a = b\beta$, so that

$$(*) \qquad |\alpha - \beta| = |b\beta|^{\frac{1}{q}}\,.$$

As $|.|$ is not trivial, we can choose $b \in L^\times$ such that

$$|b| < \min\big\{\, |a|^{\frac{q-1}{q}}, \lambda^q \, |a|^{-\frac{1}{q}} \,\big\}.$$

Let $\beta = \beta_1, \ldots, \beta_q$ be the conjugates of β over K, such that $|\beta_1| \leqslant \cdots \leqslant |\beta_q|$: we have $|a| = |\beta_1 \cdots \beta_q| \geqslant |\beta|^q$ whence $|\beta| \leqslant |a|^{\frac{1}{q}}$. If $|\beta| < |a|^{\frac{1}{q}}$ then $|b\beta| < |a|$, so that $|\beta|^q = |b\beta + a| = |a|$, whence $|\beta|^q = |a|$, contradicting $|\beta| < |a|^{\frac{1}{q}}$: we have $|\beta| = |a|^{\frac{1}{q}}$ (this can be seen directly on Newton's polygon of P, regardless to the minimality of $|\beta|$). Equation $(*)$ thus implies that $|\alpha - \beta| = |b|^{\frac{1}{q}} \, |a|^{\frac{1}{q^2}} < \lambda$, so that $|c - \beta| \leqslant \lambda$. As λ is arbitrary, this shows that L is dense in C. □

5.4. **Exercises.**

Exercise 5.4.1. Let K be a field, with separable closure K^{sep}, and K^{ab} be the maximal abelian extension of K inside K^{sep}. Put $G_K = \mathsf{Gal}(K^{\mathrm{sep}}/K)$. Prove that K^{ab} is a Galois extension of K, and that $\mathsf{Gal}(K^{ab}/K)$ is isomorphic to $G_K/[G_K, G_K]$, where $[G_K, G_K]$ denotes the closure of the commutator subgroup of G_K.

Exercise 5.4.2. Let L be a field, and view $\mathsf{Aut}(L)$ as a subset of $L^L = \prod\limits_{x \in L} L$ of all maps $L \to L$. Give L the discrete topology, L^L the product topology, and $\mathsf{Aut}(L)$ the relative topology.

(1) Prove that $\mathsf{Aut}(L)$ is a topological group; *i.e.* the composition map $\mathsf{Aut}(L) \times \mathsf{Aut}(L) \to \mathsf{Aut}(L)$ and the map $\mathsf{Aut}(L) \to \mathsf{Aut}(L)$ sending each automorphism of L to its inverse are continuous.

(2) Let K be a subfield of L. Prove that L is Galois over K if and only if there is a compact subgroup G of $\mathsf{Aut}(L)$ such that K is the field of invariants of G. Prove also that such a subgroup G, if it exists, is necessarily equal to $\mathsf{Gal}(L/K)$, and that its topology coincides with the Krull topology on $\mathsf{Gal}(L/K)$.

Exercise 5.4.3. (0) Let F be a field and $x, y \in F$. Assume that $\mathsf{char}(F) \neq 2$, and that $\sqrt{x}, \sqrt{y}, \sqrt{xy} \notin F$. Show that $[F(\sqrt{x}, \sqrt{y}) : F] = 4$. Deduce that if $F(S)$ is an extension of F generated by n square roots of elements in F such that every nonempty subset of S has product not in F, then $[F(S) : F] = 2^n$.

Let $(p_1, p_2, \ldots)$ be the sequence of prime integers, and $K = \mathbf{Q}(\sqrt{p_k})_{k \in \mathbf{Z}_{>0}}$.

(1) Show that $K/\mathbf{Q}$ is a Galois extension and describe its Galois group.

(2) Show that for all $n \in \mathbf{Z}_{>0}$, the profinite $\mathsf{Gal}(K/\mathbf{Q})$ contains non-open subgroups of index 2^n.

(3) Deduce that for all $n \in \mathbf{Z}_{>0}$, the profinite $\mathsf{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ contains non-open subgroups of index 2^n.

Exercise 5.4.4. Let G be a profinite group.
(1) Let L be a field. Assume that $G \subset \mathsf{Aut}(L)$, and that the stabilizer of each element of L in G is an open subgroup of G. Put $K = L^G$. Show that L/K is Galois, and that $G = \mathsf{Gal}(L/K)$ (this is a generalization of Artin's theorem).
(2) Show that G is the Galois group of some Galois field extension.

Exercise 5.4.5. Let $\overline{\mathbf{Q}}_p$ be an algebraic closure of $\mathbf{Q}_p$. Assume that $\overline{\mathbf{Q}}_p$ is complete for $|.|_p$. For each $m \in \mathbf{Z}_{>0}$, let $\zeta_m \in \overline{\mathbf{Q}}_p$ be a primitive m-th root of unity. Put $\alpha = \sum\limits_{n=1}^{\infty} p^n \zeta_{f(n)}$ (where $f(n) = n$ if $p \nmid n$, and $f(n) = 1$ if $p \mid n$), and $K = \mathbf{Q}_p(\alpha)$.
(1) Show that $\zeta_{f(n)} \in K$ for all $n \in \mathbf{Z}_{>0}$.
(2) Deduce that $\overline{\mathbf{Q}}_p$ is not complete.

Exercise 5.4.6. Show that $\overline{\mathbf{Q}}$ is dense in $\mathbf{C}_p$ (this implies that $\mathbf{C}_p$ is *separable i.e.* that it contains a countable dense subset).

Exercise 5.4.7. (Applications of Krasner's lemma). Let $(K, |.|)$ be a local field, and $\overline{K}$ an algebraic closure of K.
(1) Let $P, Q \in K[X]$ be monic polynomials of degree $n \in \mathbf{Z}_{>0}$. Assume that P is irreducible and separable. Show that if $|P - Q|_{\text{Gauss}}$ is small enough, then Q is also irreducible, and that if $\alpha \in \overline{K}$ is a root of P, then there exists a root β of Q such that $K(\alpha) = K(\beta)$.
From now on, we assume that K is a finite extension of $\mathbf{Q}_p$.
(2) Show that there are finitely many subextensions L of $\overline{K}/K$ of given degree n.
(3) Show that there is a finite subextension L of $K/\mathbf{Q}$ such that $[L : \mathbf{Q}] = [K : \mathbf{Q}_p]$ and $K = L\,\mathbf{Q}_p$.

Exercise 5.4.8. Let A be a closed sub-$\mathbf{Q}_p$-algebra of $\mathbf{C}_p$. Show that A is a field.

Exercise 5.4.9. Let p be a prime integer. Show that $\mathbf{C}_p$ and $\mathbf{C}$ are isomorphic as fields.

6. Rudiments in p-adic analysis

6.1. **Generalities.** Let K be a closed subfield of $\mathbf{C}_p$ and $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n \in K[\![X]\!]$ be a formal power series. Let $x \in \mathbf{C}_p$. As $(\mathbf{C}_p, |.|)$ is complete and non archimedean, the series $\sum\limits_{n=0}^{\infty} a_n x^n$ converges in $\mathbf{C}_p$ if and only if $\lim\limits_{n\to\infty} a_n x^n = 0$: in that case, we denote $f(x)$ for the sum of this series. Just as in the archimedean case (*i.e.* in the case of formal power series with coefficients in the field $\mathbf{C}$ of complex numbers), the preceding condition only depends on $|x|$: this motivates the following definition.

Definition 6.1.1. The *radius of convergence* of f is

$$r(f) = \frac{1}{\limsup\limits_{n\in\mathbf{Z}_{>0}} |a_n|^{1/n}} \in \mathbf{R}_{\geqslant 0}\,.$$

Proposition 6.1.2. The series $\sum\limits_{n=0}^{\infty} a_n x^n$ converges if $|x| < r(f)$ and diverges if $|x| > r(f)$.

Proof. Put $r = r(f)$.
- Assume $|x| < r$: we can write $|x|_p = (1-\varepsilon)r$ with $\varepsilon \in]0,1[$, so $|a_n x^n| = \big(r\,|a_n|^{1/n}(1-\varepsilon)\big)^n$ for $n \in \mathbf{Z}_{>0}$. By definition of r, there exists $N \in \mathbf{Z}_{>0}$ such that $|a_n|^{1/n} < \frac{1}{r - r\varepsilon/2}$, whence $|a_n x^n| \leqslant \big(\frac{1-\varepsilon}{1-\varepsilon/2}\big)^n$ for all $n \geqslant N$, implying that $\lim\limits_{n\to\infty} |a_n x^n| = 0$.
- Assume $|x| > r$: we can write $|x| = (1+\varepsilon)r$ with $\varepsilon \in]0,1[$. We can find a strictly increasing map $\varphi\colon \mathbf{Z}_{>0} \to \mathbf{Z}_{>0}$ such that $\lim\limits_{n\to\infty} \big|a_{\varphi(n)}\big|^{1/\varphi(n)} = \frac{1}{r}$: there exists $N \in \mathbf{Z}_{>0}$ such that $\big|a_{\varphi(n)}\big|^{1/\varphi(n)} > \frac{1}{r+r\varepsilon/2}$, whence $\big|a_{\varphi(n)} x^{\varphi(n)}\big| \geqslant \big(\frac{1+\varepsilon}{1+\varepsilon/2}\big)^n$ for all $n \geqslant N$, implying that $\lim\limits_{n\to\infty} \big|a_{\varphi(n)} x^{\varphi(n)}\big| = +\infty$, so that the series $\sum\limits_{n=0}^{\infty} a_n x^n$ diverges. □

Notation. If $a \in \mathbf{C}_p$ and $r \in \mathbf{R}_{\geqslant 0}$, we put $\mathrm{D}(a,r) = \{x \in \mathbf{C}_p\,;\, |x-a| < r\}$ (the "open disc" with center a and radius r) and $\overline{\mathrm{D}}(a,r) = \{x \in \mathbf{C}_p\,;\, |x-a| \leqslant r\}$ (the "closed disc" with center a and radius r).

Remark 6.1.3. In contrast with discs in the complex plane $\mathbf{C}$, both $\mathrm{D}(a,r)$ and $\overline{\mathrm{D}}(a,r)$ are open and closed in the topological space $(\mathbf{C}_p, |.|)$.

Corollary 6.1.4. A formal power series $f(X) \in K[\![X]\!]$ defines a continuous map $f\colon \mathrm{D}(0,r(f)) \to \mathbf{C}_p$.

Proof. We may assume $r(f) > 0$. Let $x_0 \in \mathrm{D}(0,r(f))\backslash\{0\}$, $\alpha \in]0,|x_0|\,[$ and $x \in \mathbf{C}_p$ such that $|x - x_0| < \alpha$: we have $|x| = |x_0|$, and we may evaluate f at x_0 and x. As $f(x) - f(x_0) = \sum\limits_{n=0}^{\infty} a_n(x^n - x_0^n)$, we have $|f(x) - f(x_0)| \leqslant \sup\limits_{n\in\mathbf{Z}_{>0}} |a_n|\,|x^n - x_0^n|$. As $x^n - x_0^n = (x-x_0)(x^{n-1} + x_0 x^{n-2} + \cdots + x_0^{n-1})$, we have $|x^n - x_0^n| \leqslant |x - x_0| \max\limits_{1\leqslant k\leqslant n} |x|^{n-k}\,|x_0|^{k-1} = \alpha\,|x_0|^{n-1}$ for all $n \in \mathbf{Z}_{>0}$. By definition of $r(f)$, the sequence $\big(\big|a_n x_0^{n-1}\big|\big)_{n\in\mathbf{Z}_{>0}}$ is bounded (it converges to 0): let $c(x_0) = 1 + \sup\limits_{n\in\mathbf{Z}_{>0}} \big|a_n x_0^{n-1}\big| \in \mathbf{R}_{\geqslant 1}$. We have $|f(x) - f(x_0)| \leqslant \frac{\alpha}{r} c(x_0)\alpha$: given $\varepsilon \in \mathbf{R}_{>0}$, put $\alpha = \min\big\{\frac{\varepsilon}{c(x_0)}, |x_0|\,\big\}$, so that $|x - x_0| < \alpha \Rightarrow |f(x) - f(x_0)| < \varepsilon$, showing the continuity of f at x_0.
Assume $x_0 = 0$ and choose $r \in]0, r(f)[$. As above, there exists $C_r \in \mathbf{R}_{>0}$ such that $|a_n|\,r^n \leqslant C_r$ for all $n \in \mathbf{Z}_{>0}$. If $x \in \mathrm{D}(0,r)$, we have $|f(x) - f(0)| \leqslant \sup\limits_{n\in\mathbf{Z}_{>0}} |a_n x^n|$: as $|a_n x^n| = |a_n|\,r^n\big(\frac{|x|}{r}\big)^n \leqslant C_r \frac{|x|}{r}$, we deduce that $|f(x) - f(0)| \leqslant \frac{C_r}{r}\,|x|$, showing the continuity of f at 0. □

Example 6.1.5. A formal power series with coefficients in $\mathcal{O}_K$ defines a continuous map $\mathrm{D}(0,1) \to \mathcal{O}_{\mathbf{C}_p}$.

Notation. Let $r \in \mathbf{R}_{>0}$.
(1) We denote by $\mathscr{H}_K([0,r[)$ (resp. $\mathscr{H}_K([0,r])$) the set of formal power series $f(X) \in K[\![X]\!]$ that converge on $\mathrm{D}(0,r)$ (resp. $\overline{\mathrm{D}}(0,r)$).
(2) If $r \in \mathbf{R}_{>0}$ and $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n \in K[\![X]\!]$, we put $|f|_r = \sup\limits_{n\in\mathbf{Z}_{\geqslant 0}} |a_n|\,r^n \in \mathbf{R}_{\geqslant 0} \cup \{+\infty\}$.

Lemma 6.1.6. Let $r \in \mathbf{R}_{>0}$ and $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n \in \mathscr{H}_K([0,r])$. Then $|f|_r = \max\limits_{n\in\mathbf{Z}_{\geqslant 0}} |a_n|\,r^n$.

Proof. This is trivial if $f(X) = 0$; if $f(X) \neq 0$, we have $\lim\limits_{n\to\infty} |a_n| r^n = 0$, so $E = \Big\{n \in \mathbf{Z}_{\geqslant 0}\,;\, |a_n| r^n > \frac{\|f\|_\rho}{2}\Big\}$ is finite, and $|f|_r = \max\limits_{n\in E} |a_n| r^n$. □

Definition 6.1.7. With the notations of lemma 6.1.6, assume $f \neq 0$. Put

$$\mathsf{w}_r(f) = \max\{n \in \mathbf{Z}_{\geqslant 0}\,;\, |a_n| r^n = |f|_r\}$$

(which makes sense since $\lim\limits_{n\to\infty} |a_n| r^n = 0$).

Proposition 6.1.8. (1) If $r \in \mathbf{R}_{>0}$, $\mathscr{H}_K([0,r]) \subset \mathscr{H}_K([0,r[)$ are subrings of $\mathbf{C}_p[\![X]\!]$, in particular they are integral domains.
(2) If $\rho \in [0,r[$ (resp. $\rho \in [0,r]$), the map $|.|_\rho$ defines an absolute value on $\mathscr{H}_K([0,r[)$ (resp. $\mathscr{H}_K([0,r])$).
(3) Elements in $\mathscr{H}_K([0,r])$ define bounded maps $\overline{\mathrm{D}}(0,r) \to \mathbf{C}_p$.

Proof. (2) We certainly have $|f|_\rho = 0 \Rightarrow f = 0$ and $|f+g|_\rho \leqslant \max\{|f|_\rho, |g|_\rho\}$ for all $f, g \in \mathscr{H}_K([0,r[)$. Write $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n$ and $g(X) = \sum\limits_{n=0}^{\infty} b_n X^n$. We have $(fg)(X) = \sum\limits_{n=0}^{\infty} c_n X^n$ with $c_n = \sum\limits_{i=0}^{n} a_i b_{n-i}$ for all $n \in \mathbf{Z}_{\geqslant 0}$: we have $|c_n| \rho^n \leqslant \max\limits_{0\leqslant i\leqslant n} |a_i| \rho^i |b_{n-i}| \rho^{n-i} \leqslant |f|_\rho |g|_\rho$. By lemma 6.1.6, the integers $i_0 = \min\{i \in \mathbf{Z}_{\geqslant 0}\,;\, |a_i| \rho^i = |f|_\rho\}$ and $j_0 = \min\{j \in \mathbf{Z}_{\geqslant 0}\,;\, |b_j| \rho^j = |g|_\rho\}$ are well defined. If $i, j \in \mathbf{Z}_{\geqslant 0}$ are such that $i + j = i_0 + j_0$ and $(i,j) \neq (i_0, j_0)$, we have $|a_i| \rho^i |b_j| \rho^j < |a_{i_0}| \rho^{i_0} |b_{j_0}| \rho^{j_0}$, hence $|a_i b_j| < |a_{i_0} b_{j_0}|$, so that $|fg|_\rho \geqslant |c_{i_0+j_0}| \rho^{i_0+j_0} = |a_{i_0}| \rho^{i_0} |b_{j_0}| \rho^{j_0} = |f|_\rho |g|_\rho$.

(3) If $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n$ belongs to $\mathscr{H}_K([0,r])$ and $x \in \overline{\mathrm{D}}(0,r)$, the series $f(x) := \sum\limits_{n=0}^{\infty} a_n x^n$ converges absolutely, and $|f(x)| \leqslant \sup\limits_{n\in\mathbf{Z}_{\geqslant 0}} |a_n| |x|^n \leqslant |f|_{|x|} \leqslant \|f\|_r$. □

Remark 6.1.9. (1) The restriction of $|.|_1$ to $K[X]$ is nothing but the Gauss absolute value (*cf* definition 3.5.2). In what follows, we denote it by $|.|_{\text{Gauss}}$ or simply $|.|$.
(2) Assume $r \in |K^\times|$: let $\alpha \in K$ be such that $|\alpha| = r$. The map $\phi_\alpha\colon K[\![X]\!] \to K[\![X]\!]$; $f(X) \mapsto f(\alpha X)$ induces an isometry

$$(\mathscr{H}_K([0,r]), |.|_r) \tilde{\to} (\mathscr{H}_K([0,r]), |.|_{\text{Gauss}}).$$

This allows to reduce some questions on $\mathscr{H}_K([0,r])$ to the case $r = 1$.

Lemma 6.1.10. If $r \in \mathbf{R}_{>0}$, the normed vector space $(\mathscr{H}_K([0,r]), |.|_r)$ is Banach.

Proof. Let $(f_k)_{k\in\mathbf{Z}_{\geqslant 0}}$ be a Cauchy sequence in $(\mathscr{H}_K([0,r]), |.|_r)$. For all $k \in \mathbf{Z}_{\geqslant 0}$, write $f_k(X) = \sum\limits_{n=0}^{\infty} a_{k,n} X^n$. For all $n, k_1, k_2 \in \mathbf{Z}_{\geqslant 0}$, we have $|a_{k_2,n} - a_{k_1,n}| r^n \leqslant |f_{k_2} - f_{k_1}|_r$ so that $(a_{k,n})_{k\in\mathbf{Z}_{\geqslant 0}}$ is a Cauchy sequence in $(K, |.|)$. As the latter is complete (because K is closed in $\mathbf{C}_p$), it converges to limit $a_n \in K$. Let $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n \in K[\![X]\!]$.
Let $\varepsilon \in \mathbf{R}_{>0}$: there exists $C \in \mathbf{Z}_{\geqslant 0}$ such that $k, k' \geqslant C \Rightarrow |f_{k'} - f_k|_r \leqslant \varepsilon$. For all $n \in \mathbf{Z}_{\geqslant 0}$, we have thus $|a_{k',n} - a_{k,n}| r^n \leqslant \varepsilon$: passing to the limit, we have $|a_n - a_{k,n}| r^n \leqslant \varepsilon$ for all $n \in \mathbf{Z}_{\geqslant 0}$, showing that $|f - f_k| \leqslant \varepsilon$. This implies in particular that $|f|_r \leqslant \varepsilon + |f_k|_r < +\infty$ for all $k \geqslant C$, hence $f \in \mathscr{H}_K([0,r])$, and that $(f_k)_{k\in\mathbf{Z}_{\geqslant 0}}$ converges to f for $|.|_r$. □

6.2. **The Weierstrass preparation theorem.** The reference for this part is [4, §5.2]. Again, K denotes a closed subfield of $\mathbf{C}_p$. Let $r \in \mathbf{R}_{>0}$.

Theorem 6.2.1. (Weierstrass division theorem). Let $f, g \in \mathscr{H}_K([0,r])$ be such that $g \neq 0$. There exist uniquely determined elements $q \in \mathscr{H}_K([0,r])$ and $h \in K[X]$ such that

$$(*)\qquad \begin{cases} \deg(h) < \mathsf{w}_r(g) \\ f = qg + h \end{cases}$$

Moreover, we have $|f|_r = \max\{|q|_r |g|_r, |h|_r\}$.

Proof. • Assume $r \in |K^\times|$, the isometry $\phi\colon (\mathscr{H}_K([0,r]), |.|_r) \tilde{\to} (\mathscr{H}_K([0,r]), |.|_{\text{Gauss}})$ allows to reduce to the case where $r = 1$ (*cf* remark 6.1.9). Note that $\mathsf{w}_r(g) = \mathsf{w}_1(\phi(g)) =: \mathsf{w}(g)$. There exists $\lambda \in K^\times$ such that $|g| = |\lambda|$: we may divide by λ to reduce to the case where $|g| = 1$, so that $g \in \mathcal{O}_K[\![X]\!]$.
We first show that conditions $(*)$ imply the estimate $|f| = \max\{|q|, |h|\}$. If $q \neq 0$ or $h \neq 0$, there exists $\mu \in K^\times$ such that $\max\{|\mu q|, |\mu h|\} = 1$. This implies in particular that $\mu f = \mu q g + \mu h \in \mathcal{O}_K[\![X]\!]$, whence[43]

[43] Here we denote with a bar the image of an element of $\mathcal{O}_K[\![X]\!]$ in $\kappa_K[\![X]\!]$.

$\overline{\mu f}=\overline{\mu q}\,\overline{g}+\overline{\mu h}$ in $\kappa_K[X]$: this is the euclidean division of $\overline{\mu f}$ by $\overline{g}$. As $\overline{\mu q}\neq 0$ or $\overline{\mu h}\neq 0$, we have $\overline{\mu f}\neq 0$, hence $|\mu f|=1$, so that $|\mu f|=\max\{|\mu q|,|\mu h|\}$ *i.e.* $|f|=\max\{|q|,|h|\}$. This holds obviously true when $q=0$ and $h=0$.
In particular, if $qg+h=0$ with $q\in\mathscr{H}_K([0,1])$ and $h\in K[X]$ of degree $<\mathsf{w}(g)$, this implies that $q=0$ and $h=0$, so that the map

$$\begin{aligned}\psi\colon \mathscr{H}_K([0,1])\times K[X]_{<\mathsf{w}(g)} &\to \mathscr{H}_K([0,1])\\ (q,h)&\mapsto qg+h\end{aligned}$$

is injective, and an isometry (where the LHS is equipped with the max of the absolutes values). The estimate proved above and the fact that $\mathscr{H}_K([0,1])$ and $K[X]_{<\mathsf{w}(g)}$ are Banach spaces (*cf* lemma 6.1.10) imply that the image of ψ is closed in $\mathscr{H}_K([0,1])$: as we want to prove that ψ is surjective, it is enough to check that this image is dense in $\mathscr{H}_K([0,1])$.
Write $g(X)=\sum\limits_{n=0}^{\infty}b_nX^n$. As $\lim\limits_{n\to\infty}|b_n|=0$ and $|b_n|<1$ for all $n>\mathsf{w}(g)$, there exists $\varepsilon\in[0,1[$ such that $|b_n|<\varepsilon$ for all $n>\mathsf{w}(g)$. Put $\mathfrak{m}_{K,\varepsilon}=\{x\in K\,;\,|x|\leqslant\varepsilon\}$, $\mathcal{O}_{K,\varepsilon}=\mathcal{O}_K/\mathfrak{m}_{K,\varepsilon}$ and $\pi_\varepsilon\colon\mathcal{O}_K[\![X]\!]\to\mathcal{O}_{K,\varepsilon}[\![X]\!]$ the canonical map. Then $\pi_\varepsilon(g)$ is a polynomial of degree $\mathsf{w}(g)$, whose dominant coefficient is invertible, so we can perform Euclidean divisions by $\pi_\varepsilon(g)$ in $\mathcal{O}_{K,\varepsilon}[X]$. Let $f\in\mathscr{H}_K([0,1])\backslash\{0\}$: there exists $\mu\in K^\times$ such that $|\mu f|=1$. There exist $q_0,h_0\in\mathcal{O}_K[X]$ such that $\deg(h_0)<\mathsf{w}(g)$ and $\pi_\varepsilon(\mu f)=\pi_\varepsilon(q_0)\pi_\varepsilon(g)+\pi_\varepsilon(h_0)$ is the Euclidean division of $\pi_\varepsilon(\mu f)$ by $\pi_\varepsilon(g)$. Then we have $|\mu f-q_0g-h_0|\leqslant\varepsilon$, *i.e.* $|f-\psi(q,h)|\leqslant\frac{\varepsilon}{|\mu|}=\varepsilon\,|f|$, where $q=\frac{q_0}{\mu}$ and $h=\frac{h_0}{\mu}$. This implies the density of the image of ψ, hence the result.
• The general case. By unicity of (g,h), we may use theorem 5.3.9 to reduce to the case where $K=\mathbf{C}_p$. Then $|K^\times|$ is dense in $\mathbf{R}_{>0}$. We can thus find a sequence $(r_i)_{i\in\mathbf{Z}_{\geqslant0}}$ is $\mathbf{R}_{>0}$ that converges to r from below. Then we have $|f|_r=\lim\limits_{i\to\infty}|f|_{r_i}$. Moreover, there are sequences $(q_i)_{i\in\mathbf{Z}_{\geqslant0}}$ and $(h_i)_{i\in\mathbf{Z}_{\geqslant0}}$ such that $q_i\in\mathscr{H}_K([0,r_i])$, $h_i\in K[X]_{<\mathsf{w}(g)}$ and $f=q_ig+h_i$ for all $i\in\mathbf{Z}_{\geqslant0}$. By unicity, we have $q_i=q_j$ and $h_i=h_j$ in $K[\![X]\!]$ whenever $i<j$, so that $q:=q_i$ and $h:=h_i$ does not depend of $i\in\mathbf{Z}_{\geqslant0}$. Moreover, we have $|f|_{r_i}=\max\{|q|_{r_i}|g|_{r_i},|h|_{r_i}\}$: passing to the limit on i gives $|f|_r=\max\{|q|_r\,|g|_r\,,|h|_r\}$, which implies in particular that $q\in\mathscr{H}_K([0,r])$ (because $|q|_r<+\infty$). □

Theorem 6.2.2. (Weierstrass preparation theorem). Let $f\in\mathscr{H}_K([0,r])\backslash\{0\}$. There exist uniquely determined $P\in K[X]$ and $u\in\mathscr{H}_K([0,r])^\times$ such that

$$\begin{cases}P\text{ is monic of degree }\mathsf{w}(f)\\ f=Pu.\end{cases}$$

Moreover, we have $|P|_r=r^{\mathsf{w}_r(f)}$.

Proof. • Again, assume first that $r\in|K^\times|$: the isometry $\phi\colon(\mathscr{H}_K([0,r]),|.|_r)\xrightarrow{\sim}(\mathscr{H}_K([0,r]),|.|_{\text{Gauss}})$ allows to reduce to the case where $r=1$ (*cf* remark 6.1.9). Indeed, if the case $r=1$ is known, let $\alpha\in K^\times$ be such that $|\alpha|=r$: we have $f(\alpha X)\in\mathscr{H}_K([0,1])$, so we have $f(\alpha X)=P_0(X)u_0(X)$ with $P_0\in K[X]$ monic of degree $d:=\mathsf{w}(f(\alpha X))=\mathsf{w}(f)$ and $u_0\in\mathscr{H}_K([0,1])^\times$ uniquely determined; then $f(X)=P(X)u(x)$ with $P(X)=\alpha^dP_0(\alpha^{-1}X)\in K[X]$ monic of degree d and $u(X)=\alpha^{-d}u_0(\alpha^{-1}X)\in\mathscr{H}_K([0,r])^\times$. Also, $|P_0|=1$ implies that $|P|_r=r^d$.
We prove the existence first. Rescaling by an element in $K^\times$, we may assume that $|f|=1$. Put $d=\mathsf{w}(f)$: by the Weierstrass division theorem, there exist uniquely determined $q\in\mathscr{H}_K([0,1])$ and $h\in K[X]$ such that $\deg(h)<d$ and $X^d=qf+h$. Put $P=X^d-h\in K[X]$: as $\deg(h)<d$, this is a monic polynomial of degree $d=\mathsf{w}(f)$, and $P=qf$. We also have $1=|f|=\max\{|q|\,|f|\,,|h|\}$, hence $|h|\leqslant1$: as $\deg(h)<d$, we have $|P|=\max\{\left|X^d\right|,|h|\}=1$, and $\mathsf{w}(P)=d$. As $P=qf$, this implies that $|q|=1$. We have to check that q is a unit in $\mathscr{H}_K([0,1])$. Reducing modulo $\mathfrak{m}_K$ gives $\overline{P}=\overline{q}\overline{f}$ in $\kappa_K[\![X]\!]$. As $\mathsf{w}(f)=\mathsf{w}(P)=d$, the elements $\overline{P}$ and $\overline{f}$ are both polynomials of degree d. This implies that $\overline{q}\in\kappa_K^\times$, so that $|q-q(0)|<1$ *i.e.* $\left|\frac{q}{q(0)}-1\right|<1$: the series $s=\sum\limits_{n=0}^{\infty}\left(1-\frac{q}{q(0)}\right)^n$ converges in the Banach space $(\mathscr{H}_K([0,1]),|.|)$ (lemma 6.1.10), and $\frac{q}{q(0)}s=1$. This shows that $u:=q(0)s\in\mathscr{H}_K([0,1])^\times$, and that $uq=1$. In particular, we have $f=Pu$: this proves the existence.
The unicity follows from the unicity in Weierstrass division theorem, since $X^d=u^{-1}f+(X^d-P)$ has to be Weierstrass division of X^d by f, which we know to be unique.
• The general case follows as in the end of the proof of theorem 6.2.1 □

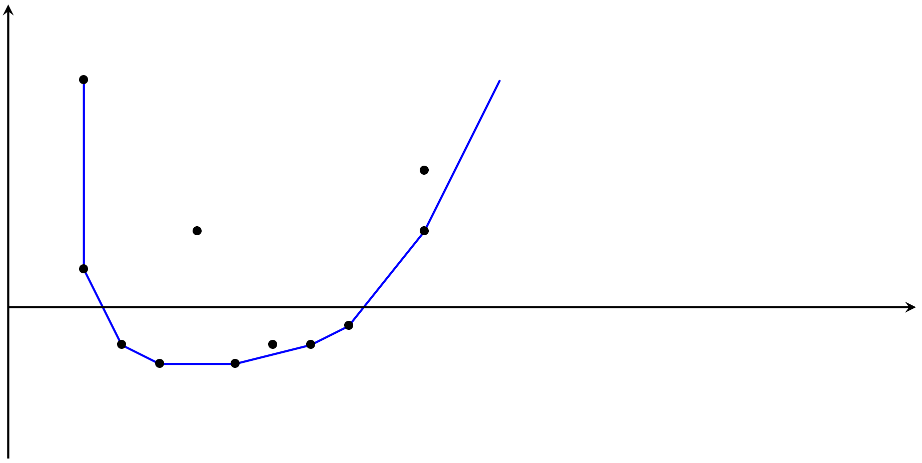
Corollary 6.2.3. A element in $\mathscr{H}_K([0,r])$ has only finitely many zeros, and these are algebraic over K.

Corollary 6.2.4. $\mathscr{H}_K([0,r])$ is a PID.

6.3. **Newton polygon and applications.** A reference for this part is [8, Chapter I §§6-7, Chapter II §§2-3]. Endow $\mathbf{C}_p$ with the p-adic valuation $v\colon \mathbf{C}_p \to \mathbf{Q} \cup \{+\infty\}$ normalized by $v(p) = 1$. Let K be a closed subfield of $\mathbf{C}_p$.

Definition 6.3.1. Let $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n \in K[\![X]\!]$.

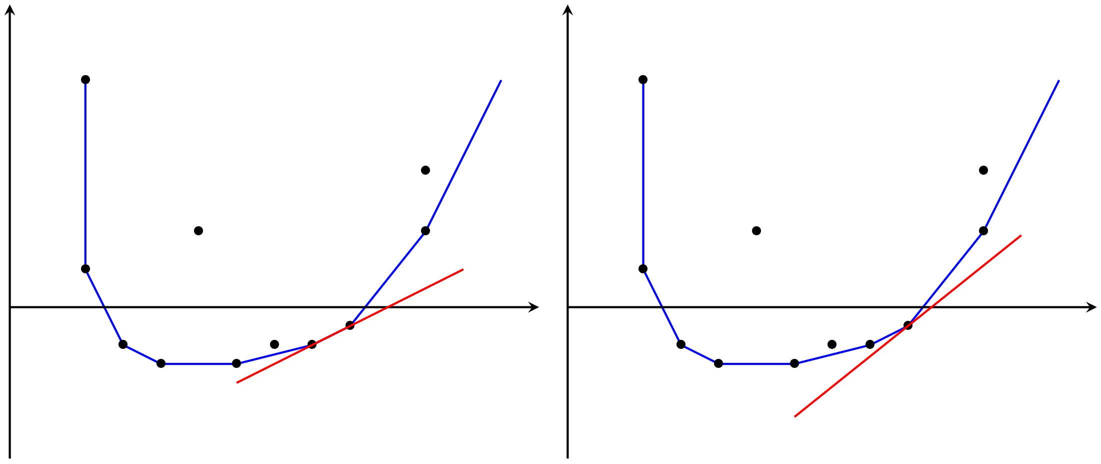
- The *Newton polygon* $\mathsf{NP}(f)$ of f is the convex hull of the set of points $\{(n, v(a_n))\}_{n\in\mathbf{N}} \cup \{(0, +\infty)\}$ in the plane. It is thus a union of segments of increasing slopes and possibly one or two half-lines.
- The *length* of a segment is the length of its projection onto the x-axis (this is an integer), that of a half-line is that of the longest piece between to points of the form $(n, v(a_n))$.
- The *breaks* are those $i \in \mathbf{Z}_{\geqslant 0}$ such that the point $(i, v(a_i))$ is a vertex of the polygon.
- f is said *pure* of slope λ if is has only one finite slope, equal to λ.



Remark 6.3.2. In general, there might be infinitely many slopes, but of course there are finitely many when $f \in K[X]$.

Definition 6.3.3. Let $\lambda \in \mathbf{R}$. The *line support* of slope λ for $\mathsf{NP}(f)$ is the line of equation $y = \lambda x + c_\lambda$ with $c_\lambda \in \mathbf{R}$ maximal such that $\mathsf{NP}(f)$ lies above it.

Remark 6.3.4. (1) Let $\lambda \in \mathbf{R}$ be such that $\mathsf{NP}(f)$ has a line support of slope λ. If $z \in \mathbf{C}_p$ is such that $v(z) \geqslant -\lambda$ (*i.e.* $|z| \leqslant p^\lambda$), we have $v(a_n z^n) \geqslant n(v(z) + \lambda) + c_\lambda$ *i.e.* $|a_n z^n| \leqslant \left(\frac{|z|}{p^\lambda}\right)^n p^{-c_\lambda}$: this implies that f converges on $\mathrm{D}(0, p^\lambda)$, and that if f converges at z, then $|f(z)| \leqslant p^{-c_\lambda}$.
(2) Let λ_∞ be the supremum of the slopes of $\mathsf{NP}(f)$. The line support of slope λ exists if and only if $\lambda \leqslant \lambda_\infty$, and what precedes imply that $r(f) = p^{\lambda_\infty}$.
(3) Assume $\mathsf{NP}(f)$ has a line support of slope λ. There are two cases: if λ is a slope of $\mathsf{NP}(f)$, then the line support contains the segment of slope λ of $\mathsf{NP}(f)$. If not, there exists exactly one $n \in \mathbf{Z}_{\geqslant 0}$ such that $v(a_n) = \lambda n + c_\lambda$.



Theorem 6.3.5. Let $P \in K[X]$ and $\lambda \in \mathbf{R}$.
(1) $P_\lambda(X) := \prod\limits_{\substack{\alpha\in\overline{K}\\ v(\alpha)=-\lambda\\ P(\alpha)=0}} (X - \alpha) \in K[X]$.

(2) The number (counting multiplicities) of roots x of P (in $\overline{K}$) such that $v(x)=-\lambda$ is equal to the length of the side of $\mathsf{NP}(P)$ of slope λ (so it is 0 if there is no such side).
(3) If $\mathsf{NP}(P)$ has more than one finite slope, then P is reducible in $K[X]$.
(4) Assume that v is discrete on K, that P is monic and that $\mathsf{NP}(P)$ has only one side of finite slope $-\frac{m}{n}$ where $\mathsf{gcd}(m,n)=1$. Then P is irreducible in $K[x]$.

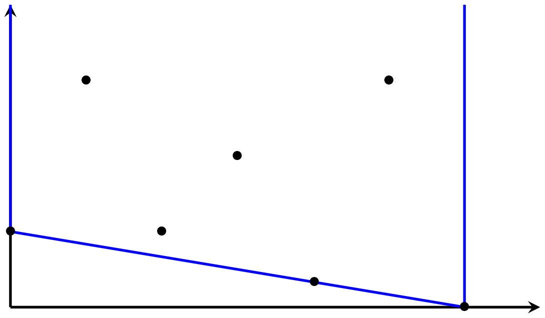
Proof. (1) Let $\alpha_1,\dots,\alpha_n\in\overline{K}$ be the roots of P (counted with multiplicities). Put $L=K(\alpha_1,\dots,\alpha_n)$. If L/K is separable (which is automatic if $\mathsf{char}(K)=0$), it is Galois. The set $\{\alpha\in\overline{K}\,;\,P(\alpha)=0,\ v(\alpha)=-\lambda\}$ is stable under the action of $\mathsf{Gal}(L/K)$ (because $v\circ\sigma=v$ for all $\sigma\in\mathsf{Gal}(L/K)$ since K is complete), which proves that $P_\lambda\in K[X]$. Assume that $\mathsf{char}(K)=p>0$. If P is irreducible, we can write $P(X)=Q(X^{p^e})$ where $e\in\mathbf{Z}_{\geqslant 0}$ and $Q\in K[X]$ is irreducible and separable. All roots of Q have the same valuation: all roots of P have the same valuation. In general, write $P=\prod\limits_{i=1}^{r}P_i$ with $P_1,\dots,P_r$ irreducible: for each $i\in\{1,\dots,r\}$, the roots of P_i all have the same valuation v_i, and $P_\lambda=\prod\limits_{\substack{1\leqslant i\leqslant r\\ v_i=-\lambda}}P_i\in K[X]$.
(2) As multiplying P by a non zero constant (resp. by X) translates $\mathsf{NP}(P)$ vertically (resp. horizontally), we may divide P by its monomial of lower degree and assume that $a_0=1$. The roots $\alpha_1,\dots,\alpha_n\in\overline{K}$ of P are nonzero: put $\beta_i=-\alpha_i^{-1}$ for $i\in\{1,\dots,n\}$. We have $P(X)=\prod\limits_{i=1}^{n}(1+\beta_iX)$. Renumbering if necessary, we may assume that $v(\beta_1)\leqslant\cdots\leqslant v(\beta_n)$. Write $\{v(\beta_1),\dots,v(\beta_n)\}=\{\nu_1,\dots,\nu_r\}$ with $\nu_1<\cdots<\nu_r$, and for $j\in\{1,\dots,r\}$, let n_j be the number of indices $i\in\{1,\dots,n\}$ such that $v(\beta_i)=\nu_j$ (so we have $\sum\limits_{j=1}^{r}n_j=n$). We have to prove that $\mathsf{NP}(P)$ has r non vertical sides, $[M_0M_1],\dots,[M_{r-1}M_r]$ with $M_0=(0,0)$, $M_1=(n_1,n_1\nu_1)$, $M_2=(n_1+n_2,n_1\nu_1+n_2\nu_2),\dots,M_j=\Big(\sum\limits_{k=1}^{j}n_k,\sum\limits_{k=1}^{j}n_k\nu_k\Big),\dots$. This is equivalent to

$$(*)\qquad\begin{cases} v(a_{n_1+\cdots+n_j})=\sum\limits_{k=1}^{j}n_k\nu_k & \text{for } j\in\{1,\dots,r\}\\ v(a_i)\geqslant\sum\limits_{k=1}^{j}n_k\nu_k+(i-n_1-\cdots-n_j)\nu_{j+1} & \text{if } n_1+\cdots+n_j<i<n_1+\cdots+n_{j+1}\end{cases}$$

(the last condition means that the points $(i,v(a_i))$ lie above the segment $[M_jM_{j+1}]$). We have

$$a_i=\sum_{1\leqslant k_1\leqslant\cdots\leqslant k_i\leqslant n}\beta_{k_1}\cdots\beta_{k_i}$$

so that $v(a_i)\geqslant\min\limits_{1\leqslant k_1\leqslant\cdots\leqslant k_i\leqslant n}v(\beta_{k_1})+\cdots+v(\beta_{k_i})\geqslant v(\beta_1)+\cdots+v(\beta_i)$ which implies the second condition in $(*)$. For the first condition, just observe that if $i=\sum\limits_{k=1}^{j}n_k$ for some $j\in\{1,\dots,r\}$, then we have $v(\beta_{k_1})+\cdots+v(\beta_{k_i})>v(\beta_1)+\cdots+v(\beta_i)$ whenever the sequence $(k_1,\dots,k_i)$ is different from $(1,2,\dots,i)$, so that $v(a_i)=v(\beta_1)+\cdots+v(\beta_i)=\sum\limits_{k=1}^{j}n_k$ in that case.
(3) The number of finite slopes in $\mathsf{NP}(P)$ is equal to the number of non trivial factors in $P=\prod\limits_{\lambda\in\mathbf{R}}P_\lambda$.
(4) There are n roots of valuation $\frac{m}{n}$, let α be any one of these. As $\mathsf{gcd}(m,n)=1$, we have $v(K(\alpha))\supset\frac{1}{n}v(K)$, so that the ramification index e of the extension $K(\alpha)/K$ satisfies $n\mid e$. As $[K(\alpha):K]\leqslant n$, we have $[K(\alpha):K]=n=\deg(P)$, so that P is irreducible.



□

Remark 6.3.6. One recovers Eisenstein's irreducibility criterion as the special case $m = 1$ in (4).

Theorem 6.3.7. Assume $f \in \mathscr{H}_K([0,r])$ (resp. $f \in \mathscr{H}_K([0,r[)$) where $r \in \mathbf{R}_{>0}$, and let $\lambda \in [-\infty, 0, \ln_p(r)]$ (resp. $\lambda \in [-\infty, \ln_p(r)[$).
(1) The number of zeros of f in $\overline{\mathrm{D}}(0,r)$ (resp. in $\mathrm{D}(0,r)$) with valuation $-\lambda$ is equal to the length of the segment of $\mathsf{NP}(f)$ of slope λ.
(2) If $\lambda \notin \{+\infty\}$ is such a slope, there exists a unique monic polynomial $P_\lambda \in K[X]$ and such that $f(X) = P_\lambda(X)g(X)$ where $g \in \mathscr{H}_K([0,r])$ (resp. $g \in \mathscr{H}_K([0,r[)$) is such that $\mathsf{NP}(g)$ is $\mathsf{NP}(f)$ without its piece of slope λ.

Proof. Write $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n$. We may of course assume that $f \neq 0$.
(1) This is obvious if $r = -\infty$ (the length of the corresponding half-line is precisely the multiplicity of 0 as a root of f: assume henceforth that $\lambda \in \mathbf{R}$.
• Assume first that λ *is not* a slope of $\mathsf{NP}(f)$: by remark 6.3.4 (3), there exists exactly one $N \in \mathbf{Z}_{\geqslant 0}$ such that $v(a_n) = \lambda n + c_\lambda$. If $\alpha \in \mathbf{C}_p$ is such that $v(\alpha) = -\lambda$, we thus have $|a_n\alpha^n| \leqslant p^{-c_\lambda}$, with equality if and only if $n = N$. the strong triangle inequality thus implies that $|f(\alpha)| = p^{-c_\lambda}$ so that $f(\alpha) \neq 0$, and f has no zero of valuation $-\lambda$.
• Assume that λ *is* a slope of $\mathsf{NP}(f)$: put $\rho = p^\lambda \leqslant r$ (resp. $< r$) and $d = \mathsf{w}_\rho(f)$. By Weierstrass preparation theorem (*cf* theorem 6.2.2), there exists a unique monic polynomial $P_\lambda \in K[X]$ such that $\deg(P_\lambda) = \mathsf{w}_\rho(P_\lambda) = d$ and $u_\lambda \in \mathscr{H}_K([0,\rho])^\times$ such that $f = P_\lambda u_\lambda$. Dividing f and u_λ by $a_{\mathsf{w}_\lambda(f)}$, we may assume that $a_{\mathsf{w}_\lambda(f)} = 1$, so that $|f|_\rho = \rho^d = |P_\lambda|_\rho$. This implies that $|u_\lambda|_\rho = 1$. If we write $u_\lambda = \sum\limits_{n=0}^{\infty} u_{\lambda,n}X^n$, this implies that $|u_{\lambda,n}| \leqslant \rho^{-n}$, for all $n \in \mathbf{Z}_{\geqslant 0}$.
Write $P_\lambda(X) = \sum\limits_{i=0}^{d} \alpha_i X^i$ (so that $\alpha_d = 1$ since P_λ is monic). As $|P_\lambda|_\rho = \rho^d$ (*cf* theorem 6.2.2), we have $|\alpha_i|\rho^i \leqslant \rho^d$, *i.e.* $v(\alpha_i) \geqslant \lambda(i-d)$, which means that $\mathsf{NP}(P_\lambda)$ lies above the line of equation $y = \lambda(x-d)$. In fact, this line is the support line of $\mathsf{NP}(P_\lambda)$ of slope λ because the point $(d,0)$ belongs to $\mathsf{NP}(P_\lambda)$, since P_λ is monic of degree d.
Let $\delta < d$ be the integer such that $(\delta, v(a_\delta))$ and $(d,0)$ are the endpoints of the segment of slope λ in $\mathsf{NP}(f)$. The length of the slope λ in $\mathsf{NP}(f)$ is thus $d-\delta$, and $v(a_\delta) = \lambda(\delta - d)$, *i.e.* $|a_\delta| = \rho^{d-\delta}$. Now the equality $f = P_\lambda u_\lambda$ implies that

$$a_\delta = \sum_{i=0}^{\delta} \alpha_i u_{\lambda,\delta-i}$$

so the strong triangle inequality implies that there exists $i \in \{0,\ldots,\delta\}$ such that $|a_\delta| \leqslant |\alpha_i u_{\lambda,d-i}|$, *i.e.* $\rho^{d-\delta} \leqslant |\alpha_i|\rho^{i-\delta}$, hence $\rho^{d-i} \leqslant |\alpha_i|$, *i.e.* $v(\alpha_i) \leqslant \lambda(i-d)$. As $v(\alpha_i) \geqslant \lambda(i-d)$ by what precedes, we have $v(\alpha_i) = \lambda(i-d)$, which means that the point $(i, v(\alpha_i))$ belongs to the support line of $\mathsf{NP}(P_\lambda)$ of slope λ. This implies in particular that the length of the slope λ in $\mathsf{NP}(P_\lambda)$ is $\geqslant d-i \geqslant d-\delta$. In particular, P_λ hence f has at least $d-\delta$ roots of valuation $-\lambda$ (*cf* theorem 6.3.5).
As $u_\lambda \in \mathscr{H}_K([0,\lambda])^\times$, the series u_λ has no zero in $\overline{\mathrm{D}}(0,\rho)$: the zeros of f in $\overline{\mathrm{D}}(0,\rho)$ are precisely those of P_λ, in particular there are exactly $\mathsf{w}_\rho(f)$ such zeros (counting multiplicities). Let $\lambda_1 < \cdots < \lambda_r$ be the slopes $\leqslant \lambda$ in $\mathsf{NP}(f)$, and for $i \in \{1,\ldots,r\}$, let ℓ_i be the length of the slope λ_i. Then f has $\deg(P_\lambda) = \mathsf{w}_\rho(f) = \ell_1 + \cdots + \ell_r$ zeros in $\overline{\mathrm{D}}(0,\rho)$. Replacing λ by λ_i in what precedes, we know that P_λ has at least hence exactly ℓ_i zeros of valuation $-\lambda_i$.
• This proves (1), and also that $\mathsf{NP}(P_\lambda)$ is $\mathsf{NP}(f)$ with the slopes $> \lambda$ removed. For (2), the existence was already proved, and the unicity follows from that in Weierstrass preparation theorem (*cf* theorem 6.2.2). The statement on $\mathsf{NP}(g)$ follows from the fact that its slopes are exactly those of $\mathsf{NP}(f)$ that are $> \lambda$ (since its zeros are those of f of valuation $> -\lambda$). □

Remark 6.3.8. One can recover corollary 6.2.3 from theorem 6.3.7.

6.4. Exponential and logarithm.

Notation. If $n = a_0 + a_1 p + \cdots + a_r p^r$ (with $a_i \in \{0,\ldots,p-1\}$ for all $i \in \{0,\ldots,r\}$ and $a_r \neq 0$) is the writing of $n \in \mathbf{Z}_{\geqslant 0}$ is base p, put $s(n) = a_0 + \cdots + a_r$ (sum of the digits of the p-adic writing of n).

Lemma 6.4.1. If $n \in \mathbf{Z}_{\geqslant 0}$, we have $v_p(n!) = \frac{n-s(n)}{p-1}$ (where v_p denotes the valuation on $\mathbf{C}_p$ normalized by $v_p(p) = 1$).

Proof. Let $k \in \mathbf{Z}_{>0}$. The number of integers less than n and that are divisible by p^k is equal to $N_k = \lfloor \frac{n}{p^k} \rfloor$ *i.e.* $N_k = a_k + a_{k+1}p + \cdots + a_r p^{r-k}$ if $k \leqslant r$ and 0 if $k > r$. The number of integers less than n and whose

p-adic valuation is equal to k is $N_k - N_{k+1}$. This implies that

$$\begin{aligned} v_p(n!) = \sum_{k=1}^{\infty} k(N_k - N_{k+1}) = \sum_{k=1}^{\infty} kN_k - \sum_{k=2}^{\infty}(k-1)N_k = \sum_{k=1}^{r} N_k &= \sum_{k=1}^{r} \big(a_k + a_{k+1}p + \cdots + a_r p^{r-k}\big) \\ &= \sum_{i=0}^{r} a_i(1 + p + \cdots + p^{i-1}) \\ &= \sum_{i=0}^{r} a_i \tfrac{p^i-1}{p-1} = \tfrac{n-s(n)}{p-1}. \end{aligned}$$

□

Definition 6.4.2. The *logarithm* and *exponential* series are

$$\ln(1+X) = \sum_{n=0}^{\infty} \tfrac{(-1)^{n-1}}{n} X^n \quad \text{and} \quad \exp(X) = \sum_{n=0}^{\infty} \tfrac{X^n}{n!}$$

respectively.

Lemma 6.4.3. We have equalities of formal power series $\ln(\exp(X)) = X$, $\exp(\ln(1+X)) = 1+X$ in $\mathbf{Q}[\![X]\!]$, and $\ln((1+X)(1+Y)) = \ln(1+X) + \ln(1+Y)$, $\exp(X+Y) = \exp(X)\exp(Y)$ in $\mathbf{Q}[\![X,Y]\!]$.

Proof. • Note that the derivative of $\ln(1+X)$ and $\exp(X)$ are $\sum\limits_{m=0}^{\infty}(-X)^m = \frac{1}{1+X}$ and $\exp(X)$ respectively. Put $f(X) = \ln(\exp(X))$ and $g(X) = \exp(\ln(X))$: differentiating we get $f'(X) = 1$ and $g'(X) = \frac{g(X)}{1+X}$. This implies that $f(X) = X$ (hence the first equality), and $g''(X) = 0$, whence $g(X) = 1+X$ by identification.

Remark 6.4.4. We have $\ln(\exp(X)) = \lim\limits_{N\to\infty} \sum\limits_{n=1}^{N} \frac{(-1)^{n-1}}{n}(\exp(X)-1)^n$. As $\exp(X)^k = \exp(kX)$ (*cf* below), we have

$$\begin{aligned} \sum_{n=1}^{N} \tfrac{(-1)^{n-1}}{n}(\exp(X)-1)^n &= \sum_{n=1}^{N} \tfrac{(-1)^{n-1}}{n} \sum_{k=0}^{n} \tbinom{n}{k}(-1)^{n-k}\exp(kX) \\ &= \sum_{n=1}^{N}\sum_{k=0}^{n}\sum_{m=0}^{\infty} \tfrac{(-1)^{k-1}}{n}\tbinom{n}{k}\tfrac{(kX)^m}{m!} \\ &= \sum_{m=0}^{\infty} \tfrac{a_m(N)}{m!} X^m \end{aligned}$$

with $a_m(N) = -\sum\limits_{n=1}^{N} \frac{\alpha_{n,m}}{n}$ where $\alpha_{n,m} := \sum\limits_{k=0}^{n}(-1)^k\binom{n}{k}k^m$.
If $n, m \in \mathbf{Z}_{\geqslant 0}$ and $P_n(X) = (1-X)^n = \sum\limits_{k=0}^{n}(-1)^k\binom{n}{k}X^k$, we have $P_n^{(m)}(X) = \sum\limits_{k=m}^{n}(-1)^k\binom{n}{k}D_m(k)X^{k-m}$ with $D_m(T) = T(T-1)\cdots(T-m+1)$.
If $m < n$, we have $\sum\limits_{k=m}^{n}(-1)^k\binom{n}{k}D_m(k) = P_m^{(m)}(1) = 0$. With $m=0$, this shows that $\alpha_{n,0} = \sum\limits_{k=0}^{n}(-1)^k\binom{n}{k} = 0$, and a straightforward induction implies that $\alpha_{n,m}$ (when $m<n$). This implies that $a_m(N) = a_m := -\sum\limits_{n=1}^{m}\frac{1}{n}\sum\limits_{k=0}^{n}(-1)^k\binom{n}{k}k^m$ whenever $N \geqslant m$, in particular $a_0 = 0$. Passing to the limit as $N \to +\infty$, we get $\ln(\exp(x)) = \sum\limits_{m=1}^{\infty}\frac{a_m}{m!}x^m$.
Assume $m > 0$: we have $-a_m = \sum\limits_{k=1}^{m}(-1)^k k^m \sum\limits_{n=k}^{m}\frac{1}{n}\binom{n}{k}$. As $\frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}$ and $\sum\limits_{n=k}^{m}\binom{n-1}{k-1}$ is the coefficient of X^{k-1} in the polynomial $\sum\limits_{n=k}^{m}(1+X)^{n-1} = \frac{(1+X)^m-(1+X)^{k-1}}{X}$, *i.e.* that of X^k in $(1+X)^m-(1+X)^{k-1}$, that is $\binom{m}{k}$, we have $-a_m = \sum\limits_{k=1}^{m}(-1)^k\binom{m}{k}k^{m-1} = \alpha_{m,m-1}$ if $m > 1$. As we have seen above, we have $\alpha_{m,m-1} = 0$, so $a_m = 0$ when $m > 1$. On the other hand, we have $a_1 = 1$, showing $\ln(\exp(X)) = X$.

• If $N \in \mathbf{Z}_{>0}$, put $u_N(x) = \sum\limits_{n=0}^{N}\frac{X^n}{n!}$. We have

$$u_{2N}(X+Y) = \sum_{n=0}^{2N}\tfrac{(X+Y)^n}{n!} = \sum_{n=0}^{2N}\sum_{k=0}^{n}\tfrac{X^kY^{n-k}}{k!(n-k)!} = \sum_{\substack{j,k\in\mathbf{Z}_{\geqslant 0}\\ j+k\leqslant 2N}}\tfrac{X^jY^k}{j!k!}$$

and $u_N(X)u_N(Y) = \sum\limits_{0\leqslant j,k\leqslant N}\frac{X^jY^k}{j!k!}$: this implies that $u_{2N}(X+Y) - u_N(X)u_N(Y) = \sum\limits_{\substack{j,k\in\mathbf{Z}_{\geqslant 0}\\ j+k\leqslant 2N\\ \max(j,k)>N}}\frac{X^jY^k}{j!k!}$.
Passing to the limit as $N\to\infty$ gives $\exp(X+Y) = \exp(X)\exp(Y)$ in $\mathbf{Q}[\![X,Y]\!]$. This implies in particular that $\exp(X)^k = \exp(kX)$ in $\mathbf{Q}[\![X]\!]$ for all $k \in \mathbf{Z}$.
• By what precedes, we have $\exp(\ln(1+X)+\ln(1+Y)) = \exp(\ln(1+X))\exp(\ln(1+Y)) = (1+X)(1+Y)$: applying ln gives $\ln((1+X)(1+Y)) = \ln(1+X)+\ln(1+Y)$ in $\mathbf{Q}[\![X,Y]\!]$.

Remark 6.4.5. These equalities also follow from the corresponding equality of power series over the complex numbers.

□

Proposition 6.4.6. (1) The radius of convergence of ln (resp. exp) is 1 (resp. $p^{-\frac{1}{p-1}}$). Moreover, we have $|\ln(1+x)|_p = |x|_p$ and $|\exp(x)-1|_p = |x|_p$ for all $x \in \mathrm{D}\left(0, p^{-\frac{1}{p-1}}\right)$.

(2) We have $\ln((1+x)(1+y)) = \ln(1+x)+\ln(1+y)$ (resp. $\exp(x+y) = \exp(x)\exp(y)$) for all $x, y \in \mathrm{D}(0,1)$ (resp. $x, y \in \mathrm{D}\left(1, p^{-\frac{1}{p-1}}\right)$).

(3) log and exp provide inverse group isomorphisms $\left(\mathrm{D}\left(1,p^{-\frac{1}{p-1}}\right),.\right) \underset{\exp}{\overset{\ln}{\rightleftarrows}} \left(\mathrm{D}\left(0,p^{-\frac{1}{p-1}}\right),+\right)$.

Proof. • Let $x \in \mathbf{C}_p$ be such that $|x|_p < 1$. If $n \in \mathbf{Z}_{>0}$, we have $\frac{1}{|n|_p} = p^{v_p(n)} \mid n$: this implies that $\left|\frac{x^n}{n}\right|_p \leqslant n\,|x|_p^n$, whence $\lim\limits_{n\to\infty}\left|\frac{x^n}{n}\right|_p = 0$, so that the series $\sum\limits_{n=0}^{\infty} \frac{(-1)^{n-1}}{n}x^n$ converges. As it obviously diverges at $x = 1$ (because $|n|_p$ takes arbitrary small values), the radius of convergence of ln is 1.
Assume that $|x|_p < p^{-\frac{1}{p-1}}$. If $n \in \{2, \ldots, n-1\}$, we have $|n|_p = 1$ whence $\left|\frac{x^n}{n}\right|_p = |x|_p^n < |x|_p$. If $n \geqslant p$, then $\frac{n-1}{\ln(n)} \geqslant \frac{p-1}{\ln(p)}$ (because the map $f\colon t \mapsto \frac{t-1}{\ln(t)}$ extended by continuity at $t = 1$ by $f(1) = 1$, is strictly increasing on $[1, +\infty[$ as a trivial computation shows). This implies that

$$v_p\left(\tfrac{x^n}{n}\right) = v_p(x) + (n-1)v_p(x) - v_p(n) > v_p(x) + \tfrac{n-1}{p-1} - \tfrac{\ln(n)}{\ln(p)} \geqslant v_p(x)$$

(since $v_p(x) > \frac{1}{p-1}$) so that $v_p\left(\frac{x^n}{n}\right) > v_p(x)$ as well. This implies that $v_p(\ln(1+x)) = v_p(x)$, *i.e.* $|\ln(1+x)|_p = |x|_p$.
• The series defining $\exp(x)$ converges if and only if $\lim\limits_{n\to\infty} v_p\left(\frac{x^n}{n!}\right) = +\infty$. As

$$v_p\left(\tfrac{x^n}{n!}\right) = nv_p(x) - v_p(n!) = n\left(v_p(x) - \tfrac{1}{p-1}\right) + \tfrac{s(n)}{p-1}$$

(*cf* lemma 6.4.1), this is equivalent to $v_p(x) - \frac{1}{p-1} > 0$, *i.e.* $|x|_p < p^{-\frac{1}{p-1}}$ (observe that $s(p^k) = 1$ for all $k \in \mathbf{Z}_{\geqslant 0}$).
Assume that $|x|_p < p^{-\frac{1}{p-1}}$, *i.e.* $v_p(x) > \frac{1}{p-1}$: if $n \in \mathbf{Z}_{\geqslant 2}$, we have

$$(n-1)v_p(x) > \tfrac{n-1}{p-1} \geqslant \tfrac{n-s(n)}{p-1} = v_p(n!),$$

i.e. $v_p\left(\frac{x^n}{n!}\right) = nv_p(x) - v_p(n!) > v_p(x)$: we have $v_p\left(\sum\limits_{n=2}^{\infty}\frac{x^n}{n!}\right) > v_p(x)$, so that $v_p(\exp(x)-1) = v_p(x)$, *i.e.* $|\exp(x)-1|_p = |x|_p$.
(2) & (3) follow from lemma 6.4.3, noting that we have absolute convergence of the series involved. □

Remark 6.4.7. (1) In contrast with the complex analytic case, the radius of convergence of ln is strictly larger that that of exp.
(2) Being continuous (*cf* corollary 6.1.4) the inverse isomorphisms of proposition 6.4.6 are also homeomorphisms.

Proposition 6.4.8. There exists a unique continuous map

$$\ln\colon \mathbf{C}_p^\times \to \mathbf{C}_p$$

having the following properties:

(i) $(\forall x, y \in \mathbf{C}_p^\times)\ \ln(xy) = \ln(x) + \ln(y)$;

(ii) $(\forall x \in \mathrm{D}(1,1))\ \ln(x) = \sum\limits_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(x-1)^n$;

(iii) $\ln(p) = 0$.

Proof. We have the exact sequence of abelian groups:

$$\{1\} \to \mathcal{O}_{\mathbf{C}_p}^\times \to \mathbf{C}_p^\times \xrightarrow{v_p} \mathbf{Q} \to 0$$

The choice of a compatible system $\left(p^{(v)}\right)_{v\in\mathbf{Q}}$ in $\mathbf{C}_p^\times$ (*i.e.* such that $p^{(1)} = p$ and $p^{(v_1+v_2)} = p^{(v_1)}p^{(v_2)}$ for all $v_1, v_2 \in \mathbf{Q}$) provides a section $\mathbf{Q} \to \mathcal{O}_{\mathbf{C}_p}^\times$ of v_p. To construct such a system, one can proceed as follows. Let $(p_n)_{n\in\mathbf{Z}_{>0}} \in \mathbf{C}_p^{\mathbf{Z}_{>0}}$ be such that $p_1 = p$ and p_{n+1} is a root of $X^{n+1} - p_n$ in $\mathbf{C}_p$ for all $n \in \mathbf{Z}_{>0}$. Then $v_p(p_n) = \frac{1}{n!}$, and if $v \in \mathbf{Q}$, the element $p^{(v)} := p_n^{n!v}$ does not depend on the choice of $n \in \mathbf{Z}_{>0}$ such that $n!v \in \mathbf{Z}$.
This implies in particular that there is a (non canonical) isomorphism:

$$\mathcal{O}_{\mathbf{C}_p}^\times \times \mathbf{Q} \xrightarrow{\sim} \mathbf{C}_p^\times$$

given by $(u, v) \mapsto up^{(v)}$. Similarly, we have the exact sequence of abelian groups:

$$\{1\} \to 1 + \mathfrak{m}_{\mathbf{C}_p} \to \mathcal{O}_{\mathbf{C}_p}^\times \to \overline{\mathbf{F}}_p^\times \to \{1\}$$

(the last map being the canonical projection). The Teichmüller map (*cf* definition 3.8.20) provides a section of the latter: there is a canonical isomorphism

$$(1+\mathfrak{m}_{\mathbf{C}_p})\times\overline{\mathbf{F}}_p^\times \xrightarrow{\sim} \mathcal{O}_{\mathbf{C}_p}^\times$$

given by $(1+x,\overline{\zeta})\mapsto(1+x)[\overline{\zeta}]$. Put together, this provides an isomorphism

$$(1+\mathfrak{m}_{\mathbf{C}_p})\times\overline{\mathbf{F}}_p^\times\times\mathbf{Q}\xrightarrow{\sim}\mathbf{C}_p^\times$$

given by $(1+x,\overline{\zeta},v)\mapsto(1+x)[\overline{\zeta}]p^{(v)}$.

• Assume the map $\ln\colon\mathbf{C}_p^\times\to\mathbf{C}_p$ exists. Let $x\in\mathfrak{m}_{\mathbf{C}_p}$, $\overline{\zeta}\in\overline{\mathbf{F}}_p^\times$ and $v\in\mathbf{Q}$. There exists $f\in\mathbf{Z}_{>0}$ such that $\overline{\zeta}^{p^f-1}=1$: as the map $[.]$ is multiplicative, we have $[\overline{\zeta}]^{p^f-1}=1$, so that $(p^f-1)\ln\big([\overline{\zeta}]\big)=\ln(1)=0$ (by property (i)), so $\ln\big([\overline{\zeta}]\big)=0$. If $n\in\mathbf{Z}_{>0}$ is such that $n!v\in\mathbf{Z}$, we have $n!v\ln\big(p^{(v)}\big)=\ln\big(p^{(v)n!v}\big)=0$ by properties (i) and (iii): properties (i) and (ii) imply that $\ln\big((1+x)[\overline{\zeta}]p^{(v)}\big)=\ln(1+x)=\sum\limits_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}(x-1)^n$. This shows the unicity of the map ln.

• The composite of the isomorphism $\mathbf{C}_p^\times\xrightarrow{\sim}(1+\mathfrak{m}_{\mathbf{C}_p})\times\overline{\mathbf{F}}_p^\times\times\mathbf{Q}$ with the first projection, followed with the group homomorphism $\ln\colon\mathrm{D}(1,1)\to\mathbf{C}_p$ (*cf* proposition 6.4.6 (3)) provides a group homomorphism $\mathbf{C}_p^\times\to\mathbf{C}_p$ having properties (i), (ii) and (iii).

Let $z\in\mathbf{C}_p^\times$. If $z'\in\mathrm{D}\big(z,p^{-\frac{1}{p-1}}|z|_p\big)$, we have $\frac{z'}{z}-1\in\mathrm{D}\big(0,p^{-\frac{1}{p-1}}\big)$, so that $\Big|\ln\big(1+\frac{z'}{z}-1\big)\Big|_p=\Big|\frac{z'}{z}-1\Big|_p$ by proposition 6.4.6 (1), *i.e.* $|\ln(z')-\ln(z)|_p=\frac{|z'-z|_p}{|z|_p}$: this shows the continuity of ln. □

Definition 6.4.9. If $n\in\mathbf{Z}_{\geqslant0}$, we put $\binom{a}{n}=\frac{a(a-1)\cdots(a-n+1)}{n!}\in\mathbf{Q}[a]$. Evaluated at an integer, this coincides with the usual binomial coefficient. We also define

$$B(a,X)=\sum_{n=0}^{\infty}\binom{a}{n}X^n\in\mathbf{Q}[\![a,X]\!].$$

Lemma 6.4.10. Let $x\in\mathfrak{m}_{\mathbf{C}_p}$. The map $\mathbf{Z}_{\geqslant0}\to\mathcal{O}_{\mathbf{C}_p}^\times;m\mapsto(1+x)^m$ is continuous (for the topology defined by $|.|_p$ on both sides). In particular, it extends by continuity into a map $\mathbf{Z}_p\to\mathcal{O}_{\mathbf{C}_p}^\times;a\mapsto(1+x)^a$.

Proof. As $(1+x)^m\in1+\mathfrak{m}_{\mathbf{C}_p}$ for all $m\in\mathbf{Z}_{\geqslant0}$, it is enough to check that $\lim\limits_{k\to\infty}(1+x)^{p^k}=1$ in $\mathbf{C}_p$: this follows from $(1+x)^{p^k}=\exp(p^k\ln(1+x))$ and $\big|\exp(p^k\ln(1+x))-1\big|_p=\big|p^k\ln(1+x)\big|_p=\frac{1}{p^k}$ for $k\geqslant1$ (*cf* proposition 6.4.6 (1) & (2)). □

Proposition 6.4.11. (1) Assume $a\in\mathbf{C}_p$. The radius of convergence of the series $B(a,X)$ is $\frac{p^{-\frac{1}{p-1}}}{|a|_p}$ if $|a|_p>1$ and at least $p^{-\frac{1}{p-1}}$ if $|a|_p\leqslant1$.

(2) If $a\in\mathbf{Z}_p$, then $B(a,X)\in\mathbf{Z}_p[\![X]\!]$ so the radius of convergence of $B(a,X)$ is at least 1, and we have $B(a,x)=(1+x)^a$ for all $x\in\mathfrak{m}_{\mathbf{C}_p}$.

(3) Assume that $|x|_p<p^{-\frac{1}{p-1}}\min\big\{1,\frac{1}{|a|_p}\big\}$. Then $B(a,x)=\exp(a\ln(1+x))$. In particular, if $m\in\mathbf{Z}_{\geqslant0}$ and $x\in\mathrm{D}\big(0,p^{-m-\frac{1}{p-1}}\big)$, we have $B\big(\frac{1}{p^m},x\big)^{p^m}=1+x$, *i.e.* $B\big(\frac{1}{p^m},x\big)$ is a p^m-th root of $1+x$.

(4) We have $B(a,X)=\exp(a\ln(1+X))$ in $\mathbf{Q}[\![a,X]\!]$. In particular, $B(a_1,X)B(a_2,X)=B(a_1+a_2,X)$ in $\mathbf{Q}[\![a_1,a_2,X]\!]$, and $\mathsf{B}(a,X)^p=\mathsf{B}(pa,X)$ in $\mathbf{Q}[\![a,X]\!]$.

Proof. (1) • Assume $|a|_p>1$: we have $|a-k|_p=|a|_p$ for all $k\in\mathbf{Z}$, so that $\big|\binom{a}{n}\big|_p=\frac{|a|_p^n}{|n!|_p}$: the computation of proposition 6.4.6 (1) implies that the radius of convergence of $B(a,X)$ is $\frac{p^{-\frac{1}{p-1}}}{|a|_p}$ in this case.

• Assume $|a|_p\leqslant1$: we have $|a-k|_p\leqslant|a|_p$ for all $k\in\mathbf{Z}$, so that $\big|\binom{a}{n}\big|_p\leqslant\frac{1}{|n!|_p}$, and the radius of convergence of $B(a,X)$ is equal to that of $\exp(X)$, *i.e.* $p^{-\frac{1}{p-1}}$.

(2) • Let $n\in\mathbf{Z}_{\geqslant0}$. The map $a\mapsto\binom{a}{n}$ is polynomial, hence continuous on $\mathbf{Z}_p$. It has values in $\mathbf{Z}\subset\mathbf{Z}_p$ on $\mathbf{Z}_{\geqslant0}$: as $\mathbf{Z}_{\geqslant0}$ is dense in $\mathbf{Z}_p$ and $\mathbf{Z}_p$ is closed, we have $\binom{a}{n}\in\mathbf{Z}_p$ for all $a\in\mathbf{Z}_p$. This shows that $B(a,X)\in\mathbf{Z}_p[\![X]\!]$, implying that the radius of convergence of $B(a,X)$ is at least 1 (note that it might be larger: it is infinite when $a\in\mathbf{Z}_{\geqslant0}$ for instance).

• Fix $x\in\mathfrak{m}_{\mathbf{C}_p}$. The maps $a\mapsto\binom{a}{n}$ being continuous and bounded by 1 on $\mathbf{Z}_p$, the series of functions $a\mapsto\binom{a}{n}x^n$ converges normally on $\mathbf{Z}_p$: its sum $a\mapsto B(a,x)$ is continuous on $\mathbf{Z}_p$. As $a\mapsto(1+x)^a$ is continuous as well (*cf* (1)), the equality $(1+x)^a=B(a,x)$ holds for all $a\in\mathbf{Z}_p$ since it holds when $a\in\mathbf{Z}_{\geqslant0}$ (binomial expansion), and $\mathbf{Z}_{\geqslant0}$ is dense in $\mathbf{Z}_p$.

(3) • If $|x|_p < p^{-\frac{1}{p-1}} \min\left\{1, \frac{1}{|a|_p}\right\}$, both series $B(a,x)$ and $\exp(a\ln(1+x))$ converge absolutely in $\mathbf{C}_p$: it is enough to check the equality in $\mathbf{Q}[\![a,X]\!]$. This follows from the equality when $a \in \mathbf{Z}_p$ and $x \in \mathfrak{m}_{\mathbf{C}_p}$.
• By proposition 6.4.6, and (2), we have $B\big(\frac{1}{p^m},x\big)^{p^m} = \exp\big(\frac{1}{p^m}\ln(1+x)\big)^{p^m} = \exp(\ln(1+x)) = 1+x$ when $x \in \mathrm{D}\left(0, p^{-m-\frac{1}{p-1}}\right)$.
(4) This follows from (3) and lemma 6.4.3. □

6.4.12. *The Artin-Hasse exponential.* In contrast with the complex analytic case, the p-adic exponential formal series has a small radius of convergence. The *Artin-Hasse exponential map* is a modified exponential map whose radius of convergence is 1.

Definition 6.4.13. The *Artin-Hasse exponential map* is

$$\mathsf{AH}(X) = \exp\left(X + \tfrac{X^p}{p} + \tfrac{X^{p^2}}{p^2} + \cdots\right) \in \mathbf{Q}[\![X]\!].$$

Lemma 6.4.14. $\mathsf{AH}(X) = \prod\limits_{\substack{n\in\mathbf{Z}_{>0}\\ p\nmid n}} (1-X^n)^{-\frac{\mu(n)}{n}}$ in $\mathbf{Q}[\![X]\!]$ (where $\mu\colon \mathbf{Z}_{>0} \to \{-1,0,1\}$ is Möbius map).

Proof. By lemma 6.4.3, we have

$$\begin{aligned}\log\Big(\prod_{\substack{n\in\mathbf{Z}_{>0}\\ p\nmid n}} (1-X^n)^{-\frac{\mu(n)}{n}}\Big) &= \sum_{\substack{n\in\mathbf{Z}_{>0}\\ p\nmid n}} -\tfrac{\mu(n)}{n}\log(1-X^n) = \sum_{\substack{n\in\mathbf{Z}_{>0}\\ p\nmid n}} \tfrac{\mu(n)}{n} \sum_{m=1}^{\infty} \tfrac{X^{nm}}{m}\\ &= \sum_{k=1}^{\infty} \tfrac{X^k}{k} \sum_{\substack{n\mid k\\ p\nmid n}} \mu(n) = \sum_{i=0}^{\infty} \tfrac{X^{p^i}}{p^i}\end{aligned}$$

since $\sum\limits_{\substack{n\mid k\\ p\nmid n}} \mu(n) = \sum\limits_{n\mid k/p^{v_p(k)}} \mu(n) = \begin{cases} 1 & \text{if } k = p^{v_p(k)}\\ 0 & \text{otherwise}\end{cases}$. □

Lemma 6.4.15. Assume $p \nmid n$ and $f(X) = 1 + \sum\limits_{i=1}^{\infty} a_i X^i \in \mathbf{Q}[\![X]\!]$ satisfies $f(X)^n \in 1 + X\,\mathbf{Z}_{(p)}[\![X]\!]$, then $f(X) \in 1 + X\,\mathbf{Z}_{(p)}[\![X]\!]$.

Proof. Write $f(X)^n = 1 + \sum\limits_{i=1}^{\infty} b_i X^i$: we show that $a_i \in \mathbf{Z}_{(p)}$ by induction on $i \in \mathbf{Z}_{>0}$. Assume $a_j \in \mathbf{Z}_{(p)}$ for all $j < i$. We have $b_i = na_i + \sum\limits_{\substack{j_1+\cdots+j_n=i\\ (\exists k\leqslant n)\ j_k<n}} a_{j_1}\cdots a_{j_n} \in na_i + \mathbf{Z}_{(p)}$, hence $na_i \in \mathbf{Z}_{(p)}$ so that $a_i \in \mathbf{Z}_{(p)}$ since $p \nmid n$. □

Proposition 6.4.16. $\mathsf{AH}(X) \in \mathbf{Z}_{(p)}[\![X]\!]$, so the radius of convergence of $\mathsf{AH}(X)$ is at least 1.

Proof. Follows from lemmas 6.4.14 & 6.4.15. □

6.4.17. *An extra useful series.* If $N \in \mathbf{Z}_{>0}$, we have

$$\begin{aligned}&B(X,Y)\prod_{i=1}^{N} B\big(\tfrac{X^{p^i}-X^{p^{i-1}}}{p^i}, Y^{p^i}\big)\\ &= \Big(\sum_{j=0}^{\infty} X(X-1)\cdots(X-j+1)\tfrac{Y^j}{j!}\Big)\prod_{i=1}^{N}\Big(\sum_{j=0}^{\infty} \tfrac{X^{p^i}-X^{p^{i-1}}}{p^i}\big(\tfrac{X^{p^i}-X^{p^{i-1}}}{p^i}-1\big)\cdots\big(\tfrac{X^{p^i}-X^{p^{i-1}}}{p^i}-j+1\big)\tfrac{Y^{jp^i}}{j!}\Big).\end{aligned}$$

This is an element of $\mathbf{Q}[\![X,Y]\!]$. The factors contributing to the coefficient of the monomial X^nY^m are $B(X,Y)$ and those $B\big(\frac{X^{p^i}-X^{p^{i-1}}}{p^i}, Y^{p^i}\big)$ for which $p^i \leqslant m$ (recall that the constant term in $B(a,T)$ is 1): this coefficient does not depend on $N \geqslant m$. This implies that the following definition makes sense:

Definition 6.4.18. We define *Dwork's series* by

$$F(X,Y) = B(X,Y)\prod_{i=1}^{\infty} B\big(\tfrac{X^{p^i}-X^{p^{i-1}}}{p^i}, Y^{p^i}\big) \in \mathbf{Q}[\![X,Y]\!].$$

Remark 6.4.19. (1) We thus can think of $F(X,Y)$ as $(1+Y)^X(1+Y^p)^{\frac{X^p-X}{p}}(1+Y^{p^2})^{\frac{X^{p^2}-X^p}{p^2}}\cdots$.
(2) The monomials X^nY^m that appear in the factors $B(X,Y)$ and $B\big(\frac{X^{p^n}-X^{p^{n-1}}}{p^n}, Y^{p^n}\big)$ satisfy $n \leqslant m$: the same holds for F, so we can write $F(X,Y) = \sum\limits_{0\leqslant n\leqslant m} a_{n,m}X^nY^m \in \mathbf{Q}[\![X,Y]\!]$.

Proposition 6.4.20. We have $F(X,Y) \in \mathbf{Z}_p[\![X,Y]\!]$.

Lemma 6.4.21. (Dwork) Let $f(X) \in 1 + X\,\mathbf{Q}_p[\![X]\!]$. Then we have $f(X) \in 1 + X\,\mathbf{Z}_p[\![X]\!]$ if and only if $\frac{f(X^p)}{f(X)^p} \in 1 + pX\,\mathbf{Z}_p[\![X]\!]$.

Proof. • Assume $f(X) \in 1 + X\,\mathbf{Z}_p[\![X]\!]$: we can write $f(X) = 1 + Xg(X)$ with $g(X) \in \mathbf{Z}_p[\![X]\!]$. We have $f(X)^p = (1 + Xg(X))^p \equiv 1 + X^pg(X^p) \mod pX\,\mathbf{Z}_p[\![X]\!]$: as $f(X) \in \mathbf{Z}_p[\![X]\!]^\times$, we deduce that $\frac{f(X^p)}{f(X)^p} \equiv 1 \mod pX\,\mathbf{Z}_p[\![X]\!]$.

• Conversely, assume that $\frac{f(X^p)}{f(X)^p} \equiv 1 \mod pX\,\mathbf{Z}_p[\![X]\!]$. Write $f(X) = \sum\limits_{n=0}^{\infty} a_nX^n$ and $\frac{f(X^p)}{f(X)^p} = \sum\limits_{n=0}^{\infty} b_nX^n$, with $(a_n)_{n\in\mathbf{Z}_{>0}} \in \mathbf{Q}_p^{\mathbf{Z}_{>0}}$ and $(b_n)_{n\in\mathbf{Z}_{>0}} \in p\,\mathbf{Z}_p^{\mathbf{Z}_{>0}}$ (and $a_0 = b_0 = 1$). We show that $a_n \in \mathbf{Z}_p$ by induction on n, starting with $a_0 = 1$. Assume that $a_k \in \mathbf{Z}_p$ for all $k < n$, so that $h(X) := \sum\limits_{k=0}^{n-1} a_kX^k \in \mathbf{Z}_p[X]$. We have $f(X) \equiv h(X) + a_nX^n \mod X^{n+1}\,\mathbf{Q}_p[\![X]\!]$, hence

$$\begin{aligned} f(X)^p \equiv (h(X) + a_nX^n)^p \mod X^{n+1}\,\mathbf{Q}_p[\![X]\!] &\equiv h(X)^p + ph(X)a_nX^n \mod X^{n+1}\,\mathbf{Q}_p[\![X]\!] \\ &\equiv h(X)^p + pa_nX^n \mod X^{n+1}\,\mathbf{Q}_p[\![X]\!] \end{aligned}$$

hence $f(X)^p\Big(\sum\limits_{m=0}^{\infty} b_mX^m\Big) \equiv h(X)^p\Big(\sum\limits_{m=0}^{n} b_mX^m\Big) + pa_nX^n \mod X^{n+1}\,\mathbf{Q}_p[\![X]\!]$ (since $b_0 = 1$). On the other hand, we have $h(X)^p \equiv \sum\limits_{k=0}^{n-1} a_kX^{pk} \mod p\,\mathbf{Z}_p[X]$ (because $h(X) \in \mathbf{Z}_p[X]$) and $b_m \in p\,\mathbf{Z}_p$ for $m \in \mathbf{Z}_{>0}$: this implies that the coefficient of X^n in the product belongs to $pa_n + a_{n/p} + p\,\mathbf{Z}_p$ if $p \mid n$ and to $pa_n + p\,\mathbf{Z}_p$ otherwise. As this coefficient is $a_{n/p}$ if $p \mid n$ and 0 otherwise, we have $a_n \in \mathbf{Z}_p$ in all cases. □

Similarly, we have:

Lemma 6.4.22. If $f(X,Y) \in 1 + X\,\mathbf{Q}_p[\![X,Y]\!] + Y\,\mathbf{Q}_p[\![X,Y]\!]$, then $f(X,Y) \in 1 + X\,\mathbf{Z}_p[\![X,Y]\!] + Y\,\mathbf{Z}_p[\![X,Y]\!]$ if and only if $\frac{f(X^p,Y^p)}{f(X,Y)^p} \in 1 + pX\,\mathbf{Z}_p[\![X,Y]\!] + pY\,\mathbf{Z}_p[\![X,Y]\!]$.

Proof of proposition 6.4.20. It is enough to apply lemma 6.4.22 to $F(X,Y)$. We have

$$F(X^p,Y^p) = B(X^p,Y^p)\prod_{i=1}^{\infty} B\big(\tfrac{X^{p^{i+1}}-X^{p^i}}{p^i}, Y^{p^{i+1}}\big) = B(X^p,Y^p)\prod_{i=2}^{\infty} B\big(\tfrac{X^{p^i}-X^{p^{i-1}}}{p^i}, Y^{p^i}\big)^p$$

so that

$$\tfrac{F(X^p,Y^p)}{F(X,Y)^p} = \tfrac{B(X^p,Y^p)}{B(X,Y)^pB\left(\frac{X^p-X}{p},Y^p\right)^p} = \tfrac{B(X^p,Y^p)}{B(X,Y)^pB(X^p-X,Y^p)} = \tfrac{B(X,Y^p)}{B(X,Y)^p}$$

by proposition 6.4.11 (4). By proposition 6.4.11 (4) again, we have

$$\tfrac{B(X,Y^p)}{B(X,Y)^p} = \tfrac{\exp(X\ln(1+Y^p))}{\exp(pX\ln(1+Y))} = \exp\big(X\ln\big(\tfrac{1+Y^p}{(1+Y)^p}\big)\big)$$

By lemma 6.4.21, we have $\frac{1+Y^p}{(1+Y)^p} \in 1 + pY\,\mathbf{Z}_p[\![Y]\!]$, hence $\ln\big(\frac{1+Y^p}{(1+Y)^p}\big) \in pY\,\mathbf{Z}_p[\![Y]\!]$, so that

$$\exp\big(X\ln\big(\tfrac{1+Y^p}{(1+Y)^p}\big)\big) \in 1 + pX\,\mathbf{Z}_p[\![X,Y]\!] + pY\,\mathbf{Z}_p[\![X,Y]\!].$$

□

6.5. **Rationality criteria.** A reference for this part is [1, Chapitre 5].

6.5.1. *The algebraic criterion.* Let K be a field, $\mathbf{a} = (a_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in K^{\mathbf{Z}_{\geqslant 0}}$ and $f(X) = \sum\limits_{n=0}^{\infty} a_nX^n \in K[\![X]\!]$. If $k, n \in \mathbf{Z}_{\geqslant 0}$, the *Hankel matrix* (resp. the *Hankel determinant*) of rank n and order k is the matrix $M_n^{(k)}(\mathbf{a}) = (a_{n+i+j})_{0\leqslant i,j\leqslant k} \in \mathsf{M}_{k+1}(K)$ (resp. $D_n^{(k)}(\mathbf{a}) = \det\big(M_n^{(k)}(\mathbf{a})\big)$).

Lemma 6.5.2. If $k \in \mathbf{Z}_{>0}$ and $n \in \mathbf{Z}_{\geqslant 0}$, we have

$$D_n^{(k)}(\mathbf{a})D_{n+2}^{(k-2)}(\mathbf{a}) = D_{n+2}^{(k-1)}(\mathbf{a})D_n^{(k-1)}(\mathbf{a}) - D_{n+1}^{(k-1)}(\mathbf{a})^2$$

(with the convention $D_n^{(-1)}(\mathbf{a}) = 1$).

Proof. This is a direct consequence of lemma 6.5.3 below. □

Lemma 6.5.3. (Sylvester relations). Let R be a commutative ring and $n \in \mathbf{Z}_{>0}$. If $A \in \mathsf{M}_{n+1}(R)$, let $\widetilde{A} \in \mathsf{M}_{n-1}(R)$ denote the matrix obtained from A by removing the extremal rows and columns. Write $\mathsf{com}(A) = (A_{i,j})_{0\leqslant i,j\leqslant n}$. Then $\det(A)\det\big(\widetilde{A}\big) = A_{0,0}A_{n,n} - A_{0,n}A_{n,0}$.

Proof. We may assume $R = \mathbf{Z}[X_{i,j}]_{0\leqslant i,j\leqslant n}$ and $A = (X_{i,j})_{0\leqslant i,j\leqslant n}$. Let $B = (b_{i,j})_{0\leqslant i,j\leqslant n} \in \mathsf{M}_{n+1}(A)$ such that $b_{i,j} = M_{i,j}$ if $i \in \{0, n\}$ and $j \in \{0, \dots, n\}$, and $b_{i,j} = \delta_{i,j}$ if $i \in \{1, \dots, n-1\}$ and $j \in \{0, \dots, n\}$:

$$B = \begin{pmatrix} A_{0,0} & A_{0,1} & \cdots & A_{0,n-1} & A_{0,n} \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \\ A_{n,0} & A_{n,1} & \cdots & A_{n,n-1} & A_{n,n} \end{pmatrix}$$

By definition of coefficients $A_{i,j}$, we have:

$$BA = \begin{pmatrix} \det(A) & 0 & \cdots & \cdots & 0 \\ * & & & & * \\ \vdots & & \widetilde{A} & & \vdots \\ * & & & & * \\ 0 & \cdots & \cdots & 0 & \det(A) \end{pmatrix}$$

which implies $\det(A)^2 \det\big(\widetilde{A}\big) = \det(A)\det(B) = \det(A)\big(A_{0,0}A_{n,n} - A_{0,n}A_{n,0}\big)$: we deduce the equality $\det(A)\det\big(\widetilde{A}\big) = A_{0,0}A_{n,n} - A_{0,n}A_{n,0}$ by dividing by $\det(A)$ (which is licit in the integral domain R). □

Theorem 6.5.4. We have $f(X) \in K(X)$ if and only if there exist $n_0, k \in \mathbf{Z}_{\geqslant 0}$ such that $D_n^{(k)}(\mathbf{a}) = 0$ for all $n \in \mathbf{Z}_{\geqslant n_0}$.

Proof. • Assume $f(X) \in K(X)$: there exist $P(X), Q(X) \in K[X]$ with $Q(X) \neq 0$ such that $f(X) = \frac{P(X)}{Q(X)}$. Write $Q(X) = X^k + b_1X^{k-1} + \cdots + b_k = \sum\limits_{\ell=0}^{k} b_{k-\ell}X^\ell$ (with $b_0 = 1$). If $m \geqslant m_0 := \max\{\deg(P), \deg(Q)\}$, the coefficient of X^m in $Q(X)f(X) = P(X)$ is $\sum\limits_{\ell=0}^{k} a_{m-\ell}b_{k-\ell} = 0$, *i.e.* $\sum\limits_{i=0}^{k} a_{m-k+i}b_i = 0$ (take $i = k - \ell$). If $n \geqslant n_0 = m_0 - k$ and $j \in \{0, \dots, k\}$, we have $m := n + k + j \geqslant m_0$, so that $\sum\limits_{i=0}^{k} a_{n+i+j}b_i = 0$, showing that $M_n^{(k)}(\mathbf{a})X = 0$ with $X = {}^{\mathrm{t}}(b_0, \dots, b_k) \in K^{k+1}\backslash\{0\}$: we have $D_n^{(k)}(\mathbf{a}) = 0$ for all $n \geqslant n_0$.

• Conversely, assume there exist $n_0, k \in \mathbf{Z}_{\geqslant 0}$ such that $D_n^{(k)}(\mathbf{a}) = 0$ for all $n \in \mathbf{Z}_{\geqslant n_0}$. If $\mathbf{a}$ is stationary, then $f(X)$ in rational: assume henceforth that $\mathbf{a}$ is not stationary. Let h be the smallest integer such that $D_n^{(h)}(\mathbf{a}) = 0$ for $n \gg 0$. We have $k > 0$ since $\mathbf{a}$ is not stationary. Let $n_0 \in \mathbf{Z}_{\geqslant 0}$ be the smallest integer such that $D_n^{(h)}(\mathbf{a}) = 0$ for $n \geqslant n_0$. Lemma 6.5.2 implies that $D_{n+2}^{(h-1)}(\mathbf{a})D_n^{(h-1)}(\mathbf{a}) = D_{n+1}^{(h-1)}(\mathbf{a})^2$ for all $n \geqslant n_0$. In particular, if $m \in \mathbf{Z}$ is such that $m \geqslant n_0$ and $D_m^{(h-1)}(\mathbf{a}) = 0$, then $D_n^{(h-1)}(\mathbf{a}) = 0$ for all $n \geqslant m$, contradicting the minimality of h. This implies that $D_n^{(h-1)}(\mathbf{a}) \neq 0$ for all $n \geqslant n_0$. This means that for $n \geqslant n_0$, the rank of $M_n^{(h)}(\mathbf{a})$ is h: the K-vector space $\mathsf{Ker}\big(M_n^{(h)}(\mathbf{a})\big)$ has dimension 1. Also, it coincides with the kernel of the matrix obtained from $M_n^{(h)}(\mathbf{a})$ by removing its first or last row. This implies that $\mathsf{Ker}\big(M_{n+1}^{(h)}(\mathbf{a})\big) = \mathsf{Ker}\big(M_n^{(h)}(\mathbf{a})\big)$, *i.e.* that $\mathsf{Ker}\big(M_n^{(h)}(\mathbf{a})\big)$ does not depend of $n \geqslant n_0$. If $X = {}^{\mathrm{t}}(b_h, \dots, b_0) \in \mathsf{Ker}\big(M_n^{(h)}(\mathbf{a})\big)$ and $Q(X) = \sum\limits_{\ell=0}^{k} b_{h-\ell}X^\ell$ then $Q(X) \neq 0$ and $Q(X)f(X) \in K[X]$, so that[44] $f(X) \in K(X)$. □

Corollary 6.5.5. We have $f(X) \in K(X)$ if and only if there exist $n_0 \in \mathbf{Z}_{\geqslant 0}$ such that $D_0^{(k)}(\mathbf{a}) = 0$ for all $k \in \mathbf{Z}_{\geqslant n_0}$.

Proof. • Assume $f(X) \in K(X)$. Let $A_n^{(k)} = (a_n, a_{n+1}, \dots, a_{n+k})$; then $D_0^{(k)} = \det(A_0^{(k)}, \dots, A_k^{(k)})$. If $Q(X) = X^h + b_1X^{h-1} + \cdots + b_h = \sum\limits_{\ell=0}^{h} b_{h-\ell}X^\ell$ (with $b_0 = 1$) is such that $Q(X)f(X) \in K[X]$, we have $\sum\limits_{\ell=0}^{h} b_\ell A_{k-\ell}^{(k)} = 0$ for $k \gg 0$, implying that the lines $A_{k-h}^{(k)}, \dots, A_K^{(k)}$ of $M_0^{(k)}(\mathbf{a})$ are linearly dependent, hence $D_0^{(k)}(\mathbf{a}) = 0$.

• Conversely, assume that $D_0^{(k)}(\mathbf{a}) = 0$ for $k \gg 0$. By lemma 6.5.2, we have

$$D_n^{(k+1)}(\mathbf{a})D_{n+2}^{(k-2)}(\mathbf{a}) = D_{n+2}^{(k)}(\mathbf{a})D_n^{(k)}(\mathbf{a}) - D_{n+1}^{(k)}(\mathbf{a})^2$$

If $D_n^{(k)}(\mathbf{a}) = 0$ for all $k \geqslant n_0$, then $D_n^{(k+1)}(\mathbf{a}) = D_n^{(k)}(\mathbf{a}) = 0$ so $D_{n+1}^{(k)}(\mathbf{a}) = 0$ for all $k \geqslant n_0$. A straightforward induction thus implies that $D_n^{(k)}(\mathbf{a}) = 0$ for all $k \geqslant n_0$ and all $n \in \mathbf{Z}_{\geqslant 0}$: by theorem 6.5.4, we have $f(X) \in K(X)$. □

[44] In fact $b_h \neq 0$, otherwise we would have $M_{n+2}^{(h-1)}(\mathbf{a})Y = 0$ with $X = {}^{\mathrm{t}}(b_{h-1}, \dots, b_0) \in K^h\backslash\{0\}$, contradicting $D_{n+1}^{(h-1)}(\mathbf{a}) \neq 0$. This shows that $\deg(Q) = h$.

6.5.6. *The analytic criterion.* As usual, let p be a prime number.

Lemma 6.5.7. Let $x \in \mathbf{Z}$. If $|x|\,|x|_p < 1$, we have $x = 0$.

Proof. Assume $x \neq 0$, we can write $x = p^{v_p(x)}y$ with $y \in \mathbf{Z}\backslash\{0\}$ prime to p: we have $|x|\,|x|_p = |y| \geqslant 1$. □

Theorem 6.5.8. Let $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n \in \mathbf{Z}[\![X]\!]$. Assume that f defines an holomorphic function on the disc $\{z \in \mathbf{C}\,;\, |z| < R\}$ and that f defines a meromorphic function (*i.e.* quotient of two holomorphic functions) on the disc $\{x \in \mathbf{C}_p\,;\, |x|_p < r\}$. If $Rr > 1$, then f is rational.

Proof. We apply theorem 6.5.4 with $K = \mathbf{Q}$.
• Making R a little smaller, we may assume that $\lim\limits_{n\to\infty} |a_n|\, R^n = 0$ (this follows from Cauchy inequalities): there exists $N \in \mathbf{Z}_{\geqslant 0}$ such that $|a_n| \leqslant R^{-n}$ for all $n \geqslant N$. If $n \geqslant N$ and $0 \leqslant i,j \leqslant k$, we have $|a_{n+i+j}| \leqslant R^{-(n+i+j)}$: Hadamard's inequality implies that

$$\left|D_n^{(k)}(\mathbf{a})\right|^2 \leqslant \prod_{j=0}^{k}\Big(\sum_{i=0}^{k} |a_{n+i+j}|^2\Big) \leqslant \prod_{j=0}^{k}\Big(\sum_{i=0}^{k} \tfrac{1+R^{-2}+\cdots+R^{-2k}}{R^{2(n+j)}}\Big) \leqslant \tfrac{C_k^2}{R^{2(k+1)n}}$$

hence $\left|D_n^{(k)}(\mathbf{a})\right| \leqslant \frac{C_k}{R^{(k+1)n}}$, where $C_k = \sqrt{\frac{(1+R^{-2}+\cdots+R^{-2k})^{k+1}}{R^{k(k+1)}}} \in \mathbf{R}_{>0}$.
• Making r a little smaller, there exist $g, h \in \mathscr{H}_{\mathbf{Q}_p}([0,r])$ such that $g = hf$. The order of vanishing of h is less that that of g: dividing g and h by the appropriate power of X, we may assume that $h(0) \neq 0$. By Weierstrass preparation theorem (*cf* theorem 6.2.2), there exist $P \in \mathbf{Q}_p[X]$ and $u \in \mathscr{H}_{\mathbf{Q}_p}([0,r])^\times$ such that $h = Pu$. Replacing h by P and g by gu^{-1}, we may assume that h is a polynomial. Dividing g and h by $h(0)$, we can further assume that $h(0) = 1$: write $h(X) = \sum\limits_{i=0}^{d} \alpha_i X^i$ (so $\alpha_0 = 1$). Write $g(X) = \sum\limits_{n=0}^{\infty} b_n X^n$. As $g \in \mathscr{H}_{\mathbf{Q}_p}([0,r])$, we have $\lim\limits_{n\to\infty} |b_n|_p\, r^n = 0$: making N larger if necessary, we may assume that $|b_n|_p \leqslant r^{-n}$ for all $n \geqslant N$. On the other hand, the equality $g = hf$ implies that $b_{m+d} = a_{m+d} + \alpha_1 a_{m+d-1} + \cdots + \alpha_d a_m$ for all $m \in \mathbf{Z}_{\geqslant 0}$. Assume $k \geqslant d$: in the determinant $D_n^{(k)}(\mathbf{a})$, we may replace a_{n+i+j} by b_{n+i+j} whenever $j \geqslant d$. If $n \geqslant N$, $i \in \{0,\ldots,k\}$ and $j \in \{d,\ldots,k\}$, we have

$$|b_{n+i+j}|_p \leqslant \begin{cases} r^{-(n+d)} & \text{if } r \geqslant 1 \\ r^{-(n+2k)} & \text{if } r < 1 \end{cases}.$$

As $|a_m|_p \leqslant 1$ since $a_m \in \mathbf{Z}$ for all $m \in \mathbf{Z}_{\geqslant 0}$, the strong triangle inequality implies that

$$\left|D_n^{(k)}(\mathbf{a})\right|_p \leqslant \begin{cases} r^{-(k+1-d)(n+d)} & \text{if } r \geqslant 1 \\ r^{-(k+1-d)(n+2k)} & \text{if } r < 1 \end{cases}.$$

In any case, we have $\left|D_n^{(k)}(\mathbf{a})\right|_p \leqslant \frac{c_k}{r^{(k+1-d)n}}$, with $c_k = \max\big\{r^{-(k+1-d)d}, r^{-2(k+1-d)k}\big\} \in \mathbf{R}_{>0}$.
• Assuming that $k \geqslant d$, we have thus

$$\left|D_n^{(k)}(\mathbf{a})\right| \left|D_n^{(k)}(\mathbf{a})\right|_p \leqslant \frac{C_k c_k}{R^{(k+1)n} r^{(k+1-d)n}}.$$

Now choose $k \geqslant d$ large enough so that $R^{k+1}r^{k+1-d} > 1$ (this is possible because $Rr > 1$): then we have $\lim\limits_{n\to\infty} \frac{C_k c_k}{R^{(k+1)n} r^{(k+1-d)n}} = 0$. Making N larger if necessary, we have $\left|D_n^{(k)}(\mathbf{a})\right| \left|D_n^{(k)}(\mathbf{a})\right|_p < 1$ for all $n \geqslant N$. As $D_n^{(k)}(\mathbf{a}) \in \mathbf{Z}$, lemma 6.5.8 implies that $D_n^{(k)}(\mathbf{a}) = 0$ for all $n \geqslant N$. □

6.6. **Exercises.**

Exercise 6.6.1. (Hensel Lemma). Let $(K, |.|)$ a complete non archimedean valued field, $P \in \mathcal{O}_K[X]$, and $\overline{P} \in \kappa_K[X]$ its reduction modulo $\mathfrak{m}_K$. Assume that there exist $f, g \in \kappa_K[X]$ such that

(i) $\overline{P} = fg$;
(ii) g is monic;
(iii) $\mathsf{gcd}(f,g) = 1$.

Show that there exist $F, G \in \mathcal{O}_K[X]$ such that:

(i) $P = FG$;
(ii) G is monic;
(iii) $\overline{F} = f$ and $\overline{G} = g$.

Exercise 6.6.2. Show that the disc of convergence of a power series $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n$ is contained in that of its derivative $f'(X) = \sum\limits_{n=1}^{\infty} n a_n X^{n-1}$. Give an example where the regions of convergence are not the same.

Exercise 6.6.3. Find an example of an infinite sum of nonzero rationals which converges with respect to $|.|_p$ for every prime p and with respect to $|.|_\infty$.

Exercise 6.6.4. Let K be a closed subfield of $\mathbf{C}_p$ and $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n \in \mathscr{H}_K([0,1[)$.
(1) Let $\rho \in [0,1[\cap \mathbf{Q}$. Show that $\sup\limits_{|z|=\rho} |f(z)| = \|f\|_\rho := \sup\limits_{n \in \mathbf{Z}_{\geqslant 0}} |a_n| \rho^n$ (in particular the maximum modulus principle holds: we have $\sup\limits_{|z| \leqslant \rho} |f(z)| = \|f\|_\rho$).
(2) Show that the map f is bounded (resp. bounded by 1) if and only if $f(X) \in \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathcal{O}_K[\![X]\!]$ (resp. $f(X) \in \mathcal{O}_K[\![X]\!]$).
(3) Show that the inclusions $\mathscr{H}_K([0,1]) \subset \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathcal{O}_K[\![X]\!] \subset \mathscr{H}_K([0,1[)$ are strict.

Exercise 6.6.5. Let K be a closed subfield of $\mathbf{C}_p$ and $0 < r_1 \leqslant r_2$. Is the inclusion

$$\iota\colon \mathscr{H}_K([0,r_2]) \to \mathscr{H}_K([0,r_1])$$

continuous for the norms $|.|_{r_2}$ and $|.|_{r_1}$?

Exercise 6.6.6. Let K be a closed subfield of $\mathbf{C}_p$ and $r \in \mathbf{R}_{>0}$. Show that $K[X]$ is dense in $(\mathscr{H}_K([0,r]), |.|_r)$.

Exercise 6.6.7. Find a locally analytic map that is not globally a power series on $\mathbf{C}_p$.

Exercise 6.6.8. Let K be a closed subfield of $\mathbf{C}_p$, $r \in \mathbf{R}_{>0}$ and $f \in K[\![X]\!]$.
(1) Show that if $r_1 \leqslant r_2$, then $\mathsf{w}_{r_1}(f) \leqslant \mathsf{w}_{r_2}(f)$.
(2) Assume $f \in \mathscr{H}_K([0,r])$ and let $r_1 \leqslant r_2 \leqslant r$. For $i \in \{1,2\}$, let $f = P_i u_i$ with $P_i \in K[X]$ monic of degree $\mathsf{w}_{r_i}(f)$ and $u_i \in \mathscr{H}_K([0,r_i])^\times$ be Weierstrass decomposition of f. Show that P_1 divides P_2 in $K[X]$.

Exercise 6.6.9. Let $f(X) = 1 + a_1 X + a_2 X^2 + \cdots \in \mathbf{C}_p[\![X]\!]$ defining an entire function on $\mathbf{C}_p$. Show that the reciprocals of the zeros of f form a sequence $(\alpha_i)_{i \in \mathbf{Z}_{>0}}$ that converges to 0, and that

$$f(X) = \prod_{i=1}^{\infty} (1 - \alpha_i X)$$

(for the metric defined by $|.|_r$ for any $r \in \mathbf{R}_{>0}$).

Exercise 6.6.10. (1) Draw the Newton polygon of $f(X) = \ln(1+X) = \sum\limits_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} X^n$. What is its radius of convergence?
(2) Show that $\lim\limits_{n\to\infty} \frac{1}{p^n}\binom{p^n}{k} = \frac{(-1)^{k-1}}{k}$, and that $f(X) = \lim\limits_{n\to\infty} \frac{(1+X)^{p^n}-1}{p^n}$.
(3) For $n \in \mathbf{Z}_{\geqslant 0}$, put $Q_n(X) = \Phi_{p^{n+1}}(1+X) = \frac{(1+X)^{p^{n+1}}-1}{(1+X)^{p^n}-1} \in \mathbf{Z}[X]$. Show that $f(X) = X \prod\limits_{n=0}^{\infty} \frac{Q_n(X)}{p}$. What are the roots of f in the open disc of convergence?

Exercise 6.6.11. (Weierstrass preparation theorem). Let $(K, |.|)$ be a complete discrete valued field. Fix a uniformizer π. If $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n \in \mathcal{O}_K[\![X]\!]$, let $\mathsf{w}(f) = \inf\{n \in \mathbf{Z}_{\geqslant 0}\,;\, a_n \in \mathcal{O}_K^\times\} \in \mathbf{Z}_{\geqslant 0} \cup \{+\infty\}$, so that $f \in \pi\mathcal{O}_K[\![X]\!] \Leftrightarrow \mathsf{w}(f) = +\infty$.
(1) Check that $\mathsf{w}(f) = 0 \Leftrightarrow f \in \mathcal{O}_K[\![X]\!]^\times$, and that $\mathsf{w}(fg) = \mathsf{w}(f) + \mathsf{w}(g)$.
(2) Let $f, g \in \mathcal{O}_K[\![X]\!]$ be such that $d := \mathsf{w}(g) < +\infty$. Show that there exist unique $q \in \mathcal{O}_K[\![X]\!]$ and $r \in \mathcal{O}_K[X]$ such that:

$$\begin{cases} \deg(r) < d \\ f = qf + r \end{cases}$$

(Weierstrass division theorem).

A polynomial $P \in \mathcal{O}_K[X]$ is called *distinguished* if $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ with $a_i \in \mathfrak{m}_K$ for all $i \in \{0, \ldots, d-1\}$. By the theory of Newton polygons, a distinguished polynomial P has exactly $\deg(P)$ roots in $\mathfrak{m}_{\overline{K}}$.
(3) Let $f \in \mathcal{O}_K[\![X]\!]$ be such that $d := \mathsf{w}(f) < +\infty$. There exists a unique distinguished polynomial P of degree d and a unique $u \in \mathcal{O}_K[\![X]\!]^\times$ such that $f = Pu$.
(4) Show that if $f \in K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]\backslash\{0\}$, there exist a unique $\mu \in \mathbf{Z}$, a unique distinguished polynomial P and $u \in \mathcal{O}_K[\![X]\!]^\times$ such that $f = \pi^\mu Pu$. In particular, f has exactly $\mathsf{w}(\pi^{-\mu}f)$ zeros in $\mathfrak{m}_{\overline{K}}$.
(5) Show that $K \otimes_{\mathcal{O}_K} \mathcal{O}_K[\![X]\!]$ is a PID.
(6) Assume $K \subset \mathbf{C}_p$. Show that $f \in \mathscr{H}_K([0,1[)\backslash\{0\}$ is bounded if and only if f has finitely many zeros in $\mathrm{D}(0,1)$.
(7) Construct a bounded element in $\mathscr{H}_{\mathbf{C}_p}([0,1])$ having infinitely many zeros in $\mathrm{D}(0,1)$.

Exercise 6.6.12. Let $(K, |.|)$ be a complete discrete valued field. Fix a uniformizer π. Show that $\mathcal{O}_K[\![X]\!]$ is a noetherian local ring, with maximal ideal $\mathfrak{m} = \langle \pi, X\rangle$, and whose other prime ideals are $\{0\}$, $\langle \pi \rangle$ and $\langle P \rangle$ with $P \in \mathcal{O}_K[X]$ an irreducible and distinguished polynomial.

Exercise 6.6.13. Let p be a prime number. Construct a continuous surjective map $\mathbf{Z}_p \to [0,1]$. Describe continuous maps $[0,1] \to \mathbf{Z}_p$.

Exercise 6.6.14. Let p be a prime number and $\mathscr{A} = \mathscr{C}^0(\mathbf{Z}_p, \mathbf{Q}_p)$. If $f \in \mathscr{A}$, put $\|f\|_\infty = \sup\limits_{x \in \mathbf{Z}_p} |f(x)|_p$. If $n \in \mathbf{Z}_{\geqslant 0}$, the *binomial polynomial* of index n is $\left(\binom{X}{n}\right) = \frac{X(X-1)\cdots(X-n+1)}{n!}$.
(1) Show that $(\mathscr{A}, \|.\|_\infty)$ is a Banach space.
(2) Show that $\left\|\binom{X}{n}\right\|_\infty = 1$ for all $n \in \mathbf{Z}_{\geqslant 0}$.
If $k \in \mathbf{Z}_{\geqslant 0}$ and $f \in \mathscr{A}$, we define $f^{[k]}$ inductively by $f^{[0]} = f$ and $f^{[k+1]}(x) = f^{[k]}(x+1) - f^{[k]}(x)$. The k-th *Mahler coefficient* of f is $a_k(f) = f^{[k]}(0)$.
(3) Show that if $f \in \mathscr{A}$, there exists $m \in \mathbf{Z}_{\geqslant 0}$ such that $\left\|f^{[p^m]}\right\|_\infty \leqslant \frac{\|f\|_\infty}{p}$.
(4) Show that $\lim\limits_{n \to \infty} a_n(f) = 0$.
(5) Show that $f = \sum\limits_{n=0}^{\infty} a_n(f)\binom{X}{n}$ in $(\mathscr{A}, \|.\|_\infty)$.
(6) Show that $\|f\|_\infty = \sup\limits_{n \in \mathbf{Z}_{\geqslant 0}} |a_n(f)|_p$.

Exercise 6.6.15. Show that $\sum\limits_{n=0}^{\infty} \binom{1/2}{n}\left(\frac{7}{9}\right)^n = -\frac{4}{3}$ in $\mathbf{Q}_7$. Compute $\sum\limits_{n=0}^{\infty} \binom{1/2}{n}\left(\frac{7}{9}\right)^n$ in $\mathbf{R}$.

Exercise 6.6.16. Prove that $\mathsf{AH}(X)$ converges in $\mathrm{D}(0,1)$ but not in $\overline{\mathrm{D}}(0,1)$ (hint: compute $\frac{\mathsf{AH}'(X)}{\mathsf{AH}(X)}$).

Exercise 6.6.17. Find the coefficients in $\mathsf{AH}(X)$ through the X^{p-1} term.

Exercise 6.6.18. Use Dwork's lemma to show that $\mathsf{AH}(X) \in \mathbf{Z}_p[\![X]\!]$.

Exercise 6.6.19. A slight generalization of previous exercise. Let $g(X) = \sum\limits_{i=0}^{\infty} b_i X^{p^i} \in \mathbf{Q}_p[\![X]\!]$. Show that $\exp(g(X)) \in 1 + X\,\mathbf{Z}_p[\![X]\!]$ if and only if $b_{i-1} - pb_i \in p\,\mathbf{Z}_p$ for all $i \in \mathbf{Z}_{\geqslant 0}$ (with $b_{-1} := 0$).

7. Rational points

7.1. **Equations over a finite field.** Let p be a prime number, $r \in \mathbf{Z}_{>0}$ and $q = p^r$. If $I \subset \mathbf{F}_q[X_1, \ldots, X_n]$ is an ideal, we denote by

$$\mathsf{V}(I) = \{\mathbf{x} \in \mathbf{F}_q^n \,;\, (\forall P \in I)\, P(\mathbf{x}) = 0\} \subset \mathbf{A}^n(\mathbf{F}_q).$$

its set of zeros in $\mathbf{F}_q^n$. A quite important problem is to determine if $\mathsf{V}(I) \neq \varnothing$, or better understand $\#\mathsf{V}(I)$. In what follows we provide partial (and classical) results in special cases.

Lemma 7.1.1. If $n \in \mathbf{Z}_{\geqslant 0}$, we put $s(n) = \sum\limits_{x \in \mathbf{F}_q} x^n$. We have $s(n) = \begin{cases} -1 & \text{if } n > 0 \text{ and } q-1 \mid n \\ 0 & \text{otherwise} \end{cases}$.

Proof. • Assume $n > 0$ and $q - 1 \mid n$: we have $x^n = 1$ for all $x \in \mathbf{F}_q^\times$ (since the latter has order $q - 1$), and $x^n = 0$ if $x = 0$, so that $s(n) = \sum\limits_{x \in \mathbf{F}_q^\times} 1 = q - 1 = -1$.

• If $n = 0$, we have $x^n = 1$ for all $x \in \mathbf{F}_q$, so that $s(0) = \sum\limits_{x \in \mathbf{F}_q} 1 = q = 0$.

• Assume $n > 0$ and $q-1 \nmid n$. The group $\mathbf{F}_q^\times$ is cyclic: let ω be a generator. Then $s(n) = \sum\limits_{x \in \mathbf{F}_q^\times} x^n = \sum\limits_{k=0}^{q-2} \omega^{nk}$, hence $\omega^n s(n) = s(n)$, *i.e.* $(1 - \omega^n)s(n) = 0$. As $q - 1 \nmid n$, we have $\omega^n \neq 1$, whence $s(n) = 0$. □

Theorem 7.1.2. (Chevalley-Warning). Let $(P_i)_{1 \leqslant i \leqslant r} \in \mathbf{F}_q[X_1, \ldots, n]^r$ and

$$V = \mathsf{V}(\langle P_1, \ldots, P_r \rangle) = \{\mathbf{x} \in \mathbf{F}_q^n \,;\, (\forall i \in \{1, \ldots, r\})\, P_i(\mathbf{x}) = 0\} \subset \mathbf{A}^n(\mathbf{F}_q).$$

Assume that $\sum\limits_{i=1}^{r} \deg(P_i) < n$. Then $p \mid \#V$.

Proof. Put $P = \prod\limits_{i=1}^{r} (1 - P_i^{q-1}) \in \mathbf{F}_q[X_1, \ldots, X_n]$. If $\mathbf{x} \in \mathbf{F}_q^n$, we have

$$P(\mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{x} \in V \\ 0 & \text{otherwise} \end{cases}.$$

(if $P_i(\mathbf{x}) \neq 0$, we have $P_i(\mathbf{x})^{q-1} = 1$, whence $P(\mathbf{x}) = 0$). This means that P, seen as a map on $\mathbf{F}_q^n$ with values in $\{0, 1\}$ is the characteristic map of V. This implies that $\sum\limits_{\mathbf{x} \in \mathbf{F}_q^n} P(\mathbf{x})$ is the image of $\#V$ in $\mathbf{F}_q$: we have to check that $\sum\limits_{\mathbf{x} \in \mathbf{F}_q^n} P(\mathbf{x}) = 0$. The hypothesis implies that $\deg(P) < (q - 1)n$, which implies that P is an $\mathbf{F}_q$-linear combination of monomials $X_1^{d_1} \cdots X_n^{d_n}$ with $d_1 + \cdots + d_n < (q-1)n$, in particular so that there exists $i \in \{1, \ldots, n\}$ such that $d_i < q-1$. By lemma 7.1.1, we have then $\sum\limits_{\mathbf{x} \in \mathbf{F}_q^n} x_1^{d_1} \cdots x_n^{d_n} = s(d_1) \cdots s(d_n) = 0$, implying the theorem. □

Corollary 7.1.3. Under the hypothesis of the previous theorem, if the polynomials $P_1, \ldots, P_n$ have no constant term, they have a non trivial common zero.

Example 7.1.4. A non degenerate quadratic form over $\mathbf{F}_q$ in more than 3 variables has a nonzero isotropic vector.

Remark 7.1.5. The bound $\sum\limits_{i=1}^{r} \deg(P_i) < n$ is optimal: if $\mathsf{N}\colon \mathbf{F}_{q^n} \to \mathbf{F}_q$ is the norm map, then N is a polynomial map in n variables which is homogeneous of degree n, and $V = \{0\}$ has cardinality prime to p.

7.1.6. *Counting solutions using trigonometric sums.* Here we assume that $r = 1$, *i.e.* $q = p$. Choose $\zeta \in \mathbf{C}$ a primitive p-th root of unity.

Lemma 7.1.7. If $x \in \mathbf{F}_p$, we have

$$\sum_{y \in \mathbf{F}_p} \zeta^{xy} = \begin{cases} p & \text{if } x = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Proof. We have $\zeta^x = 1$ if $x = 0$ and ζ^x is a primitive p-th root of unity if $x \neq 0$: the lemma follows from $\sum\limits_{y \in \mathbf{F}_p} \zeta^y = \sum\limits_{k=0}^{p-1} \zeta^k = 0$. □

Proposition 7.1.8. Let $P \in \mathbf{F}_p[X_1, \dots, X_n]$. Then

$$\# \mathsf{V}(\langle P\rangle) = \frac{1}{p} \sum_{\substack{x \in \mathbf{F}_p \\ \mathbf{x} \in \mathbf{F}_p^n}} \zeta^{xP(\mathbf{x})} = p^{n-1} + \frac{1}{p} \sum_{\substack{x \in \mathbf{F}_p^\times \\ \mathbf{x} \in \mathbf{F}_p^n}} \zeta^{xP(\mathbf{x})}$$

Proof. Follows from lemma 7.1.7. □

In general, controlling the "error term" $\frac{1}{p} \sum\limits_{\substack{x \in \mathbf{F}_p^\times \\ \mathbf{x} \in \mathbf{F}_p^n}} \zeta^{xP(\mathbf{x})}$ is quite hard and the general statement for this is Weil conjectures (*cf* remark 7.2.9). Following [3, I §2 (2)], we will treat the case of diagonal hypersurfaces, *i.e.* that where

$$P(X_1, \dots, X_n) = a_1 X_1^{d_1} + \cdots + a_n X_n^{d_n}$$

where $(a_1, \dots, a_n) \in \mathbf{F}_p^n \backslash \{0\}$.

Definition 7.1.9. (1) A *character* of a finite abelian group G is a group homomorphism $\chi \colon G \to \mathbf{C}^\times$. Such a character has values in the group of $\#G$-th roots of unity.
(2) Let $\chi \colon \mathbf{F}_p^\times \to \mathbf{C}^\times$ be a character. We extend it into a map $\chi \colon \mathbf{F}_p \to \mathbf{C}$ by putting

$$\chi(0) = \begin{cases} 1 & \text{if } \chi \text{ is trivial} \\ 0 & \text{otherwise} \end{cases}.$$

Note that $\chi(xy) = \chi(x)\chi(y)$ for all $x, y \in \mathbf{F}_p$. If $a \in \mathbf{F}_p$, we put

$$\tau_a(\chi) = \sum_{x \in \mathbf{F}_p} \chi(x) \zeta^{ax} \in \mathbf{C}$$

(*Gauss sum*).

Proposition 7.1.10. We have $|\tau_a(\chi)| = \begin{cases} \sqrt{p} & \text{if } \chi \neq \mathbf{1} \text{ and } a \in \mathbf{F}_p^\times \\ 0 & \text{otherwise} \end{cases}.$

Proof. • Assume $\chi \neq \mathbf{1}$ and $a \in \mathbf{F}_p^\times$. We have $|\tau_a(\chi)|^2 = \sum\limits_{x, y \in \mathbf{F}_p^\times} \chi(x)\overline{\chi(y)}\zeta^{a(x-y)}$. As $|\chi(y)| = 1$, we have $\overline{\chi(y)} = \chi(y)^{-1} = \chi(y^{-1})$ for all $y \in \mathbf{F}_p^\times$. This implies that

$$|\tau_a(\chi)|^2 = \sum_{x, y \in \mathbf{F}_p^\times} \chi(xy^{-1})\zeta^{a(x-y)} = \sum_{z \in \mathbf{F}_p^\times} \sum_{y \in \mathbf{F}_p^\times} \chi(z) \zeta^{a(z-1)y}$$

By lemma 7.1.7, we have $\sum\limits_{y \in \mathbf{F}_p^\times} \zeta^{a(z-1)y} = -1$ unless $z = 1$, in which case it is equal to $p-1$. This implies that

$$|\tau_a(\chi)|^2 = p - 1 - \sum_{z \in \mathbf{F}_p^\times \backslash \{1\}} \chi(z) = p - \sum_{z \in \mathbf{F}_p^\times} \chi(z)$$

As χ is non trivial, we have $\sum\limits_{z \in \mathbf{F}_p^\times} \chi(z) = 0$, whence $|\tau_a(\chi)|^2 = p$, *i.e.* $|\tau_a(\chi)| = \sqrt{p}$.

• We have $\tau_a(\mathbf{1}) = 0$ by lemma 7.1.7. We have $\tau_0(\chi) = \sum\limits_{x \in \mathbf{F}_p} \chi(x) = 0$ if $\chi \neq \mathbf{1}$. □

Theorem 7.1.11. We have $\left|\# \mathsf{V}(\langle P\rangle) - p^{n-1}\right| \leqslant C(p-1)p^{\frac{n}{2}-1}$ with $C = \prod\limits_{i=1}^{n} (\delta_i - 1)$ where $\delta_i = \mathsf{gcd}(d_i, p-1)$ for $i \in \{1, \dots, n\}$.

Proof. By proposition 7.1.8, we have

$$(*) \qquad p\big(\# \mathsf{V}(\langle P\rangle) - p^{n-1}\big) = \sum_{\substack{x \in \mathbf{F}_p^\times \\ \mathbf{x} \in \mathbf{F}_p^n}} \zeta^{x(a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n})} = \sum_{x \in \mathbf{F}_p^\times} \prod_{i=1}^{n} \Sigma_\zeta(x a_i, d_i)$$

where $\Sigma_\zeta(a, d) = \sum\limits_{y \in \mathbf{F}_p} \zeta^{ay^d} = \sum\limits_{z \in \mathbf{F}_p} m_d(z) \zeta^{az}$ with $m_d(z) = \#\{y \in \mathbf{F}_p \, ; \, y^d = z\}$.

We have $m_d(0) = 1$. Let $z \in \mathbf{F}_p^\times$. If ω is a generator of the cyclic group $\mathbf{F}_p^\times$, we can write $z = \omega^k$ for a unique $k \in \{0, \dots, p-2\}$. Writing $y = \omega^u$, we have $y^d = z \Leftrightarrow du \equiv k \mod (p-1)\mathbf{Z}$. If $\delta = \mathsf{gcd}(d, p-1)$, a necessary condition for the existence of such u is that $\delta \mid k$, in which case the congruence is equivalent to $\frac{d}{\delta}u \equiv \frac{k}{\delta} \mod \frac{p-1}{\delta}\mathbf{Z}$: as $\frac{d}{\delta}$ is prime to $\frac{p-1}{\delta}$ hence invertible mod $\frac{p-1}{\delta}$, this last congruence has a unique solution modulo $\frac{p-1}{\delta}$, hence δ solutions mod $p-1$. This shows that

$$m_d(z) = \begin{cases} \delta & \text{if } \delta \mid k \\ 0 & \text{otherwise} \end{cases}.$$

Let $\varepsilon \in \mathbf{C}$ be a primitive δ-th root of unity. If $s \in \{0, \ldots, \delta-1\}$ and $x \in \mathbf{F}_p^\times$, let

$$\chi_s \colon \mathbf{F}_p^\times \to \mathbf{C}^\times$$

be the character defined by $\chi_s(\omega) = \varepsilon^s$ (this makes sense since ε^s is a $p-1$-th root of unity, because $\delta \mid p-1$). Let $z = \omega^k \in \mathbf{F}_p^\times$ with $\delta \mid k$, we have $\chi_s(z) = \varepsilon^{sk} = 1$ for all $s \in \{0, \ldots, \delta-1\}$, so that $\sum\limits_{s=0}^{\delta-1} \chi_s(z) = \delta$. If $\delta \nmid k$, we have $(\varepsilon^k - 1)\sum\limits_{s=0}^{\delta-1} \chi_s(z) = \varepsilon^{\delta k} - 1 = 0$, hence $\sum\limits_{s=0}^{\delta-1} \chi_s(z) = 0$ since $\varepsilon^k \neq 1$. In any case we have

$$m_d(z) = \sum_{s=0}^{\delta-1} \chi_s(z)$$

What precedes thus imply $\Sigma_\zeta(a,d) = \sum\limits_{z\in\mathbf{F}_p}\sum\limits_{s=0}^{\delta-1} \chi_s(z)\zeta^{az} = \sum\limits_{s=0}^{\delta-1} \tau_a(\chi_s) = \sum\limits_{s=1}^{\delta-1} \tau_a(\chi_s)$ (since $\tau_a(\delta_0) = \tau_a(\mathbf{1}) = 0$ by proposition 7.1.10). In particular, we have $|\Sigma_\zeta(a,d)| \leqslant \sum\limits_{s=1}^{\delta-1} |\tau_a(\chi_s)| = (\delta-1)\sqrt{p}$. Thus equation $(*)$ implies that

$$p\left|\#\mathsf{V}(\langle P\rangle) - p^{n-1}\right| = \sum_{x\in\mathbf{F}_p^\times}\prod_{i=1}^n \left((\delta_i - 1)\sqrt{p}\right) = (p-1)\Big(\prod_{i=1}^n (\delta_i - 1)\Big)p^{\frac{n}{2}}$$

hence the result. □

7.2. **Rationality of Zeta functions of schemes of finite type over finite fields.** What follows is taken almost verbatim from [19]. Other references are [13, Chapter V] and [8, Chapter II]. Let q be a power of a prime p, and V a $\mathbf{F}_q$-scheme of finite type. Denote by $|V|$ the set of closed points of V.

Definition 7.2.1. If $x \in |V|$, the corresponding residue field $\kappa(x)$ is a finite extension of $\mathbf{F}_q$. The *degree* of x is then $\deg(x) = [\kappa(x) : \mathbf{F}_q]$.

Remark 7.2.2. A point of V with values in $\mathbf{F}_{q^d}$ is a morphism of $\mathbf{F}_q$-schemes $\mathsf{Spec}(\mathbf{F}_{q^d}) \to X$. The data of such a point is equivalent to its image in the topological space V, which is a closed point $x \in |V|$, and a local morphism of $\mathbf{F}_q$-algebras $\mathcal{O}_{V,x} \to \mathbf{F}_{q^d}$, *i.e.* a $\mathbf{F}_q$-linear morphism $\kappa(x) \to \mathbf{F}_{q^d}$. The closed point x being fixed, there are $\deg(x)$ such morphisms, *i.e.* $\deg(x)$ points. The set of points with values in $\mathbf{F}_{q^d}$ is denoted $V(\mathbf{F}_{q^d})$.

Lemma 7.2.3. For all $k \in \mathbf{Z}_{\geqslant 1}$, the set $V(\mathbf{F}_{q^k})$ is finite.

Proof. Being of finite type over $\mathbf{F}_q$, the scheme V can be covered by finitely many affine $\mathbf{F}_q$-schemes: write $V = \bigcup\limits_{i=1}^r \mathsf{Spec}(A_i)$ where A_i is a $\mathbf{F}_q$-algebra of finite type for $i \in \{1, \ldots, r\}$. If $x \in |V|$, there exists $i \in \{1, \ldots, r\}$ such that $x \in \mathsf{Spec}(A_i)$. If x is the image of an element of $\mathsf{V}(\mathbf{F}_{q^k})$, it corresponds to the kernel of a morphism of $\mathbf{F}_q$-algebras $A_i \to \mathbf{F}_{q^k}$ (*cf* remark 7.2.2). As A_i is a quotient of $\mathbf{F}_q[X_1, \ldots, X_{n_r}]$ for some $n_r \in \mathbf{Z}_{\geqslant 0}$, there are finitely many such morphisms, *a fortiori* finitely many such closed points. Each of these corresponding to at most k morphisms $\mathcal{O}_{V,x} \to \mathbf{F}_{q^k}$, this shows the finiteness of $V(\mathbf{F}_{q^k})$. □

Definition 7.2.4. The *zeta function* of V is

$$\mathsf{Z}_V(T) = \prod_{x\in|V|} \frac{1}{1 - T^{\deg(x)}} \in \mathbf{Z}[\![T]\!].$$

Observe that the product converges in $\mathbf{Z}[\![T]\!]$ thanks to the previous lemma.

Lemma 7.2.5. We have $\mathsf{Z}_V(T) = \exp\Big(\sum\limits_{k=1}^\infty \#V(\mathbf{F}_{q^k})\frac{T^k}{k}\Big)$.

Proof. Taking the logarithm in $\mathbf{Q}[\![T]\!]$, we have

$$\ln(\mathsf{Z}_V(T)) = \sum_{x\in|V|} -\ln\left(1 - T^{\deg(x)}\right) = \sum_{x\in|V|}\sum_{n=1}^\infty \frac{T^{n\deg(x)}}{n} = \sum_{k=1}^\infty N_k(V)\frac{T^k}{k}$$

where $N_k(V) = \sum\limits_{\substack{x\in|V|\\ \deg(x)|k}} \deg(x) = \#V(\mathbf{F}_{q^k})$ by remark 7.2.2. □

Example 7.2.6. (1) If $V = \mathbf{A}^n_{\mathbf{F}_q}$, we have $\#V(\mathbf{F}_{q^k}) = q^{nk}$ for $k \in \mathbf{Z}_{>0}$, so $\sum\limits_{k=1}^{\infty} \#V(\mathbf{F}_{q^k})\frac{T^k}{k} = -\ln(1-q^nT)$, hence $\mathsf{Z}_{\mathbf{A}^n_{\mathbf{F}_q}}(T) = \frac{1}{1-q^nT}$.
(2) As we have $\mathbf{P}^n_{\mathbf{F}_q} = \mathbf{A}^n_{\mathbf{F}_q} \sqcup \mathbf{P}^{n-1}_{\mathbf{F}_q}$, a straightforward induction gives $\mathsf{Z}_{\mathbf{P}^n_{\mathbf{F}_q}}(T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^nT)}$.

Lemma 7.2.7. If V is the union of two subschemes V' and V'', then $\mathsf{Z}_V(T) = \frac{\mathsf{Z}_{V'}(T)\,\mathsf{Z}_{V''}(T)}{\mathsf{Z}_{V'\cap V''}(T)}$.

Proof. Obvious. □

Theorem 7.2.8. (Dwork) $\mathsf{Z}_V(T) \in \mathbf{Q}(T)$.

Remark 7.2.9. (1) In fact, one has $\mathsf{Z}_V(T) = \frac{P(T)}{Q(T)}$ where $P(T), Q(T) \in \mathbf{Z}[T]$ have constant term equal to 1. Indeed, theorem 7.2.8 shows that We can write $\mathsf{Z}_V(T) = \frac{P(T)}{Q(T)}$ where $P(T), Q(T) \in \mathbf{Q}[T]$. We may assume that $\mathsf{gcd}(P,Q) = 1$. As $\mathsf{Z}_V(0) = 1$, we may divide P and Q by their constant terms, and assume that $P(0) = Q(0) = 1$. Let p be a prime number. We have $\mathsf{Z}_V(T) \in \mathbf{Z}[\![T]\!] \subset \mathbf{Z}_p[\![T]\!]$. Assume $P(T) \notin \mathbf{Z}_p[T]$: one coefficient of P has negative valuation, so its Newton polygon has a negative slope. This implies that P has a root $\lambda \in \mathrm{D}(0,1)$. As $Q(T) = P(T)\,\mathsf{Z}_V(T)$ and $\mathsf{Z}_V(T)$ converges on $\mathrm{D}(0,1)$ (because it has integral coefficients), we have $Q(\lambda) = 0$ as well, contradicting the fact that $\mathsf{gcd}(P,Q) = 1$. This shows that $P(T) \in \mathbf{Z}_p[T]$, so that $Q(T) = P(T)\,\mathsf{Z}_V(T) \in \mathbf{Z}_p[T]$. This means that the coefficients of P and Q have non-negative p-adic valuations for all primes p: they are integers.
(2) This result is the first of *Weil conjectures*. There are the following. Assume that V is a projective and geometrically irreducible[45] and smooth over $\mathbf{F}_q$. Then the following hold:

- (Functional equation) we have
$$\mathsf{Z}_V(q^{-d}T^{-1}) = \pm q^{\frac{de}{2}}T^e\,\mathsf{Z}_V(T)$$
where $d = \dim(V)$ and e is the "Euler characteristic" of V;
- (Riemann hypothesis) we can write
$$\mathsf{Z}_V(T) = \frac{P_1(T)P_3(T)\cdots P_{2d-1}(T)}{P_0(T)P_2(T)\cdots P_{2d}(T)}$$
where $P_j(T) \in \mathbf{Z}[T]$ are such that $P_0(T) = 1-T$ and $P_{2d}(T) = 1-q^dT$ and $P_j(T) = \prod\limits_{i=1}^{b_j}(1-\alpha_{i,j}T)$ where[46] $|\alpha_{i,j}| = q^{j/2}$ for all $i \in \{1,\dots,b_j\}$.

For instance, if V is a curve of genus g, we have $\mathsf{Z}_V(T) = \frac{P(T)}{(1-T)(1-qT)}$ where $P \in 1 + T\,\mathbf{Z}[T]$ is a polynomial of degree $2g$, whose roots have absolute value $\sqrt{q}$.

7.2.10. *First reductions.*

Lemma 7.2.11. If $d \in \mathbf{Z}_{>0}$, we have $\mathbf{Q}(T) \cap \mathbf{Z}[\![T^d]\!] \subset \mathbf{Q}(T^d)$.

Proof. Let $P, Q \in \mathbf{Q}[X]\backslash\{0\}$ be coprime and such that $\frac{P(T)}{Q(T)} \in \mathbf{Z}[\![T^d]\!]$. We may assume that $Q(0) = 1$. Let $\zeta \in \mathbf{C}$ be a primitive d-th root of unity: the hypothesis implies that $\frac{P(T)}{Q(T)} = \frac{P(\zeta T)}{Q(\zeta T)}$ in $\mathbf{C}(T)$, whence $P(T)Q(\zeta T) = P(\zeta T)Q(T)$ in $\mathbf{C}[T]$. As $\mathsf{gcd}(P,Q) = 1$, Gauss lemma implies that $Q(T) \mid Q(\zeta T)$, whence $Q(T) = Q(\zeta T)$ (since $Q(T)$ and $Q(\zeta T)$ have same degree and same constant term). This shows that $Q(T) = Q(\zeta^k T)$ for all $k \in \mathbf{Z}$, so that $Q(T) = \frac{1}{d}\sum\limits_{k=0}^{d-1} P(\zeta^k T) \in \mathbf{C}[T^d] \cap \mathbf{Q}[T] = \mathbf{Q}[T^d]$ (because $\sum\limits_{k=0}^{d-1}\zeta^{ki} = 0$ unless $d \mid i$). Similarly $P(T) \in \mathbf{Q}[T^d]$, and we are done. □

Lemma 7.2.12. Theorem 7.2.8 follows from the special case where $V = \mathsf{V}(f) \subset \mathbf{A}^n_{\mathbf{F}_p}$ for some polynomial $f(\underline{X}) \in \mathbf{F}_p[X_1,\dots,X_n]$.

[45] *i.e.* such that $V \times_{\mathbf{F}_q} \overline{\mathbf{F}}_q$ is irreducible.

[46] Moreover, if V is the reduction mod $\mathfrak{p}$ of a non singular projective variety $\widetilde{V}$ over a number field K, the integers b_j are precisely the "Betti numbers" of $\widetilde{V}$, *i.e.* the dimensions of the Betti cohomology groups of the topological manifold $\widetilde{V}(\mathbf{C})$.

Proof. • Put $d = [\mathbf{F}_q : \mathbf{F}_p]$. As V is of finite type over $\mathbf{F}_q$, it is of finite type over $\mathbf{F}_p$ as well. If $x \in |V|$, we have $[\kappa(x) : \mathbf{F}_p] = [\kappa(x) : \mathbf{F}_q]d$, so that $\mathsf{Z}_{V/\mathbf{F}_p}(T) = \mathbf{Z}_{V/\mathbf{F}_q}(T^d)$. If the theorem is known for varieties over $\mathbf{F}_p$, this shows that $\mathsf{Z}_{V/\mathbf{F}_q}(T^d) \in \mathbf{Q}(T) \cap \mathbf{Z}\llbracket T^d \rrbracket \subset \mathbf{Q}(T^d)$ by lemma 7.2.11, so that $\mathsf{Z}_{V/\mathbf{F}_q}(T) \in \mathbf{Q}(T)$. This implies that to prove theorem 7.2.8, we may restrict to the case where $q = p$ is prime.

• As V is of finite type over $\mathbf{F}_p$, we have $X = \bigcup\limits_{i=1}^{r} V_i$ where $V_1, \dots, V_r$ are affine open subschemes. By lemma 7.2.7, we have

$$\mathsf{Z}_V(T) = \prod_{\substack{I \subset \{1,\dots,r\} \\ I \neq \varnothing}} \mathsf{Z}_{V_I}(T)^{(-1)^{\#I}}$$

where $V_I = \bigcap\limits_{i \in I} V_i$ for all $I \subset \{1, \dots, r\}$. It is enough to show that $\mathsf{Z}_{V_I}(T) \in \mathbf{Q}(T)$ when $I \neq \varnothing$. As V_I is a subscheme of an affine hence separated scheme when $I \neq \varnothing$, we can reduce to the case reduce to the case where V is separated. In that case, the intersections V_I are affine (*cf* [15, Chap. 3.3, Prop. 3.6]): we are reduced to the case when V is affine, *i.e.* $V = \mathsf{V}(I) \subset \mathbf{A}^n_{\mathbf{F}_p}$ where $I = \langle f_1, \dots, f_m \rangle \subset \mathbf{F}_p[X_1, \dots, X_n]$ is an ideal. Assume $m > 1$: let $V' = \mathsf{V}(\langle f_1, \dots, f_{m-1} \rangle)$ and $V'' = \mathsf{V}(f_m)$. Then $V = V' \cap V''$: by lemma 7.2.7, we have $\mathsf{Z}_V(T) = \frac{\mathsf{Z}_{V'}(T)\,\mathsf{Z}_{V''}(T)}{\mathsf{Z}_{V' \cup V''}(T)}$. As $V' \cup V'' = \mathsf{V}(\langle f_1, \dots, f_{m-1} \rangle f_m)$, a straightforward induction reduces to the case where $m = 1$, *i.e.* where $V = \mathsf{V}(f) \subset \mathbf{A}^n_{\mathbf{F}_p}$ for some polynomial $f(\underline{X}) \in \mathbf{F}_p[X_1, \dots, X_n]$. □

If $f(\underline{X}) \in \mathbf{F}_p[X_1, \dots, X_n]$, put

$$\widetilde{\mathsf{V}}(f) = \mathsf{V}(f) \cap \mathrm{D}(X_1 \cdots X_n) \subset \mathbf{A}^n_{\mathbf{F}_p}.$$

A point of $f(\underline{X})$ with values in $\mathbf{F}_q$ thus corresponds to the data of an element $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{F}_q^n$ such that $f(x_1, \dots, x_n) = 0$ and $x_1 \cdots x_n \neq 0$.

Lemma 7.2.13. Theorem 7.2.8 follows from the special case where $V = \widetilde{\mathsf{V}}(f) \subset \mathbf{A}^n_{\mathbf{F}_p}$ for some polynomial $f(\underline{X}) \in \mathbf{F}_p[X_1, \dots, X_n]$.

Proof. By lemma 7.2.12, we already reduced the proof to the case where $V = \mathsf{V}(f)$ for some polynomial $f(\underline{X}) \in \mathbf{F}_p[X_1, \dots, X_n]$. Now we have

$$\mathsf{V}(f) = \widetilde{\mathsf{V}}(f) \sqcup (\mathsf{V}(f) \cap \mathsf{V}(X_1 \cdots X_n)).$$

By lemma 7.2.7, the rationality of $\mathsf{Z}_{\mathsf{V}(f)}$ follows from that of $\mathsf{Z}_{\widetilde{\mathsf{V}}(f)}$ and that of $\mathsf{Z}_{\mathsf{V}(F) \cap \mathsf{V}(X_1 \cdots X_n)}$. As we have $\mathsf{V}(f) \cap \mathsf{V}(X_1 \cdots X_n) = \bigcup\limits_{i=1}^{n} \mathsf{V}(f) \cap \mathsf{V}(X_i)$, this reduces to that of $\mathsf{Z}_{\widetilde{\mathsf{V}}(f)}$ and of the zeta functions of the various intersections of the $\mathsf{V}(f) \cap \mathsf{V}(X_i)$. As those identify with subschemes of $\mathbf{A}^{n-1}_{\mathbf{F}_p}$, we can use induction on n to reduce to the rationality of $\mathsf{Z}_{\widetilde{\mathsf{V}}(f)}$. □

7.2.14. *Factorization of additive characters on finite fields.* Recall that in section 6.4.17, we defined the series $B(X, Y) = \sum\limits_{n=0}^{\infty} \binom{X}{n} Y^n = (1 + Y)^X \in \mathbf{Q}\llbracket X, Y \rrbracket$ and Dwork's series

$$F(X, Y) = B(X, Y) \prod_{i=1}^{\infty} B\Big(\tfrac{X^{p^i} - X^{p^{i-1}}}{p^i}, Y^{p^i}\Big) \in \mathbf{Z}_p\llbracket X, Y \rrbracket$$

(*cf* proposition 6.4.20). Formally, we have

$$F(X, Y) = \prod_{i=0}^{\infty} (1 + Y^{p^i})^{\frac{X^{p^i} - X^{p^{i-1}}}{p^i}}$$

Write

$$F(X, Y) = \sum_{m=0}^{\infty} B_m(X) Y^m.$$

In each monomial of factor $B\Big(\frac{X^{p^i} - X^{p^{i-1}}}{p^i}, Y^{p^i}\Big)$, the degree in X is less or equal to that of Y: this thus holds also for $F(X, Y)$. This implies that $\deg(B_m) \leqslant m$ for all $m \in \mathbf{Z}_{\geqslant 0}$. This shows in particular that we have

$$F(X, Y) = \sum_{m=0}^{\infty} X^m \alpha_m(Y)$$

where $\alpha_m(Y) \in Y^m\,\mathbf{Z}_p\llbracket Y \rrbracket$.

Fix $\varepsilon \in \mathbf{C}_p$ be a primitive p-th root of unity and let $\lambda = \varepsilon - 1$: we have $\lambda \neq 0$, so that $0 = \frac{\varepsilon^p - 1}{\varepsilon - 1} = \frac{(1+\lambda)^p - 1}{\lambda}$, so that $\lambda^{p-1} + \sum\limits_{k=1}^{p-2} \binom{p}{k} \lambda^{k-1} + p = 0$. This shows that $v_p(\lambda) > 0$, hence $v_p\big(\binom{p}{k}\lambda^{k-1}\big) > 1$ for $k \in \{1, \ldots, p-2\}$, so that $v_p(\lambda^{p-1}) = 1$, *i.e.* $v_p(\lambda) = \frac{1}{p-1}$. Put

$$\Theta(X) = F(X, \lambda) = \sum_{m=0}^{\infty} \beta_m X^m$$

where $\beta_m = \alpha_m(\lambda) \in \mathbf{Z}_p[\lambda] = \mathbf{Z}_p[\varepsilon]$. Note that $v_p(\beta_m) \geqslant \frac{m}{p-1}$ since $\alpha_m(Y) \in Y^m \mathbf{Z}_p[\![Y]\!]$. This implies that the radius of convergence of Θ is larger that $p^{\frac{1}{p-1}} > 1$, *i.e.* that Θ converges on $\mathrm{D}\big(0, p^{\frac{1}{p-1}}\big)$.

If $k \in \mathbf{Z}_{>0}$ and $t \in \mathbf{F}_{p^k}$, we have $\mathsf{Tr}_{\mathbf{F}_{p^k}/\mathbf{F}_p}(t) = \sum\limits_{j=0}^{k-1} t^{p^j} \in \mathbf{F}_p$, so that $\varepsilon^{\mathsf{Tr}_{\mathbf{F}_{p^k}/\mathbf{F}_p}(t)}$ makes sense, and defines a character

$$\begin{aligned} \varepsilon^{\mathsf{Tr}_{\mathbf{F}_{p^k}/\mathbf{F}_p}} \colon \mathbf{F}_{p^k} &\to \mathbf{C}_p^\times \\ t &\mapsto \varepsilon^{\mathsf{Tr}_{\mathbf{F}_{p^k}/\mathbf{F}_p}(t)} \end{aligned}$$

Recall that the Teichmüller lift of t is the unique element $[t] \in \mathcal{O}_{\overline{\mathbf{Q}}_p}$ that lifts $t \in \overline{\mathbf{F}}_p$ and such that $[t]^{p^k} = [t]$ (*cf* definition 3.8.20). The following statement provides an analytic expression of this character (more precisely its expression as the value at $[t] \in \mathcal{O}_{\mathbf{C}_p}$ of an analytic map defined on $\mathrm{D}\big(0, p^{\frac{1}{p-1}}\big)$).

Proposition 7.2.15. For all $t \in \mathbf{F}_{p^k}$, we have

$$\varepsilon^{\mathsf{Tr}_{\mathbf{F}_{p^k}/\mathbf{F}_p}(t)} = \Theta([t])\Theta([t^p]) \cdots \Theta([t^{p^{k-1}}]).$$

Proof. The equality $\mathsf{Tr}_{\mathbf{F}_{p^k}/\mathbf{F}_p}(t) = \sum\limits_{j=0}^{k-1} t^{p^j} \in \mathbf{F}_p$ is the reduction modulo $\mathfrak{m}_{\overline{\mathbf{Q}}_p}$ of

$$\mathsf{Tr}_k([t]) := \sum_{j=0}^{k-1} [t]^{p^j} \in \mathbf{Z}_p$$

so that $\varepsilon^{\mathsf{Tr}_{\mathbf{F}_{p^k}/\mathbf{F}_p}(t)} = \varepsilon^{\mathsf{Tr}_k([t])} = B(\mathsf{Tr}_k([t]), \lambda)$.
On the other hand, $B(\mathsf{Tr}_k([t]), Y) = (1+Y)^{\mathsf{Tr}_k([t])} = \prod\limits_{j=0}^{k-1} B([t]^{p^j}, Y)$ in $\mathbf{C}_p[\![Y]\!]$. Moreover, we have

$$F([t]^{p^j}, Y) = B([t]^{p^j}, Y) \prod_{i=1}^{\infty} B\big(\tfrac{[t]^{p^{i+j}} - [t]^{p^{i+j-1}}}{p^i}, Y\big)$$

for all $j \in \{0, \ldots, k-1\}$. Multiplying all those equalities in $\mathbf{C}_p[\![Y]\!]$ gives

$$\begin{aligned} \prod_{j=0}^{k-1} F([t]^{p^j}, Y) &= \Big(\prod_{j=0}^{k-1} B([t]^{p^j}, Y)\Big) \prod_{i=1}^{\infty} \Big(\prod_{j=0}^{k-1} B\big(\tfrac{[t]^{p^{i+j}} - [t]^{p^{i+j-1}}}{p^i}, Y\big)\Big) \\ &= \Big(\prod_{j=0}^{k-1} B([t]^{p^j}, Y)\Big) \prod_{i=1}^{\infty} B\Big(\tfrac{1}{p^i} \sum_{j=0}^{k-1} \big([t]^{p^{i+j}} - [t]^{p^{i+j-1}}\big), Y\Big) \\ &= \prod_{j=0}^{k-1} B([t]^{p^j}, Y) \end{aligned}$$

in $\mathbf{C}_p[\![Y]\!]$ because $\sum\limits_{j=0}^{k-1} \big([t]^{p^{i+j}} - [t]^{p^{i+j-1}}\big) = 0$ since $[t]^{p^k} = [t]$ and $B(0, y) = 1$. We thus have

$$B(\mathsf{Tr}_k([t]), Y) = \prod_{j=0}^{k-1} F([t]^{p^j}, Y)$$

in $\mathbf{C}_p[\![Y]\!]$. We may evaluate both sides at λ (the LHS because $\mathsf{Tr}_k([t]) \in \mathbf{Z}_p$ and the RHS because the radius of convergence of Θ in greater that $p^{\frac{1}{p-1}}$), and get

$$\varepsilon^{\mathsf{Tr}_{\mathbf{F}_{p^k}/\mathbf{F}_p}(t)} = \Theta([t])\Theta([t^p]) \cdots \Theta([t^{p^{k-1}}]).$$

□

7.2.16. *Spectral theory of an operator in infinite dimension.* Put $\underline{X} = (X_0, \ldots, X_n)$ and let $E = \mathbf{C}_p[\![\underline{X}]\!]$ be the ring of formal power series in the variables $X_0, \ldots, X_n$ with coefficients in $\mathbf{C}_p$.
If $\underline{w} = (w_0, \ldots, w_n) \in \mathbf{Z}_{\geqslant 0}^{n+1}$, put $|\underline{w}| = w_0 + \cdots + w_n \in \mathbf{Z}_{\geqslant 0}$ and $\underline{X}^{\underline{w}} = X_0^{w_0} \cdots X_n^{w_n}$. If $G(\underline{X}) \in E$, the multiplication by $G(\underline{X})$ defines a $\mathbf{C}_p$-linear endomorphism $\mu_{G(\underline{X})} \in \mathsf{End}_{\mathbf{C}_p}(E)$. If $m \in \mathbf{Z}_{\geqslant 0}$, we define an element $\psi_m \in \mathsf{End}_{\mathbf{C}_p}(E)$ by

$$\psi_m\Big(\sum_{\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}} a_{\underline{w}} \underline{X}^{\underline{w}}\Big) = \sum_{\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}} a_{m\underline{w}} \underline{X}^{\underline{w}}.$$

Let

$$\Psi_{m,G} = \psi_m \circ \mu_{G(\underline{X})} \in \mathsf{End}_{\mathbf{C}_p}(E)$$

be the composite. In the canonical basis $\big(\underline{X}^{\underline{w}}\big)_{\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}}$, the (infinite) matrix of $\Psi_{m,G}$ is $(g_{m\underline{w}-\underline{u}})_{\underline{u},\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}}$, where $G(\underline{X}) = \sum\limits_{\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}} g_{\underline{w}} \underline{X}^{\underline{w}}$.

Remark 7.2.17. If $m, m' \in \mathbf{Z}_{\geqslant 2}$, we have $\psi_m \circ \psi_{m'} = \psi_{mm'}$ and $\mu_{G(\underline{X})} \circ \psi_m = \psi_m \circ \mu_{G(\underline{X}^m)}$. Indeed, if $\underline{u} \in \mathbf{Z}_{\geqslant 0}^{n+1}$, we have $\psi_m\big(\underline{X}^{\underline{u}}\big) = \begin{cases} \underline{X}^{\underline{u}/m} & \text{if } m \mid \underline{u} \\ 0 & \text{otherwise} \end{cases}$. Also, we have $\mu_{G(\underline{X}^m)}\big(\underline{X}^{\underline{u}}\big) = \sum\limits_{\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}} g_{\underline{w}} \underline{X}^{m\underline{w}+\underline{u}}$: we get $(\psi_m \circ \mu_{G(\underline{X}^m)})\big(\underline{X}^{\underline{u}}\big) = \sum\limits_{\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}} g_{\underline{w}} \psi_m\big(\underline{X}^{m\underline{w}+\underline{u}}\big) = G\psi_m\big(\underline{X}^{\underline{u}}\big)$ by linearity, so that $\mu_G \circ \psi_m = \psi_m \circ \mu_{G(\underline{X}^m)}$.

Lemma 7.2.18. Assume there exists a constant $C \in \mathbf{R}_{>0}$ such that $v_p(g_{\underline{w}}) \geqslant C\,|\underline{w}|$ for all $\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}$. Then for all $k \in \mathbf{Z}_{>0}$, the series giving the trace of $\Psi_{m,G}^k$ converges, and we have

$$(m^k - 1)^{n+1} \operatorname{Tr}(\Psi_{m,G}^k) = \sum_{\substack{\mathbf{x} \in \mathbf{C}_p^{n+1} \\ \mathbf{x}^{m-1} = \mathbf{1}}} G(\mathbf{x}) G(\mathbf{x}^m) \cdots G(\mathbf{x}^{m^{k-1}})$$

(if $\mathbf{x} = (x_0, \ldots, x_n) \in \mathbf{C}_p^{n+1}$, the condition $\mathbf{x}^{m-1} = \mathbf{1}$ means that $x_i^{m-1} = 1$ for all $i \in \{0, \ldots, n\}$).

Proof. • An immediate induction on k using remark 7.2.17, implies that

$$\begin{aligned} \Psi_{m,G}^k = \Psi_{m,G}^{k-1} \circ \Psi_{m,G} &= \psi_{m^{k-1}} \circ \mu_{G(\underline{X})G(\underline{X}^m)\cdots G(\underline{X}^{m^{k-2}})} \circ \psi_m \circ \mu_G \\ &= \psi_{m^k} \circ \mu_{G(\underline{X}^m)G(\underline{X}^{m^2})\cdots G(\underline{X}^{m^{k-1}})} \circ \mu_G \\ &= \psi_{m^k} \circ \mu_{G(\underline{X})G(\underline{X}^m)G(\underline{X}^{m^2})\cdots G(\underline{X}^{m^{k-1}})} \end{aligned}$$

thus we may replace m by m^k and $G(\underline{X})$ by $G(\underline{X})G(\underline{X}^m)G(\underline{X}^{m^2}) \cdots G(\underline{X}^{m^{k-1}})$, and assume that $k = 1$.
• The matrix of $\Psi_{m,G}$ being $(g_{m\underline{w}-\underline{u}})_{\underline{u},\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}}$, we have $\operatorname{Tr}(\Psi_{m,G}) = \sum\limits_{\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}} g_{(m-1)\underline{w}}$ (the series converges thanks to the hypothesis of the lemma. On the other hand, we have

$$\sum_{\substack{\mathbf{x} \in \mathbf{C}_p^{n+1} \\ \mathbf{x}^{m-1} = \mathbf{1}}} \mathbf{x}^{\underline{w}} = \begin{cases} (m-1)^{n+1} & \text{if } m-1 \mid \underline{w} \\ 0 & \text{otherwise} \end{cases}.$$

This implies that $\sum\limits_{\substack{\mathbf{x} \in \mathbf{C}_p^{n+1} \\ \mathbf{x}^{m-1} = \mathbf{1}}} G(\mathbf{x}) = (m-1)^{n+1} \sum\limits_{\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}} g_{(m-1)\underline{w}}$. □

Assume again the existence of a constant $C \in \mathbf{R}_{>0}$ such that $v_p(g_{\underline{w}}) \geqslant C\,|\underline{w}|$ for all $\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}$. Put

$$\det(\mathsf{Id}_E - T\Psi_{m,G}) := \sum_{d=0}^{\infty} \gamma_d T^d$$

where

$$\gamma_d := (-1)^d \sum_{\substack{\underline{u}_1, \ldots, \underline{u}_d \in \mathbf{Z}_{\geqslant 0}^{n+1} \\ \underline{u}_j \text{ distinct} \\ \sigma \in \mathfrak{S}_d}} \varepsilon(\sigma) \prod_{j=1}^{d} \big(\psi_{m,G}\big)_{\underline{u}_j, \underline{u}_{\sigma(j)}} = (-1)^d \sum_{\substack{\underline{u}_1, \ldots, \underline{u}_d \in \mathbf{Z}_{\geqslant 0}^{n+1} \\ \underline{u}_j \text{ distinct} \\ \sigma \in \mathfrak{S}_d}} \varepsilon(\sigma) \prod_{j=1}^{d} g_{m\underline{u}_{\sigma(j)} - \underline{u}_j}.$$

This sum does converge in $\mathbf{C}_p$ because we have

$$v_p\Big(\varepsilon(\sigma) \prod_{j=1}^{d} g_{m\underline{u}_{\sigma(j)} - \underline{u}_j}\Big) = \sum_{j=1}^{d} v_p(g_{m\underline{u}_{\sigma(j)} - \underline{u}_j}) \geqslant C(m-1) \sum_{j=1}^{d} |\underline{u}_j|$$

Lemma 7.2.19. Let F be a field, $d \in \mathbf{Z}_{>0}$ and $M \in \mathsf{M}_d(F)$. Then $\det(\mathrm{I}_n - TM) = \exp\Big(-\sum\limits_{k=1}^{\infty} \operatorname{Tr}(M^k) \frac{T^k}{k}\Big)$.

Proof. Let $\overline{F}$ be an algebraic closure of F, and $\lambda_1, \ldots, \lambda_d \in \overline{F}$ are the eigenvalues of M. For $k \in \mathbf{Z}_{>0}$ we have $\mathsf{Tr}(M^k) = \sum\limits_{j=1}^{d} \lambda_j^k$, so that $-\sum\limits_{k=1}^{\infty} \mathsf{Tr}(M^k)\frac{T^k}{k} = -\sum\limits_{j=1}^{d}\sum\limits_{k=1}^{\infty} \frac{(\lambda_j T)^k}{k} = \sum\limits_{j=1}^{d} \ln(1-\lambda_j T) = \ln(\det(\mathrm{I}_n - TM))$. □

Lemma 7.2.20. Assume there exists a constant $C \in \mathbf{R}_{>0}$ such that $v_p(g_{\underline{w}}) \geqslant C\,|\underline{w}|$ for all $\underline{w} \in \mathbf{Z}_{\geqslant 0}^{n+1}$. Then we have:

(i) $\det(\mathsf{Id}_E - T\Psi_{m,G}) = \exp\Big(-\sum\limits_{k=1}^{\infty} \mathsf{Tr}\left(\Psi_{m,G}^k\right)\frac{T^k}{k}\Big)$;

(ii) the radius of convergence of the series $\det(\mathsf{Id}_E - T\Psi_{m,G}) \in \mathbf{C}_p[\![T]\!]$ is infinite.

Proof. (i) If $N \in \mathbf{Z}_{>0}$, let $\Psi_{m,G,\leqslant N}$ be the endomorphism of E whose matrix is that of $\Psi_{m,G}$ with entries for which $|\underline{u}| > N$ or $|\underline{w}| > N$ are replaced by 0. Then $\det(\mathrm{I}_E - T\Psi_{m,G,\leqslant N}) = \exp\Big(-\sum\limits_{k=1}^{\infty} \mathsf{Tr}\left(\Psi_{m,G,\leqslant N}^k\right)\frac{T^k}{k}\Big)$ by lemma 7.2.19. Endowing $\mathbf{C}_p[\![T]\!]$ with the topology coefficientwise convergence, the equality follows by passing to the limit as $N \to \infty$.

(ii) It is enough to check that $\lim\limits_{d\to\infty} \frac{v_p(\gamma_d)}{d} = +\infty$. We already know that

$$v_p(\gamma_d) \geqslant C(m-1) \inf_{\substack{\underline{u}_1,\ldots,\underline{u}_d \in \mathbf{Z}_{\geqslant 0}^{n+1} \\ \underline{u}_j \text{ distinct}}} \Big(\sum_{j=1}^{d} |\underline{u}_j|\Big).$$

Order the elements of $\mathbf{Z}_{\geqslant 0}^{n+1}$ into a sequence $(\underline{w}_s)_{s\in\mathbf{Z}_{>0}}$ such that $|\underline{w}_s| \leqslant |\underline{w}_{s+1}|$ for all $s \in \mathbf{Z}_{>0}$. Then we have $v_p(\gamma_d) \geqslant C(m-1)\sum\limits_{s=1}^{d} |\underline{w}_s|$. As $\lim\limits_{s\to\infty} |\underline{w}_s| = +\infty$, we have $\lim\limits_{d\to\infty} \frac{1}{d}\sum\limits_{s=1}^{d} |\underline{w}_s|$ (Cesàro), *i.e.* $\lim\limits_{d\to\infty} \frac{v_p(\gamma_d)}{d} = +\infty$. □

7.2.21. *Analytic expression of the Zeta function and end of the proof.* Recall (*cf* lemma 7.2.13) that we reduced the proof of theorem 7.2.8 to the special case where $q = p$ is prime and $V = \widetilde{\mathsf{V}}(f) \subset \mathbf{A}_{\mathbf{F}_p}^n$ for some polynomial $f(\underline{X}) \in \mathbf{F}_p[X_1, \ldots, X_n]$. If $k \in \mathbf{Z}_{>0}$ we have:

$$\widetilde{\mathsf{V}}(f)(\mathbf{F}_{p^k}) = \big\{(x_1,\ldots,x_n) \in \mathbf{F}_{p^k}^n \,;\, f(x_1,\ldots,x_n) = 0,\ (\forall i \in \{1,\ldots,n\})\, x_i^{p^k-1} = 1\big\}$$

Lemma 7.2.22. The series $\mathsf{Z}_{\widetilde{\mathsf{V}}(f)}(T)$ defines a holomorphic function on the disc $\big\{z \in \mathbf{C}\,;\, |z| < \frac{1}{p^n}\big\}$.

Proof. We have $0 \leqslant \#\widetilde{\mathsf{V}}(f)(\mathbf{F}_{p^k}) \leqslant p^{kn}$ for all $k \in \mathbf{Z}_{>0}$: the radius of convergence of $\sum\limits_{k=1}^{\infty} \#\widetilde{\mathsf{V}}(f)(\mathbf{F}_{p^k})\frac{T^k}{k}$ is at least $\frac{1}{p^n}$, so does that of the series $\mathsf{Z}_{\widetilde{\mathsf{V}}(f)}(T)$. □

According to theorem 6.5.8, theorem 7.2.8 follows if we can show that the series $\mathsf{Z}_{\widetilde{\mathsf{V}}(f)}(T)$ defines a meromorphic function on the disc $\{x \in \mathbf{C}_p\,;\, |z|_p < r\}$ where $\frac{r}{p^n} > 1$. In fact, we have much better:

Theorem 7.2.23. The series $\mathsf{Z}_{\widetilde{\mathsf{V}}(f)}(T)$ defines a meromorphic function on $\mathbf{C}_p$.

Proof. Fix $k \in \mathbf{Z}_{>0}$. If $t \in \mathbf{F}_{p^k}$, we have

$$\Theta_k(t) := \varepsilon^{\mathsf{Tr}_{\mathbf{F}_{p^k}/\mathbf{F}_p}(t)} = \Theta([t])\Theta([t^p])\cdots\Theta([t^{p^{k-1}}]).$$

where $[t] \in \overline{\mathbf{Q}}_p$ is the Teichmüller representative of t (*cf* proposition 7.2.15). As Θ_k is a non-trivial character on $\mathbf{F}_{p^k}$, we have

$$\sum_{x_0\in\mathbf{F}_{p^k}} \Theta_k(x_0 u) = \begin{cases} p^k & \text{if } u = 0 \\ 0 & \text{if } u \neq 0 \end{cases}$$

(the first equality is trivial, for the second, pick $u_0 \in \mathbf{F}_{p^k}$ such that $\Theta_k(u_0) \neq 1$, which is possible since Θ_k is non trivial, then $\Theta_k(u_0)\sum\limits_{x_0\in\mathbf{F}_{p^k}} \Theta_k(x_0 u) = \sum\limits_{x_0\in\mathbf{F}_{p^k}} \Theta_k(x_0 u + u_0) = \sum\limits_{x_0\in\mathbf{F}_{p^k}} \Theta_k(x_0 u)$ because the map $y \mapsto y + u_0$ is a permutation of $\mathbf{F}_{p^k}$). If we apply this to $u = f(\mathbf{x})$ and sum over all values of $\mathbf{x} \in \mathbf{F}_{p^k}^{\times n}$, we get

$$p^k\#\widetilde{\mathsf{V}}(f)(\mathbf{F}_{p^k}) = \sum_{\mathbf{x}\in\mathbf{F}_{p^k}^{\times n}}\sum_{x_0\in\mathbf{F}_{p^k}} \Theta_k(x_0 f(\mathbf{x})) = (p^k-1)^n + \sum_{x_0\in\mathbf{F}_{p^k}^{\times}}\sum_{\mathbf{x}\in\mathbf{F}_{p^k}^{\times n}} \Theta_k(x_0 f(\mathbf{x}))$$

Write $X_0 f(X_1,\ldots,X_n) = \sum\limits_{m=1}^{M} a_m \underline{X}^{\underline{w}_m} \in \mathbf{F}_p[X_0,\ldots,X_n]$ with $a_m \in \mathbf{F}_p$ and $\underline{w}_m = (w_{m,0},\ldots,w_{m,n}) \in \mathbf{Z}_{\geqslant 0}^{n+1}$ for all $m \in \{1,\ldots,M\}$ (here $\underline{X}^{\underline{w}_m} = X_0^{w_{m,0}}\cdots X_n^{w_{m,n}}$). If $x_0 \in \mathbf{F}_{p^k}^{\times}$ and $\mathbf{x} = (x_1,\ldots,x_n) \in \mathbf{F}_{p^k}^{\times n}$, we have

$$\Theta_k(x_0 f(\mathbf{x})) = \prod_{m=1}^{M} \Theta_k\big(a_m \widetilde{\mathbf{x}}^{\underline{w}_m}\big)$$

where $\widetilde{\mathbf{x}}^{\underline{w}_m} = \prod\limits_{i=0}^{n} x_m^{w_{m,i}} \in \mathbf{F}_{p^k}$. The previous equality becomes

$$\begin{aligned} p^k\#\widetilde{\mathsf{V}}(f)(\mathbf{F}_{p^k}) &= (p^k-1)^n + \sum_{\widetilde{\mathbf{x}}\in\mathbf{F}_{p^k}^{\times(n+1)}} \prod_{m=1}^{M} \Theta_k\big(a_m\widetilde{\mathbf{x}}^{\underline{w}_m}\big) \\ &= (p^k-1)^n + \sum_{\widetilde{\mathbf{x}}\in\mathbf{F}_{p^k}^{\times(n+1)}} \prod_{m=1}^{M}\prod_{j=0}^{k-1} \Theta\big(\big[a_i\widetilde{\mathbf{x}}^{p^j\underline{w}_m}\big]\big) \end{aligned}$$

Put

$$G(\underline{X}) = \prod_{m=1}^{M} \Theta\big([a_m]\underline{X}^{\underline{w}_m}\big) \in \mathbf{Z}_p[\varepsilon][\![\underline{X}]\!].$$

The previous equality is then

$$p^k\#\widetilde{\mathsf{V}}(f)(\mathbf{F}_{p^k}) = (p^k-1)^n + \sum_{\widetilde{\mathbf{x}}\in\mathbf{F}_{p^k}^{\times(n+1)}} \prod_{j=0}^{k-1} G\big(\big[\widetilde{\mathbf{x}}^{p^j}\big]\big)$$

Recall the the map Θ converges on the disc $\mathrm{D}\left(0, p^{\frac{1}{p-1}}\right) \subset \mathbf{C}_p$: this implies that the series $G(\underline{X})$ converges on the polydisc $\mathrm{D}\left(0, p^{\frac{1}{p-1}}\right)^{n+1}$. This means that we can write $G(\underline{X}) = \sum\limits_{\underline{w}\in\mathbf{Z}_{\geqslant 0}^{n+1}} g_{\underline{w}}\underline{X}^{\underline{w}} \in \mathbf{C}_p[\![\underline{X}]\!]$ where $v(g_{\underline{w}}) + C\,|\underline{w}| \xrightarrow{+} \infty$ for all $C \in \left]0, \frac{1}{p-1}\right[$. This implies in particular that the hypothesis of lemmas 7.2.18 and 7.2.20 are satisfied by $G(\underline{X})$. By lemma 7.2.18, we thus have

$$\begin{aligned} p^k\#\widetilde{\mathsf{V}}(f)(\mathbf{F}_{p^k}) &= (p^k-1)^n + (p^k-1)^{n+1}\,\mathsf{Tr}(\Psi_G^k) \\ &= \sum_{i=0}^{n}(-1)^i\tbinom{n}{i}p^{k(n-i)} + \sum_{i=0}^{n+1}(-1)^i\tbinom{n+1}{i}p^{k(n+1-i)}\,\mathsf{Tr}(\Psi_G^k) \end{aligned}$$

Multiplying by $\frac{T^k}{k}$, summing over $k \in \mathbf{Z}_{>0}$ gives

$$\begin{aligned} \ln\big(\mathsf{Z}_{\widetilde{\mathsf{V}}(f)}(pT)\big) &= \sum_{i=0}^{n}(-1)^i\tbinom{n}{i}\sum_{k=1}^{\infty}\frac{(p^{n-i}T)^k}{k} + \sum_{i=0}^{n+1}(-1)^i\tbinom{n+1}{i}\sum_{k=1}^{\infty}\mathsf{Tr}(\Psi_G^k)\frac{(p^{n+1-i}T)^k}{k} \\ &= -\sum_{i=0}^{n}(-1)^i\tbinom{n}{i}\ln(1-p^{n-i}T) - \sum_{i=0}^{n+1}(-1)^i\tbinom{n+1}{i}\ln\big(\Delta(p^{n+1-i}T)\big) \end{aligned}$$

where $\Delta(T) = \det(\mathsf{Id} - T\Psi_G) = \exp\Big(-\sum\limits_{k=1}^{\infty}\frac{\mathsf{Tr}(\Psi_G^k)}{k}T^k\Big)$ (*cf* lemma 7.2.20 (i)). Taking exponentials gives thus:

$$\mathsf{Z}_{\widetilde{\mathsf{V}}(f)}(pT) = \Big(\prod_{i=0}^{n}(1-p^{n-i}T)^{(-1)^{i+1}\binom{n}{i}}\Big)\Big(\prod_{i=0}^{n+1}\Delta(p^{n+1-i}T)^{(-1)^{i+1}\binom{n+1}{i}}\Big)$$

As the series Δ is holomorphic on $\mathbf{C}_p$ (*cf* lemma 7.2.20 (ii)), the series $\mathsf{Z}_{\widetilde{\mathsf{V}}(f)}(pT)$ is meromorphic on $\mathbf{C}_p$: so does $\mathsf{Z}_{\widetilde{\mathsf{V}}(f)}(T)$. □

7.3. **Lifting solutions from characteristic p to characteristic 0.** The following is a trivial generalization of Newton's lemma (*cf* theorem 3.3.10):

Theorem 7.3.1. Let $(K, |.|)$ be a complete non archimedean valued field ,$n \in \mathbf{Z}_{>0}$, $P \in \mathcal{O}_K[X_1, \ldots, X_n]$ and $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{O}_K^n$. Assume that there exist $i \in \{1, \ldots, n\}$ and $\varepsilon \in [0, 1[$ such that

$$|P(\mathbf{x})| \leqslant \varepsilon\left|\frac{\partial P}{\partial X_i}(\mathbf{x})\right|^2.$$

Then there exists $\mathbf{x}' = \mathbf{x} + \eta e_i \in \mathcal{O}_K^n$ (where $(e_1, \ldots, e_n)$ is the canonical basis of K^n) such that $P(\mathbf{x}') = 0$ and $|\eta| \leqslant \varepsilon\left|\frac{\partial P}{\partial X_i}(\mathbf{x})\right|$.

Proof. Write $\mathbf{x} = (x_1, \ldots, x_n)$ and put $Q(X) = P(x_1, \ldots, x_{i-1}, X, x_{i+1}, \ldots, x_n) \in \mathcal{O}_K[X]$: we have thus $Q(x_i) = Q(\mathbf{x})$ and $Q'(x_i) = \frac{\partial P}{\partial X_i}(\mathbf{x})$. The hypothesis thus imply that we may apply Newton's lemma to Q at x_i, and find $x_i' = x_i + \eta$ such that $Q(x_i') = 0$ and $|\eta| \leqslant \varepsilon\left|\frac{\partial P}{\partial X_i}(\mathbf{x})\right|$, so that $\mathbf{x}' = (x_1, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_n)$ has the required property. □

Corollary 7.3.2. Let $A = (a_{i,j})_{1\leqslant i,j\leqslant n} \in \mathsf{GL}_n(\mathbf{Z}_p)$ be a symmetric matrix, $q(\underline{X}) = \sum\limits_{1\leqslant i,j\leqslant n} a_{i,j}X_iX_j$ the associated quadratic form on $\mathbf{Q}_p^n$, and $a \in \mathbf{Z}_p$. Let $\mathbf{x} = (x_1,\ldots,x_n) \in \mathbf{Z}_p^3 \backslash p\,\mathbf{Z}_p^n$ be such that $q(\mathbf{x}) \equiv a \mod 4p\,\mathbf{Z}_p$. Then there exists $\mathbf{x}' \in \mathbf{Z}_p^3$ such that $q(\mathbf{x}') = a$ and $\mathbf{x}' \equiv \mathbf{x} \mod 2p\,\mathbf{Z}_p$.

Proof. We have $\frac{\partial q}{\partial X_i}(\mathbf{x}) = 2\sum\limits_{j=1}^{n} a_{i,j}x_j$ for all $i \in \{1,\ldots,n\}$. As $A \in \mathsf{GL}_n(\mathbf{Z}_p)$ and $\mathbf{x} \notin p\,\mathbf{Z}_p^n$, there exists $i \in \{1\ldots,n\}$ such that $\sum\limits_{j=1}^{n} a_{i,j}x_j \in \mathbf{Z}_p^\times$. If $p \neq 2$, this implies that $v_p\big(\frac{\partial q}{\partial X_i}(\mathbf{x})\big) = 0$, so the generalized Newton's lemma (theorem 7.3.1) implies the existence of $\mathbf{x}'$. If $p = 2$, this implies that $v_2\big(\frac{\partial q}{\partial X_i}(\mathbf{x})\big) = 1$: as $v_2(q(\mathbf{x}) - a) \geqslant 3$ the generalized Newton's lemma again implies the existence of $\mathbf{x}'$. □

7.4. **The Hasse principle for quadratic forms.** What follows is almost a mere translation[47] of [22, Chap. III & IV].

7.4.1. *Squares in* $\mathbf{Q}_p^\times$. If $x \in \mathbf{Z}_p$, denote by $\overline{x}$ the image of x in $\mathbf{F}_p$.

Proposition 7.4.2. Let $x \in \mathbf{Q}_p^\times$. Write $x = p^{v_p(x)}u$ with $u \in \mathbf{Z}_p^\times$. Then x is a square in $\mathbf{Q}_p$ if and only if $2 \mid v_p(x)$ and $\big(\frac{\overline{u}}{p}\big) = 1$ (*i.e.* $\overline{u}$ is a square in $\mathbf{F}_p$) and $\overline{u} \equiv 1 \mod 8\,\mathbf{Z}_2$ if $p = 2$.

Proof. • Assume x is a square: write $x = y^2$ with $y \in \mathbf{Q}_p^\times$. We have $y = p^{v_p(y)}v$ with $v \in \mathbf{Z}_p^\times$. Then $p^{v_p(x)}u = p^{2v_p(y)}v$, hence $v_p(x) = 2v_p(y)$ is even, and $u = v^2$ is a square, hence $\overline{u} = \overline{v}^2$ is a square in $\mathbf{F}_p$. If $p = 2$, we have $v \equiv 1 \mod 2\,\mathbf{Z}_2$ hence $u \equiv 1 \mod 8\,\mathbf{Z}_2$.
• Conversely, assume $v_p(x) = 2n$ with $n \in \mathbf{Z}$ and $\overline{u}$ is a square in $\mathbf{F}_p$. Put $P(X) = X^2 - u \in \mathbf{Z}[X]$: there exists $v_0 \in \mathbf{Z}_p^\times$ such that $P(v_0) \in p\,\mathbf{Z}_p$. We have $P'(v_0) = 2v$. If $p \neq 2$, we have $P'(v_0) \in \mathbf{Z}_p^\times$, so Newton's lemma implies that there exists $v \in \mathbf{Z}_p^\times$ such that $P(v) = 0$, so that $x = y^2$ with $y = p^n v$. If $p = 2$, we have $P(v_0) \in 8\,\mathbf{Z}_2$ and $P'(v_0) \in 2\,\mathbf{Z}_2^\times$. By Newton's lemma again, there exists $v \in \mathbf{Z}_2^\times$ such that $P(v) = 0$, which shows that x is a square. □

Notation. If $p = 2$, and $x \in \mathbf{Z}_2^\times$, we have $x \equiv 1 \mod 2\,\mathbf{Z}_2$, so that $x^2 \equiv 1 \mod 8\,\mathbf{Z}_2$. Let $\varepsilon(x)$ (resp. $\omega(x)$) be the image of $\frac{x-1}{2}$ (resp. $\frac{x^2-1}{8}$) in $\mathbf{F}_2$. We have

$$\varepsilon(x) = \begin{cases} 0 & \text{if } x \equiv 1 \mod 4\,\mathbf{Z}_2 \\ 1 & \text{if } x \equiv 3 \mod 4\,\mathbf{Z}_2 \end{cases} \quad\text{and}\quad \omega(x) = \begin{cases} 0 & \text{if } x \equiv \pm 1 \mod 8\,\mathbf{Z}_2 \\ 1 & \text{if } x \equiv \pm 3 \mod 8\,\mathbf{Z}_2 \end{cases}.$$

Corollary 7.4.3. If $p \neq 2$, there are isomorphisms

$$\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2} \simeq (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{F}_p^\times / \mathbf{F}_p^{\times 2}) \xrightarrow{\sim} (\mathbf{Z}/2\mathbf{Z})^2$$

if $p = 2$, there are isomorphisms

$$\mathbf{Q}_2^\times / \mathbf{Q}_2^{\times 2} \simeq (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}_2^\times / (1 + 8\,\mathbf{Z}_2)) \simeq (\mathbf{Z}/2\mathbf{Z})^2$$

in which $(\varepsilon,\omega)\colon \mathbf{Z}_2^\times / (1 + 8\,\mathbf{Z}_2) \to (\mathbf{Z}/2\mathbf{Z})^2$ is a group isomorphism. A system of representatives is $\{1,u,p,pu\}$ (where $u \in \mathbf{Z}_p^\times$ is not a square) if $p \neq 2$ and $\{\pm 1, \pm 5, \pm 2, \pm 10\}$ if $p = 2$.
In particular, $\mathbf{Q}_p^{\times 2}$ is an open subgroup of $\mathbf{Q}_p^\times$.

Proof. The only thing that has to be checked is the fact that ε and ω are group homomorphisms. If $x = 1 + 2u$ and $y = 1 + 2v$ are elements in $\mathbf{Z}_2^\times = 1 + 2\,\mathbf{Z}_2$, we have $xy \equiv 1 + 2(x+y) \mod 4\,\mathbf{Z}_2$ so that $\varepsilon(xy)$ is the image of $u+v \mod 2\,\mathbf{Z}_2$, *i.e.* $\varepsilon(x) + \varepsilon(y)$. Similarly, we have $x^2 = 1 + 4(u+u^2)$ and $y^2 = 1 + 4(v+v^2)$, so that $(xy)^2 \equiv 1 + 4(u+u^2+v+v^2) \mod 16\,\mathbf{Z}_2$, so that $\omega(xy)$ is the image of $\frac{u+u^2}{2} + \frac{v+v^2}{2} \mod 2\,\mathbf{Z}_2$, *i.e.* $\omega(x) + \omega(y)$. □

7.4.4. *The Hilbert symbol.* In what follows, K is either $\mathbf{R}$ or $\mathbf{Q}_p$ for some prime p.

Definition 7.4.5. Let $a, b \in K^\times$. The *Hilbert symbol* of a and b (relative to K) is

$$(a,b) = \begin{cases} 1 & \text{if } ax^2 + by^2 - z^2 = 0 \text{ has a nonzero solution in } K^3 \\ -1 & \text{otherwise} \end{cases}.$$

Obviously (a,b) only depends on the images of a and b in $K^\times/K^{\times 2}$: we will often consider $(.,.)$ as a map $(K^\times/K^{\times 2}) \times (K^\times/K^{\times 2}) \to \{\pm 1\}$.

Lemma 7.4.6. Let $a, b \in K^\times$. Then $(a,b) = 1$ if and only if $a \in \mathsf{N}_{K(\sqrt{b})/K}\big(K(\sqrt{b})^\times\big)$.

[47] It seems excluded to improve upon Serre's writing...

Proof. If $b = \beta^2$ with $\beta \in K^\times$, then $(0,1,\beta) \in K^3$ is a nonzero solution of $ax^2 + by^2 - z^2 = 0$, and $K^\times = \mathsf{N}_{K(\sqrt{b})/K}\big(K(\sqrt{b})^\times\big)$: this gives the equivalence in this case. Assume henceforth that b is not a square in K, so that $\big[K(\sqrt{b}) : K\big] = 2$. Elements is $K(\sqrt{b})$ are thus of the form $u + v\sqrt{b}$ with $u, v \in K$, and $\mathsf{N}_{K(\sqrt{b})/K}(u + v\sqrt{b}) = u^2 - bv^2$. If $(a,b) = 1$, let $(x,y,z) \in K^3\backslash\{(0,0,0)\}$ be such that $ax^2 + by^2 - z^2 = 0$. Assume $x = 0$: we have $y \neq 0$ (this would imply $z = 0$ which is not), so $b = \big(\frac{z}{y}\big)^2$, contradicting the fact that b is not a square. As $x \neq 0$, we have $a = \big(\frac{z}{x}\big)^2 - b\big(\frac{y}{x}\big)^2 = \mathsf{N}_{K(\sqrt{b})/K}\big(\frac{z+y\sqrt{b}}{x}\big) \in \mathsf{N}_{K(\sqrt{b})/K}\big(K(\sqrt{b})^\times\big)$. Conversely, assume that $a = \mathsf{N}_{K(\sqrt{b})/K}(u + v\sqrt{b}) = u^2 - bv^2$: then $(1, v, u)$ is a nonzero solution to $ax^2 + by^2 - z^2 = 0$ in K^3, hence $(a,b) = 1$, showing the equivalence in that case. □

Lemma 7.4.7. If $a, b, c \in K^\times$, we have:

(i) $(a,b) = (b,a)$ and $(a,c^2) = 1$;
(ii) $(a,-a) = 1$ and $(a, 1-a) = 1$ if $a \neq 1$;
(iii) $(a,b) = 1 \Rightarrow (ac,b) = (c,b)$;
(iv) $(a,b) = (a,-ab) = (a,(1-a)b)$ (assuming $a \neq 1$ for the last equality).

Proof. (i) is obvious. For (ii), $(1,1,0)$ (resp. $(1,1,1)$) is a nonzero solution of $ax^2 - ay^2 - z^2 = 0$ (resp. $ax^2 + (1-a)y^2 - z^2 = 0$). If $(a,b) = 1$, then $a \in \mathsf{N}_{K(\sqrt{b})/K}(K(\sqrt{b})^\times)$ (*cf* lemma 7.4.6), so

$$(ac,b) = 1 \Leftrightarrow ac \in \mathsf{N}_{K(\sqrt{b})/K}\big(K(\sqrt{b})^\times\big) \Leftrightarrow c \in \mathsf{N}_{K(\sqrt{b})/K}\big(K(\sqrt{b})^\times\big) \Leftrightarrow (ac,b) = 1$$

(since $\mathsf{N}_{K(\sqrt{b})/K}\big(K(\sqrt{b})^\times\big)$ is a subgroup of $K^\times$), proving (iii). Finally, (iv) follows from (i)-(iii). □

Notation. • If $u \in \mathbf{Z}_p^\times$, we denote by $\overline{u}$ its image in $\mathbf{F}_p^\times$, and we put $\big(\frac{u}{p}\big) = \big(\frac{\overline{u}}{p}\big)$ (the Legendre symbol of $\overline{u}$, which is ±1 following to $\overline{u}$ is a square in $\mathbf{F}_p$ or not).
• If $p = 2$ and $u \in \mathbf{Z}_2^\times$, recall that we denote by $\varepsilon(u)$ (resp. $\omega(u)$) the image of $\frac{u-1}{2}$ (resp. $\frac{u^2-1}{8}$) in $\mathbf{F}_2$.

Theorem 7.4.8. Let $a, b \in K^\times$.
• If $K = \mathbf{R}$, we have $(a,b) = -1 \Leftrightarrow a, b \in \mathbf{R}_{<0}$.
• If $K = \mathbf{Q}_p$, write $a = p^\alpha u$ and $b = p^\beta v$ with $\alpha, \beta \in \mathbf{Z}$ and $u, v \in \mathbf{Z}_p^\times$. Then

$$(a,b) = \begin{cases} (-1)^{\alpha\beta\varepsilon(p)}\big(\frac{\overline{u}}{p}\big)^\beta\big(\frac{\overline{v}}{p}\big)^\alpha & \text{if } p \neq 2 \\ (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)} & \text{if } p = 2 \end{cases}.$$

Theorem 7.4.9. The Hilbert symbol is a non degenerate pairing on the $\mathbf{F}_2$-vector space $K^\times/K^{\times2}$.

Proof of theorem 7.4.8. The case where $K = \mathbf{R}$ is trivial, since $K^\times/K^{\times2} \simeq \{\pm1\}$ as $K^{\times2} = \mathbf{R}_{>0}$. We henceforth assume that $K = \mathbf{Q}_p$ for some prime p.
First observe that if $v \in \mathbf{Z}_p^\times$ and $z^2 - px^2 - vy^2 = 0$ has a nonzero solution in $\mathbf{Q}_p^3$, then it has a solution such that $x \in \mathbf{Z}_p$ and $y, z \in \mathbf{Z}_p^\times$ (clearing the denominators, we may assume that $(x,y,z) \in \mathbf{Z}_p^3\backslash p(\mathbf{Z}_p)^3$; if $p \mid z$, then $p \mid vy^2$ hence $p \mid y$ since $v \in \mathbf{Z}_p^\times$, so that $p \mid x$, contradicting $(x,y,z) \notin p\,\mathbf{Z}^3$, hence $z \in \mathbf{Z}_p^\times$, whence $vy^2 = z^2 - px^2 \in \mathbf{Z}_p^\times$, *i.e.* $y \in \mathbf{Z}_p^\times$).
The Hilbert symbol is symmetric, and it is affected by α and β only through their images in $\mathbf{Z}/2\,\mathbf{Z}$: we may restrict to the following three cases:

(1) $\alpha = \beta = 0$;
(2) $\alpha = 1$ and $\beta = 0$;
(3) $\alpha = \beta = 1$.

Case where $p \neq 2$. In case (1), we have to check that $(a,b) = 1$. By example 7.1.4, the quadratic form $ax^2 + by^2 - z^2$ has a nonzero isotropic vector in $\mathbf{F}_p^3$: as its discriminant $-ab$ belongs to $\mathbf{Z}_p^\times$, corollary 7.3.2 applies, showing that $ax^2 + by^2 - z^2$ has a nonzero isotropic vector in $\mathbf{Z}_p^3$, *i.e.* that $(a,b) = 1$.
In case (2), we have to check that $(pu, v) = \big(\frac{v}{p}\big)$. By lemma 7.4.7 (iii), we have $(pu,v) = (p,v)$ since $(u,v) = 1$ (*cf* case (1)): we may assume $u = 1$. If $(p,v) = 1$, there exists $(x,y,z) \in \mathbf{Z}_p^3$ such that $y, z \in \mathbf{Z}_p^\times$ such that $z^2 - px^2 - vy^2 = 0$ (*cf* above): reducing modulo p gives $\overline{vy}^2 = \overline{z}^2$, which implies that $\overline{v}$ is a square in $\mathbf{F}_p$, *i.e.* $\big(\frac{v}{p}\big) = 1$. Conversely, assume that $\big(\frac{v}{p}\big) = 1$: this implies that $\overline{v}$ is a square in $\mathbf{F}_p$, so that v is a square in $\mathbf{Z}_p$, so that $(p,v) = 1$ (*cf* 7.4.7 (i)). This shows that $(p,v) = \big(\frac{v}{p}\big)$ as required.
In case (3), we have to check that $(pu, pv) = (-1)^{\varepsilon(p)}\big(\frac{u}{p}\big)\big(\frac{v}{p}\big)$. By 7.4.7 (iv), we have

$$(pu,pv) = (pu, -p^2uv) = (pu, -uv) = \big(\tfrac{-uv}{p}\big)$$

(the last equality follows from case (2)), hence $(pu, pv) = (-1)^{\varepsilon(p)}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$ by multiplicativity of the Legendre symbol, and the equality $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$.

Case where $p = 2$. Here again, we may reduce to the three cases (1)-(3) as above. Assume (1): we must show that $(u, v) = 1$ if $\varepsilon(u)\varepsilon(v) = 0$ and $(u, v) = -1$ if $\varepsilon(u)\varepsilon(v) = 1$. If $u \equiv 1 \mod 8\,\mathbf{Z}_2$, then u is a square in $\mathbf{Z}_2$, so $(u, v) = 1$. If $u \equiv 5 \mod 8\,\mathbf{Z}_2$, then $u + 4v \equiv 1 \mod 8\,\mathbf{Z}_2$: there exists $w \in \mathbf{Z}_2$ such that $w^2 = u + 4v$, so that the for $ux^2 + vy^2 - z^2$ vanishes at $(1, 2, w)$, and $(u, v) = 1$. This shows that $\varepsilon(u) = 0 \Rightarrow (u, v) = 1$ (symmetrically, we have $\varepsilon(v) = 0 \Rightarrow (u, v) = 1$). Assume $u, v \in -1 + 4\,\mathbf{Z}_2$: if $(x, y, z) \in \mathbf{Z}^2$ is a primitive solution of $ux^2 + vy^2 - z^2 = 0$, we have $x^2 + y^2 + z^2 \equiv 0 \mod 4\,\mathbf{Z}_2$. As squares in $\mathbf{Z}/4\,\mathbf{Z}$ are 0 and 1, this shows that $x, y, z \in 2\,\mathbf{Z}_2$, contradicting the fact that (x, y, z) is primitive. Thus $(u, v) = -1$ in this case.
In case (2), we have to check that $(2u, v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)}$. First observe that $(2, v) = (-1)^{\omega(v)}$, *i.e.* that $2x^2 + vy^2 - z^2$ represents 0 if and only if $v \equiv \pm 1 \mod 8$. Indeed, assume $(2, v) = 1$: there exist $x, y, z \in \mathbf{Z}_2$ such that $y, z \in \mathbf{Z}_2^\times$ and $2x^2 + vy^2 = z^2$ (from the observation above). We have $y^2, z^2 \in 1 + 8\,\mathbf{Z}_2$, hence $2x^2 + v \equiv 1 \mod 8\,\mathbf{Z}_2$: as squares in $\mathbf{Z}/8\,\mathbf{Z}$ are 0, 1 and 4, we have $v \equiv \pm 1 \mod 8\,\mathbf{Z}_8$, hence $\omega(v) = 0$ and $(2, v) = (-1)^{\omega(v)}$. Conversely, if $v \equiv 1 \mod 8\,\mathbf{Z}_2$, then v is a square in $\mathbf{Z}_2$, so $(2, v) = 1$, and if $v \equiv -1 \mod 8\,\mathbf{Z}_2$, then $(1, 1, 1)$ is a solution of $2x^2 + vy^2 - z^2 \bmod 8$, so $(2, v) = 1$ by corollary 7.3.2.
It remains to check that $(2u, v) = (2, v)(u, v)$. By lemma 7.4.7 (iii), this holds if $(u, v) = 1$ or $(2, v) = 1$: assume $(u, v) = (2, v) = -1$. Then $u, v \equiv 3 \mod 4\,\mathbf{Z}_2$ and $v \equiv \pm 3 \mod 8\,\mathbf{Z}_2$ hence $v \equiv 3 \mod 8\,\mathbf{Z}_2$. Multiplying u and v by squares, we may thus assume that $(u, v) \in \{(-1, 3), (3, -5)\}$: we conclude since $(1, 1, 1)$ is a solution of $-2x^2 + 3y^2 = z^2$ and $6x^2 - 5y^2 = z^2$.
In case (3), we have to show that $(2u, 2v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(u)+\omega(v)}$. As $(2u, 2v) = (2u, -4uv) = (2u - uv)$ by lemma 7.4.7 (iv), we get $(2u, 2v) = (-1)^{\varepsilon(u)+\varepsilon(-uv)+\omega(-uv)}$ by the previous case. As $\varepsilon(-1) = 1$, $\omega(-1) = 0$ and $\varepsilon(u)(1 + \varepsilon(u)) = 0$, we have indeed $\varepsilon(u) + \varepsilon(-uv) + \omega(-uv) = \varepsilon(u)\varepsilon(v) + \omega(u) + \omega(v)$ as required. □

Proof of theorem 7.4.9. Here again, this is trivial when $K = \mathbf{R}$: we henceforth assume $K = \mathbf{Q}_p$ for some prime p.
The formulas of theorem 7.4.8 show the bilinearity of $(.,.)$ (since ε and ω are group homomorphisms). To show it is non degenerate, we have to check that whenever $a \in K^\times$ is not a square, there exists $b \in K^\times$ such that $(a, b) = -1$. It is enough to check this on representatives of $K^\times/K^{\times 2}$. If $p \neq 2$, and $u \in \mathbf{Z}_p$ is not a square, we have $(u, p) = (pu, u) = -1$. If $p = 2$, we have $(5, 2x) = -1$ if $x \in \{\pm 1, \pm 5\}$ and $(-1, -1) = (-1, -5) = -1$. □

Notation. From now on, we denote by V the set of places of $\mathbf{Q}$, *i.e.* the set of primes and ∞. If $v \in V$, we denote by $\mathbf{Q}_v$ the corresponding completion (so that $\mathbf{Q}_\infty = \mathbf{R}$), and $(.,.)_v$ the corresponding Hilbert symbol on $\mathbf{Q}_v \times \mathbf{Q}_v$.

Theorem 7.4.10. (Product formula, Hilbert). If $a, b \in \mathbf{Q}^\times$, then $(a, b)_v = 1$ for all but finitely many $v \in V$, and

$$\prod_{v \in V} (a, b)_v = 1.$$

Proof. By bilinearity of the Hilbert symbol, it is enough to check both statements when a and b are either -1 or a prime. When $a = b = -1$, we have $(a, b)_2 = (a, b)_\infty = -1$ and $(a, b)_v = 1$ if $v \in V\backslash\{2, \infty\}$. If $a = -1$ and b is a prime, then $(-1, b)_v = 1$ for all $v \in V$ if $b = 2$, and $(-1, b)_v = 1$ if $v \in V\backslash\{2, b\}$ and $(-1, b)_2 = (-1, b)_b = (-1)^{\varepsilon(b)}$.
It remains to deal with the case where a and b are prime. If $a = b$, we have $(a, b)_v = (-1, b)_v$ for all $v \in V$, by lemma 7.4.7 (iv), so we are reduced to the preceding case: assume henceforth that $a \neq b$. If $b = 2$, we have $(a, b)_v = (-1)^{\omega(a)}$, $(a, 2)_a = \left(\frac{2}{a}\right) = (-1)^{\omega(a)}$. If $a, b \in V\backslash\{2, a, b, \infty\}$, we have $(a, b)_v = 1$. Also $(a, b)_v = (-1)^{\varepsilon(a)\varepsilon(b)}$, $(a, b)_a = \left(\frac{b}{a}\right)$ and $(a, b)_b = \left(\frac{a}{b}\right)$, so that the product formula reduces to the equality $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\varepsilon(a)\varepsilon(b)}$, which is nothing but the quadratic reciprocity law. □

Theorem 7.4.11. Let $(a_i)_{i \in I}$ be a finite family of elements in $\mathbf{Q}^\times$, and $(\varepsilon_{i,v})_{\substack{i \in I \\ v \in V}}$ a family of elements in $\{\pm 1\}$. Then there exists $x \in \mathbf{Q}^\times$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all $i \in I$ and $v \in V$ if and only if the following conditions are satisfied:

(1) all but finitely many $\varepsilon_{i,v}$ are equal to 1;
(2) $\prod\limits_{v \in V} \varepsilon_{i,v} = 1$ for all $i \in I$;
(3) for all $v \in V$, there exists $x_v \in \mathbf{Q}_v^\times$ such that $(a_i, x_v)_v = \varepsilon_{i,v}$.

Proof. By theorem 7.4.10, the conditions are clearly necessary. Conversely, assume they are satisfied. After multiplication of the a_i by nonzero squares, we may assume that $a_i \in \mathbf{Z}\backslash\{0\}$ for all $i \in I$. Let S be the

subset of V formed by 2, ∞ and the primes that divide $\prod\limits_{i\in I} a_i$: this is a finite set. Let T be the set of those $v \in V$ such that $\varepsilon_{i,v} = -1$ for some $i \in I$: this is a finite set as well.
Special case: $S \cap T = \varnothing$. Put $a = \prod\limits_{\ell\in T\backslash\{\infty\}} \ell$ and $m = 8 \prod\limits_{\ell\in S\backslash\{2,\infty\}} \ell$: the hypothesis implies that a and m are coprime. By Dirichlet's theorem on arithmetic progressions, there exists a prime p such that $p \equiv a \mod m\mathbf{Z}$, and $p \notin S \cup T$. Put $x = ap$.
Assume $v \in S$: we have $\varepsilon_{i,v} = 1$ (since $S \cap T = \varnothing$). As $x > 0$, we have $(a_i, x)_\infty = 1$ for all $i \in I$. If v is a prime ℓ, we have $x = ap \equiv a^2 \mod m\mathbf{Z}$, so $x \equiv a^2 \mod 8\mathbf{Z}$ and $x \equiv a^2 \mod \ell\mathbf{Z}$ if $\ell \neq 2$: this shows that x is a square in $\mathbf{Q}_v^\times$ (*cf* proposition 7.4.2), so that $(a_i, x)_v = 1$ for all $i \in I$.
Assume $v = \ell \in V\backslash S$: we have $a_i \in \mathbf{Z}_\ell^\times$ for all $i \in I$. As $\ell \neq 2$, we have $(a_i, x)_\ell = \big(\frac{a_i}{\ell}\big)^{v_\ell(x)}$. If $\ell \notin T \cup \{p\}$, we have $x \in \mathbf{Z}_\ell^\times$, so that $(a_i, x)_\ell = 1 = \varepsilon_{i,v}$ since $v \notin T$. If $\ell \in T$, we have $v_\ell(x) = 1$ and there exists $x_\ell \in \mathbf{Q}_\ell^\times$ such that $(a_i, x_\ell)_\ell = \varepsilon_{i,\ell}$ for all $i \in I$ (by condition (3)). As $\ell \in T$, at least one of the $\varepsilon_{i,\ell}$ is -1: as $(a_i, x_\ell)_\ell = \big(\frac{a_i}{\ell}\big)^{v_\ell(x_\ell)}$ by theorem 7.4.8 (since $v_\ell(a_i) = 0$ and $\ell \neq 2$), we have $v_\ell(x_\ell) \equiv 1 \mod 2\mathbf{Z}$, so that

$$(a_i, x)_\ell = \big(\frac{a_i}{\ell}\big) = (a_i, x_\ell)_\ell = \varepsilon_{i,\ell}$$

for all $i \in I$ (by theorem 7.4.8 again). If $\ell = p$, we reduce to the previous cases thanks to the product formula:

$$(a_i, x)_p = \prod_{v\in V\backslash\{p\}} (a_i, x)_v = \prod_{v\in V\backslash\{p\}} \varepsilon_{i,v} = \varepsilon_{i,p},$$

which finishes the proof of the special case.
General case. By corollary 7.4.3, squares in $\mathbf{Q}_v^\times$ form an open subgroup of $\mathbf{Q}_v^\times$: by the approximation theorem (*cf* theorem 3.1.15), there exists $x' \in \mathbf{Q}^\times$ such that x'/x_v is a square in $\mathbf{Q}_v^\times$ for all $v \in S$. This implies in particular that $(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v}$ for all $v \in V$ and all $i \in I$. For all $v \in V$ and $i \in I$, put $\varepsilon'_{i,v} = (a_i, x')_v \varepsilon_{i,v} \in \{\pm 1\}$. Obviously the family $(\varepsilon'_{i,v})_{\substack{i\in I\\ v\in V}}$ satisfies conditions (1)-(3) (with $x'_v = x' x_v$ for all $v \in V$), and $\varepsilon'_{i,v} = 1$ for all $i \in I$ and $v \in S$. We can thus apply the special case to $(\varepsilon'_{i,v})_{\substack{i\in I\\ v\in V}}$: there exists $y \in \mathbf{Q}^\times$ such that $(a_i, y)_v = \varepsilon'_{i,v}$ for all $i \in I$ and $v \in V$, and we may take $x = x'y$. □

7.4.12. *Complements on quadratic forms.* In this part, K is a field of characteristic $\neq 2$, E a finite dimensional K-vector space, q a quadratic form on E, and φ the associated symmetric bilinear form. Recall that (E, q) admits an orthogonal basis, *i.e.* a K-basis of E in which (the matrix of) q is diagonal.

Notation. We denote by $\mathsf{disc}(q)$ th *discriminant* of q. This is an element in $K/K^{\times 2}$ but it will frequently denote a representative in K.

Definition 7.4.13. Two bases $\mathbf{e}$ and $\mathbf{e}'$ are *contiguous* if they share at least one vector.

Theorem 7.4.14. Assume $n = \dim_K(E) \geqslant 3$ and q is non-degenerate. Let $\mathbf{e}$ and $\mathbf{e}'$ be two orthogonal bases. then there exists a chain $\mathbf{e}_0 = \mathbf{e}, \ldots, \mathbf{e}_r = \mathbf{e}'$ of orthogonal bases such that $\mathbf{e}_i$ is contiguous to $\mathbf{e}_{i-1}$ for all $i \in \{1, \ldots, r\}$ (we say that the chain links $\mathbf{e}$ to $\mathbf{e}'$).

Proof. Write $\mathbf{e} = (e_1, \ldots, e_n)$ and $\mathbf{e}' = (e'_1, \ldots, e'_n)$.
- Case where $q(e_1)q(e'_1) \neq \varphi(e_1, e'_1)^2$. This means that $\{e_1, e'_1\}$ is linearly independent and that the restriction of q to the plane $P = \mathsf{Vect}(e_1, e'_1)$ is non-degenerate. As $q(e_1)q(e'_1) \neq 0$ (because $\mathbf{e}$ and $\mathbf{e}'$ are orthogonal and q non-degenerate), there exist $\tilde{e}_2$ and $\tilde{e}'_2$ such that $(e_1, \tilde{e}_2)$ and $(e'_1, \tilde{e}'_2)$ are orthogonal bases of P. Let $H = P^\perp$: as P is non-degenerate, we have $P \overset{\perp}{\oplus} H = E$ and H is non-degenerate. Let $(\tilde{e}_3, \ldots, \tilde{e}_n)$ be an orthogonal basis of H. Then

$$\mathbf{e} \to (e_1, \tilde{e}_2, \tilde{e}_3, \ldots, \tilde{e}_n) \to (e'_1, \tilde{e}'_2, \tilde{e}_3, \ldots, \tilde{e}_n) \to \mathbf{e}'$$

is a chain of contiguous bases.
- The case $q(e_1)q(e'_2) \neq \varphi(e_1, e'_2)^2$ is similar, replacing e'_1 by e'_2.
- Case where $q(e_1)q(e'_i) = \varphi(e_1, e'_i)^2$ for $i \in \{1, 2\}$. Then there exists $\lambda \in K^\times$ such that $\tilde{e} := e'_1 + \lambda e'_2$ is non-isotropic, and $P = \mathsf{Vect}(e_1, \tilde{e})$ is non-degenerate. Indeed, we have $q(\tilde{e}) = q(e'_1) + \lambda^2 q(e'_2)$, so we have to choose $\lambda \neq -\frac{q(e'_1)}{q(e'_2)}$. This is possible if $\#K > 3$. If $K = \mathbf{F}_3$, we can take $\lambda = 1$ (since squares are 0 and 1). Recall that $K \neq \mathbf{F}_2$ since $\mathsf{char}(K) \neq 2$. This choice of λ made, we have

$$\begin{aligned} q(e'_1)q(\tilde{e}) - \varphi(e_1, \tilde{e})^2 &= q(e_1)\big(q(e'_1) + \lambda^2 q(e'_2)\big) - \big(\varphi(e_1, e'_1) + \lambda\varphi(e_1, e'_2)\big)^2 \\ &= q(e_1)q(e'_1) + \lambda^2 q(e_1)q(e'_2) - \varphi(e_1, e'_1)^2 - \lambda^2\varphi(e_1, e'_2)^2 - 2\lambda\varphi(e_1, e'_1)\varphi(e_1, e'_2) \\ &= -2\lambda\varphi(e_1, e'_1)\varphi(e_1, e'_2) \neq 0 \end{aligned}$$

since $\lambda \neq 0$ and $\varphi(e_1, e'_1)\varphi(e_1, e'_2) \neq 0$ (because $q(e_1)q(e'_1)q(e'_2) \neq 0$ as $\mathbf{e}$ and $\mathbf{e}^prime$ are orthogonal and q non-degenerate) so that P is non-degenerate.
As $\tilde{e}$ is non-isotropic and $\mathsf{Vect}(e'_1, e'_2)$ non-degenerate, there exists $\tilde{e}'$ such that $(\tilde{e}, \tilde{e}')$ is an orthogonal basis of $\mathsf{Vect}(e'_1, e'_2)$. Put $\mathbf{e}'' = (\tilde{e}, \tilde{e}', e'_3, \ldots, e'_n)$: this is an orthogonal basis of E which is contiguous to $\mathbf{e}'$. As $\mathsf{Vect}(e_1, \tilde{e})$ is non-degenerate, the first case seen above shows that there exists a chain of contigous bases that links $\mathbf{e}$ to $\mathbf{e}''$. □

Definition 7.4.15. Recall that one says that q *represents* $a \in K$ when there exists $x \in E\backslash\{0\}$ such that $q(x) = a$ (in particular, q represents 0 when q has nonzero isotropic vectors).

Lemma 7.4.16. Let $f = f(X_1, \ldots, X_{n-1})$ be a non-degenerate quadratic form and $a \in K^\times$. The following are equivalent:

(i) f represents a;
(ii) $f \sim g \oplus aX^2$ for some quadratic form g in $n-2$ variables;
(iii) $f \ominus aX_n^2$ represents 0.

Proof. Write $E = K^{n-1}$. Assume (i): there exists $e \in E\backslash\{0\}$ such that $q(e) = a$. As f is non-degenerate, we have $Ke \overset{\perp}{\oplus} e^\perp = E$, and $f \sim g \oplus aX^2$ where g is the restriction of f to $e^{\perp}$" this shows (ii). The implication (ii)⇒(iii) is obvious. Assume (iii): there exists $(x_1, \ldots, x_n) \in K^n\backslash\{0\}$ such that $f(x_1, \ldots, x_{n-1}) = ax_n^2$. If $x_n \neq 0$, then $f\big(\frac{x_1}{x_n}, \ldots, \frac{x_{n-1}}{x_n}\big) = a$. If $x_n = 0$ then f represents 0: it contains an hyperbolic plane, so it is surjective and represents a. This shows (i). □

Lemma 7.4.17. Let g, h be two non-degenerate quadratic forms of rank $\geqslant 1$ and $f = g \ominus h$. The following are equivalent:

(i) f represents 0;
(ii) there exists $a \in K^\times$ which is represented by g and h;
(iii) there exists $a \in K^\times$ such tha $g \ominus aX^2$ and $h \ominus aX^2$ represent 0.

Proof. The equivalence (ii)⇔(iii) follows from lemma 7.4.16 and (ii)⇒(i) is obvious. Assume (i): there exist x, y such that $g(x) = h(y)$. If $a = g(x) \neq 0$, this gives (ii). If $g(x) = 0$, then g and f are surjective: they both represent $a = 1$. □

Recall that two quadratic forms on a finite field of odd characteristic (resp. on $\mathbf{R}$) are equivalent if and only if they have same rank and same discrimininant (resp. if they have the same signature).

7.4.18. *Classification of quadratic forms over* $\mathbf{Q}_p$. In this section p is a prime and (E, q) is a non-degenerate quadratic space over $\mathbf{Q}_p$.

Notation. Let $\mathbf{e} = (e_1, \ldots, e_n)$ be a orthogonal basis of E. For each $i \in \{1, \ldots, n\}$, put $a_i = q(e_i)$, so that $q\Big(\sum\limits_{i=1}^n x_i e_i\Big) = \sum\limits_{i=1}^n a_i x_i^2$. We have $\mathsf{disc}(q) = \prod\limits_{i=1}^n a_i$ in $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$. Put

$$\varepsilon(q, \mathbf{e}) = \prod_{1 \leqslant i < j \leqslant n} (a_i, a_j)_p \in \{\pm 1\}.$$

Theorem 7.4.19. The number $\varepsilon(q, \mathbf{e})$ does not depend of the choice of $\mathbf{e}$.

Proof. This is obvious if $n = 1$ since $\varepsilon(q, \mathbf{e}) = 1$. If $n = 2$, then $\varepsilon(q, \mathbf{e}) = 1$ if and only if the form $a_1X^2 + a_2Y^2 - Z^2$ represents 0, *i.e.* if and only if q represents 1 (*cf* lemma 7.4.16), which is independent of the choice of $\mathbf{e}$. We proceed by induction on n: assume henceforth that $n \geqslant 3$. By theorem 7.4.14, it is enough to show that $\varepsilon(q, \mathbf{e}) = \varepsilon(q, \mathbf{e}')$ when $\mathbf{e}$ and $\mathbf{e}'$ are contiguous: we may assume that $\mathbf{e}' = (e_1, e'_2, \ldots, e'_n)$ (by the bilinearity of Hilbert symbol, *cf* theorem 7.4.9, $\varepsilon(q, \mathbf{e})$ does not change when the vectors of $\mathbf{e}$ are permuted). Then we have

$$\varepsilon(q, \mathbf{e}) = (a_1, a_2 \cdots a_n)_p \prod_{2 \leqslant i < j \leqslant n} (a_i, a_j)_p = (a_1, \mathsf{disc}(q)a_1)_p \prod_{2 \leqslant i < j \leqslant n} (a_i, a_j)_p$$

and similarly

$$\varepsilon(q, \mathbf{e}') = (a_1, \mathsf{disc}(q)a_1)_p \prod_{2 \leqslant i < j \leqslant n} (a'_i, a'_j)_p$$

(where $a'_i = q(e'_i)$ for $i \in \{2, \ldots, n\}$). The indiction hypothesis applied to the restriction of q to $e_1^\perp$ implies that $\prod\limits_{2 \leqslant i < j \leqslant n} (a_i, a_j)_p = \prod\limits_{2 \leqslant i < j \leqslant n} (a'_i, a'_j)_p$, so that $\varepsilon(q, \mathbf{e}) = \varepsilon(q, \mathbf{e}')$. □

Theorem 7.4.19 implies that $\varepsilon(q) := \varepsilon(q, \mathbf{e})$ is an invariant of q, as do the rank and the discriminant.

Theorem 7.4.20. Let f be a quadratic form of rank n over $\mathbf{Q}_p$. The f represents 0 if and only if

(i) $n = 2$ and $\mathsf{disc}(f) = -1$ (in $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$);
(ii) $n = 3$ and $\varepsilon(f) = (-1, -\mathsf{disc}(f))_p$;
(iii) $n = 4$ and $\mathsf{disc}(f) \neq 1$ or $\mathsf{disc}(f) = 1$ and $\varepsilon(f) = (-1,-1)_p$;
(iv) $n \geqslant 5$.

Corollary 7.4.21. Let f be a quadratic form of rank n over $\mathbf{Q}_p$. The f represents $a \in \mathbf{Q}_p^\times$ if and only if

(i) $n = 1$ and $\mathsf{disc}(f) = a$ (in $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$);
(ii) $n = 2$ and $\varepsilon(f) = (a, -\mathsf{disc}(f))_p$;
(iii) $n = 3$ and $\mathsf{disc}(f) \neq -1$ or $\mathsf{disc}(f) = -a$ and $\varepsilon(f) = (-1, -\mathsf{disc}(f))_p$;
(iv) $n \geqslant 4$.

Proof. By lemma 7.4.16, the quadratic form represents a if and only if $g := f \ominus aX^2$ represents 0. As $\mathsf{disc}(g) = -a\,\mathsf{disc}(f)$ and $\varepsilon(g) = (-a, \mathsf{disc}(f))_p \varepsilon(f)$, this follows from theorem 7.4.20. □

Proof of theorem 7.4.20. Write $f = a_1X_1^2 + \cdots + a_nX_n^2$.
(i) Assume $n = 2$: the quadratic form f represents 0 if and only if $-\frac{a_2}{a_1}$ is a square. As $-\frac{a_2}{a_1} = -\mathsf{disc}(f)$ in $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$, this is equivalent to $\mathsf{disc}(f) = -1$ in $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$.
(ii) Assume $n = 3$: the quadratic form f represents 0 if and only if $-a_3 f \sim -a_1a_3X_1^2 - a_2a_2X_2^2 - X_3^2$ represents 0. By the very definition of the Hilbert symbol, this is equivalent to

$$1 = (-a_1a_3, -a_2a_3)_p = (-1,-1)_p(-1,a_1)_p(-1,a_2)_p(a_3,a_3)_p \underbrace{(a_1,a_2)_p(a_1,a_3)_p(a_2,a_3)_p}_{\varepsilon(f)}.$$

As $(a_3,a_3)_p = (-1,a_3)_p$ by lemma 7.4.7 (ii), this is equivalent to $1 = (-1,-1)_p(-1,\mathsf{disc}(f))_p\varepsilon(f)$ hence to the equality $\varepsilon(f) = (-1, -\mathsf{disc}(f))_p$.
(iii) Assume $n = 4$: the quadratic form f represents 0 if and only if the forms $a_1X_1^2 + a_2X_2^2$ and $-a_3X_3^2 - a_4X_4^2$ both represent some element $a \in \mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$ (*cf* lemma 7.4.17). By the case (ii) of corollary 7.4.21 (which follows from the case (ii) of theorem 7.4.20 proved above), such an a is characterized by the following conditions :

$$(a, -a_1a_2)_p = (a_1,a_2)_p \quad \text{and} \quad (a, -a_3a_4)_p = (-a_3,-a_4)_p.$$

The subset A (resp. B) of $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$ defined by the first (resp. the second) condition is an affine hyperplane in the $\mathbf{F}_2$-vector space $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$. Thus f does not represent 0 if and only if $A \cap B = \varnothing$. This precisely means that the orthogonal vectors to A and B (for the non-degenerate pairing $(.,.)_p$) are equal, *i.e.* that $-a_1a_2 = -a_3a_4$ and that $(a_1,a_2)_p = -(-a_3,-a_4)_p$. The is equivalent to $\mathsf{disc}(f) = 1$. On the other hand, we have $\varepsilon(f) = (a_1,a_2)_p(a_1a_2, a_3a_4)_p(a_3,a_4)_p$: if the first condition holds, we have

$$\varepsilon(f) = (a_1,a_2)_p(-1,a_3a_4)_p(a_3,a_4)_p = (a_1,a_2)_p(-a_3,-a_4)_p(-1,-1)_p$$

(since $(x,x) = (-1,x)$ by lemma 7.4.7 (ii)), so that the second condition is equivalent to $\varepsilon(f) = -(-1,-1)_p$.
(iv) Assume $n \geqslant 5$. By corollary 7.4.21 (ii), a form in two variables represents half of the elements in $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$ (because the equation $\varepsilon(f) = (a, -\mathsf{disc}(f))_p$ defines an affine hyperplane in the $\mathbf{F}_2$-vector space $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$). As $\#(\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}) \geqslant 4$ (*cf* corollary 7.4.3), there exists at least one $a \in \mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$ which is distinct from $\mathsf{disc}(f)$ and represented by the form. This holds of course for quadratic forms of rank $\geqslant 3$ as well, hence for f. By lemma 7.4.16, we can write $f \sim g \oplus aX^2$ where g is a quadratic form of rank $n-1 \geqslant 4$. Then $\mathsf{disc}(g) = \frac{\mathsf{disc}(f)}{a} \neq 1$: by (iii), g represents 0, so f represents 0 as well. □

Theorem 7.4.22. Two quadratic forms over $\mathbf{Q}_p$ are equivalent if and only if they have same rank, same discriminant and same invariant ε.

Proof. We already know that two equivalent quadratic forms have same rank, same discriminant and same invariant ε. Conversely, assume f and g are two quadratic forms having same rank n, same discriminant and same invariant ε: we show by induction on n that $f \sim g$. This is obvious if $n = 0$: assume $n > 0$. By corollary 7.4.21, f and g represent the same elements in $\mathbf{Q}_p^\times$: we can find $a \in \mathbf{Q}_p^\times$ which is represented by both f and g. Then we can write $f \sim f' \oplus aX^2$ and $g \sim g' \oplus aX^n$, where f' and g' are of rank $n-1$. As $\mathsf{disc}(f') = a\,\mathsf{disc}(f) = a\,\mathsf{disc}(g) = \mathsf{disc}(g')$ and $\varepsilon(f') = (a, \mathsf{disc}(f'))_p\varepsilon(f) = (a, \mathsf{disc}(g'))_p\varepsilon(g) = \varepsilon(g')$, the induction hypothesis implies that $f' \sim g'$, hence $f \sim g$. □

Corollary 7.4.23. Up to equivalence, there exists exactly one anisotropic form of rank 4 over $\mathbf{Q}_p$, which is $X_1^2 - aX_2^2 - bX_3^2 + abX_4X_4^2$ for any $a, b \in \mathbf{Q}_p^\times$ such that $(a,b)_p = -1$.

Proposition 7.4.24. Let $n \in \mathbf{Z}_{>0}$, $d \in \mathbf{Q}_p^\times$ and $\varepsilon \in \{\pm 1\}$. There exists rank n a quadratic form f over $\mathbf{Q}_p$ such that $\mathsf{disc}(f) = d$ and $\varepsilon(f) = \varepsilon$ if and only if $n = 1$ and $\varepsilon = 1$, or $n = 2$ and $d \neq -1$, or $n = 2$ and $\varepsilon = 1$ or $n \geqslant 3$.

Proof. This is obvious if $n = 1$. If $n = 2$, write $f \sim aX_1^2+bX_2^2$: if $d = -1$ we have $\varepsilon = (a, b)_p = (a, -d)_p = 1$, so we cannot have $d = -1$ and $\varepsilon = -1$ simultaneously. Conversely, if $d = -1$ and $\varepsilon = 1$, we can take $f = X_1^2 - X_2^2$, and if $d \neq -1$, there exists $a \in \mathbf{Q}_p^\times$ such that $(a, -d)_p = \varepsilon$, and we take $f = aX_1^2 + adX_2^2$. If $n \geqslant 3$, let $a \in \mathbf{Q}_p^\times$ whose image in $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$ is distinct from $-d$: by what precedes, there exists a rank 2 quadratic form g such that $\mathsf{disc}(g) = ad$ and $\varepsilon(g) = \varepsilon(a, -d)_p$, so that $f = g + aX^2$ works. When $n \geqslant 3$, we reduce to the case $n = 3$ bytaking $f = g + X_4^2 + \cdots + X_n^2$ where g has rank 3, discriminant d and $\varepsilon(g) = \varepsilon$. □

Corollary 7.4.25. The number of equivalences of rank n quadratic forms over $\mathbf{Q}_p$ is summarized in the following table:

n	1	2	$\geqslant 3$
$p = 2$	8	15	16
$p \neq 2$	4	7	8

7.4.26. *Classification of quadratic forms over* $\mathbf{Q}$. Recall that V is the set of places of $\mathbf{Q}$, *i.e.* the set of prime numbers and a point ∞, and that for each $v \in V$, we denote by $\mathbf{Q}_v$ the corresponding completion of $\mathbf{Q}$ (so $\mathbf{Q}_\infty = \mathbf{R}$). If f is a quadratic form over $\mathbf{Q}$ and $v \in V$, then if can be seen as a quadratic form f_v over $\mathbf{Q}_v$, so besides the global invariants given by the rank and the discriminant, we have the local invariants $\varepsilon_v(f) := \varepsilon(f_v) \in \{\pm 1\}$ for $v \in V \backslash \{\infty\}$, and the signature (s, t). By the product formula, we have

$$\prod_{v \in V} \varepsilon_v(f) = 1$$

Theorem 7.4.27. (Hasse-Minkowski). f represents 0 if and only if f_v represents 0 for all $v \in V$.

Proof. Write $f = a_1X_1^2 + \cdots + a_nX_n^2$ with $a_1, \ldots, a_n \in \mathbf{Q}^\times$. Replacing f by $a_1^{-1}f$, we may of course assume $a_1 = 1$. Assume f_v represents 0 for all $v \in V$: we have to prove that f represents 0 (the converse is obvious).

• Assume $n = 2$. Write $f = X_1^2 - aX_2^2$. As f_∞ represents 0, we have $a > 0$: write $a = \prod\limits_{p \in V\backslash\{\infty\}} p^{v_p(a_2)}$. As f_p represents 0, the element a is a square in $\mathbf{Q}_p^\times$, so that $v_p(a)$ is even. As this holds for all prime p, this means that a is a square in $\mathbf{Q}^\times$, and f represents 0.

• Assume $n = 3$. Write $f = X_1^2 - aX_2^2 - bX_3^2$. Multiplying a and b by appropriate squares in $\mathbf{Q}^\times$, we may assume that a and b are squarefree integers. We may also assume $|a| \leqslant |b|$. We proceed by induction on $m = |a| + |b| > 1$ (since $ab \neq 0$). If $m = 2$, we have $f = X_1^2 \pm X_2^2 \pm X_3^2$. As f_∞ represents 0, the case $f = X_1^2 + X_2^2 + X_3^2$ is impossible; in all other cases f represents 0. Assume $m > 2$, so that $|b| \geqslant 2$. Write $b = \pm p_1 \cdots p_r$ where $p_1, \ldots, p_r$ are paiwise distinct primes. Let $p \in \{p_1, \ldots, p_r\}$. If $p \nmid a$, then $a \in \mathbf{Z}_p^\times$. By hypothesis there exists $(x, y, z) \in \mathbf{Z}_p^3 \backslash p\,\mathbf{Z}_p^3$ such that $x^2 - ay^2 - bz^2$, hence $x^2 - ay^2 \equiv 0 \mod p\,\mathbf{Z}_p$. If $p \mid y$, then $p \mid x$, so that $p^2 \mid -bz^2$, whence $p \mid z$ (because $v_p(b) = 1$), contradicting the fact that $(x, y, z) \notin p\,\mathbf{Z}_p^3$. This implies that $y \in \mathbf{Z}_p^\times$, and a is a square modulo p. Of course, this also holds when $p \mid a$. As this is true for each $p \in \{p_1, \ldots, p_r\}$, this shows that a is a square modulo b (by the Chinese remainder theorem): we can find $t, b' \in \mathbf{Z}$ such that $t^2 = a + bb'$. We may assume $|t| \leqslant \frac{|b|}{2}$. As $bb' = t^2 - a = \mathsf{N}_{K(\sqrt{a})/K}(t + \sqrt{a})$ (where $K = \mathbf{Q}$ or $K = \mathbf{Q}_p$), lemma 7.4.6 implies that f represents 0 in K if and only if $f' := X_1^2 - aX_2^2 - b'X_3^2$ does. In particular, f'_v represents 0 for all $v \in V$. As $|b'| = \frac{|t^2-a|}{|b|} \leqslant \frac{|b|}{4} + 1 < |b|$ (since $|b| \geqslant 2$), we have $b' = b''u^2$ with b'' a squarefree integers, $u \in \mathbf{Z}$ and $|b''| < |b|$. The inductin hypothesis implies that f' represents 0: so does f.

• Assume $n = 4$. Write $f = (aX_1^2 + bX_2^2) - (cX_3^2 + dX_4^2)$. Let $v \in V$. As f_v represents 0, lemma 7.4.17 implies the existence of $x_v \in \mathbf{Q}_v^\times$ which is represented by both $aX_1^2 + bX_2^2$ and $cX_3^2 + dX_4^2$. By corollary 7.4.21 (which also holds when $v = \infty$), this means that $(x_v, -ab)_v = (a, b)_v$ and $(x_v, -cd)_v = (c, d)_v$. As $\prod\limits_{v \in V} (a, b)_v = \prod\limits_{v \in V} (c, d)_v = 1$, theorem 7.4.11 applied to $(-ab, -cd)$ (hence $\#I = 2$) implies the existence of $x \in \mathbf{Q}^\times$ such that $(x, -ab)_v = (a, b)_v$ and $(x, -cd)_v = (c, d)_v$ for all $v \in V$. This means that the quadratic forms $aX_1^2 + bX_2^2 - xZ^2$ and $cX_3^2 + dX_4^2 - xZ^2$ represent 0 in $\mathbf{Q}_v$ for all $v \in V$: by the case $n = 3$ treated above, this implies that they represent 0 in $\mathbf{Q}$. In particular, $x \in \mathbf{Q}^\times$ is represented by $aX_1^2 + bX_2^2$ and $cX_3^2 + dX_4^2$: by lemma 7.4.17 again, this implies that f represents 0.

• Assume $n \geqslant 5$. We use induction on n. Write $f = h \ominus g$ with $h = a_1X_1^2 + a_2X_2^2$ and $g = -a_3X_3^2 - \cdots - a_nX_n^2$. Let S be the subset of V made of ∞, 2 and those primes p such that $v_p(a_i) \neq 0$ for some $i \in \{3, \ldots, n\}$: this is a finite set. Let $v \in S$. As f_v represents 0, there exists $a_v \in \mathbf{Q}_v^\times$ which is represented by h_v and g_v (*cf* lemma 7.4.17): there exists $(x_{1,v}, \ldots, x_{n,v}) \in \mathbf{Q}_v^n \backslash \{0\}$ such that $h(x_{1,v}, x_{2,v}) = a_v = g(x_{3,v}, \ldots, x_{n,v})$. As squares form an open subset of $\mathbf{Q}_v^\times$ (*cf* corollary 7.4.3) and $\mathbf{Q}^\times$ is dense in $\mathbf{Q}_v^\times$, there exist $x_1, x_2 \in \mathbf{Q}^\times$ such that $a = h(x_1, x_2) \in \mathbf{Q}^\times$ satisfies $a \in a_v\,\mathbf{Q}_v^{\times 2}$ for all $v \in S$. Let $f_1 = aZ^2 - g$: this is a rank $n - 1$

quadratic form over $\mathbf{Q}$. As g_v represents a_v hence a, the form $f_{1,v}$ represents 0 for all $v \in S$. If $v \in V \backslash S$, we have $a_i \in \mathbf{Z}_v^\times$ for all $i \in \{3, \ldots, n\}$, so that $\mathsf{disc}(g) \in \mathbf{Z}_v^\times$. As $v \neq 2$, we have $\varepsilon_v(f_1) = 1$ (*cf* theorem 7.4.8). As the rank of g is $\geqslant 3$, theorem 7.4.20 implies that g_v represents 0 (as $v \neq 2$, the Hilbert symbols is trivial on pairs of units, *cf* theorem 7.4.8 again). This show that $f_{1,v}$ represents 0 for all $v \in V$: the induction hypothesis implies that f_1 represents 0 hence g represents a over $\mathbf{Q}$. By lemma 7.4.17, this shows that f represents 0. □

Remark 7.4.28. The analogue of Hasse-Minkowski theorem fails for forms of higher degree. For instance the form of degree 4

$$(X_1^2 + \cdots + X_n^2)^2 - 2(X_{n+1}^2 + \cdots + X_{2n})^2$$

does not represent 0 in $\mathbf{Q}$, but it does in $\mathbf{R}$ and $\mathbf{Q}_p$ for all prime p when $n \geqslant 5$ (by theorem 7.4.20).

Corollary 7.4.29. *f represents $a \in \mathbf{Q}^\times$ if and only if it does in $\mathbf{Q}_v$ for all $v \in V$.*

Proof. This follows from theorem 7.4.27 applied to the form $aZ^2 - f$ and lemma 7.4.16. □

Corollary 7.4.30. *If f is of rank $\geqslant 5$, then it represents 0 if and only if it does in $\mathbf{R}$.*

Proof. This follows from theorems 7.4.27 and 7.4.20. □

Theorem 7.4.31. *Two quadratic forms f and g over $\mathbf{Q}$ are equivalent if and only if they are over $\mathbf{Q}_v$ for all $v \in V$.*

Proof. The necessity is trivial. For the converse, we proceed by induction on the rank n of f and g. There is nothing to do if $n = 0$: assume $n > 0$. There exists $a \in \mathbf{Q}^\times$ which is represented by f, hence also by g (*cf* corollary 7.4.29). This implies that $f \sim aX^2 \oplus f'$ and $g \sim aX^2 \oplus g'$ where f' and g' are of rank $n-1$. By Witt simplification theorem we have $f'_v \sim g'_v$ for all $v \in V$: the induction hypothesis implies that $f' \sim g'$, so that $f \sim g$. □

Proposition 7.4.32. *Let $d \in \mathbf{Q}^\times / \mathbf{Q}^{\times 2}$, $(\varepsilon_v)_{v \in V} \in \{\pm 1\}^V$ and $(s,t) \in \mathbf{Z}_{\geqslant 0}^2$. Then there exists a quadratic form f of rank n over $\mathbf{Q}$ whose invariants are d, $(\varepsilon_v)_{v \in V}$ and (s,t) if and only if*

(i) $\varepsilon_v = 1$ for all but finitely many $v \in V$ and $\prod\limits_{v \in V} \varepsilon_v = 1$;
(ii) $\varepsilon_v = 1$ if $n = 1$ or $n = 2$ and $d_v = -1$ in $\mathbf{Q}_v^\times / \mathbf{Q}_v^{\times 2}$;
(iii) $s + t = n$;
(iv) $d_\infty = (-1)^t$;
(v) $\varepsilon_\infty = (-1)^{\frac{t(t-1)}{2}}$.

Proof. The necessity is obvious. For the converse, the case $n = 1$ is trivial.
Assume $n = 2$. If $v \in V$, the non-degeneracy of the Hilbert symbol (*cf* theorem 7.4.9) and condition (ii) imply the existence of $x_v \in \mathbf{Q}_v^\times$ such that $(x_v, -d_v)_v = \varepsilon_v$. Condition (i) and theorem 7.4.11 then implies the existence of $x \in \mathbf{Q}^\times$ such that $(x, -d)_v = \varepsilon_v$ for all $v \in V$, so we can take $f = xX_1^2 + xdX_2^2$.
Assume $n = 3$. Let S be the subset of V made of those v such that $(-d_v, -1)_v = -\varepsilon_v$: this is a finite set. If $v \in S$, we can find $c_v \in \mathbf{Q}_v^\times$ whose image in $\mathbf{Q}_v^\times / \mathbf{Q}_v^{\times 2}$ is distinct from $-d_v$. As $\mathbf{Q}_v^{\times 2}$ is open in $\mathbf{Q}_v^\times$, the approximation theorem (*cf* theorem 3.1.15) implies the existence of $c \in \mathbf{Q}^\times$ whose image in $\mathbf{Q}_v^\times / \mathbf{Q}_v^{\times 2}$ coincides with that of c_v for all $v \in S$. By the case $n = 2$ seen above, there exists a form g of rank 2 over $\mathbf{Q}$ such that $\mathsf{disc}(g) = cd$, $\varepsilon_v(g) = (c, -d)_v \varepsilon_v$ for all $v \in V$. Then we can take $f = cX^2 + g$.
For $n \geqslant 4$, we use induction on n. If $s \geqslant 1$, the induction hypothesis implies the existence of a quadratic form g of rank $n-1$ over $\mathbf{Q}$, with invariants d, $(\varepsilon_v)_{v \in V}$ and $(s-1, t)$, and we can take $f = X^2 \oplus g$. If $s = 0$, the induction hypothesis implies the existence of a quadratic form h of rank $n-1$ over $\mathbf{Q}$, with invariants $-d$, $(\varepsilon_v(-1, -d)_v)_{v \in V}$ and $(s, t-1)$, and we can take $f = -X^2 \oplus h$. □

7.4.33. *Cubic forms.* Let K be a field (of characteristic 0 to simplify), $n, d \in \mathbf{Z}_{>0}$ and $\mathscr{H}_{n,d}$ be the space of homogeneous polynomials of degree d in $K[X_1, \ldots, X_n]$ (this is a K-vector space of dimension $\binom{n+d-1}{n-1}$). An element $f \in \mathscr{H}_{n,d} \backslash \{0\}$ defines a projective hypersurface $\mathsf{V}(f) \subset \mathbf{P}^{n-1}(K)$. A point $P \in \mathsf{V}(f)$ is a *singular point* when[48] $\frac{\partial f}{\partial X_i}(\widehat{P}) = 0$ for all $i \in \{1, \ldots, n\}$ (where $\widehat{P} \in \mathbf{A}^n(K) \backslash \{0\}$ is a lift of $P \in \mathbf{P}^{n-1}(K)$). The hypersurface $\mathsf{V}(F)$ is *non-singular* if it has no singular points.
The resultant polynomial of a collection of elements in $K[X_1, \ldots, X_n]$ is a polynomial in the coefficients of these polynomials which vanishes if and only if they all have a common root (*cf* [9, Chapter 13 1.A]). The *discriminant* $\Delta(f)$ of f is then the resultant of the polynomials $\frac{\partial f}{\partial X_i}$ for $i \in \{1, \ldots, n\}$: this is an

[48] By Euler's formula, we have $df = \sum\limits_{i=1}^n X_i \frac{\partial f}{\partial X_i}$: the vanishing of the partial derivatives at $P \in \mathbf{P}^{n-1}(K)$ implies $P \in \mathsf{V}(f)$.

homogeneous polynomial of degree $n(d-1)^{n-1}$ in the $\binom{n+d-1}{n-1}$ coefficients of f and is non-zero at f if and only if $\mathsf{V}(f)$ is a non-singular projective hypersurface.

Theorem 7.4.34. (Demyanov, Lewis, *cf* [6], [14]). Let p be a prime, $K/\mathbf{Q}_p$ a finite extension and

$$f = \sum_{1\leqslant i\leqslant j\leqslant k\leqslant n} a_{i,j,k}X_iX_jX_k \in K[X_1,\ldots,X_n]$$

be a cubic form. If $n \geqslant 10$ then f represents 0.

Proof. • Assume first that $\mathsf{V}(f)$ is non-singular, *i.e.* that $\Delta(f) \in K^\times$: we have $\delta(f) := v_K(\Delta(f)) \in \mathbf{Z}$, and $\delta(f) \in \mathbf{Z}_{\geqslant 0}$ when $f \in \mathcal{O}_K[X_1,\ldots,X_n]$. We say that a form $g \in \mathscr{H}_{n,3}$ is *K-equivalent* to f if there exists $M \in \mathsf{GL}_n(K)$ such that $g = f\circ M$. Of course, g is non-singular as well, and f is equivalent to an element in $\mathcal{O}_K[X_1,\ldots,X_n]$, moreover, f represents 0 if and only if g does. We say that f is *reduced* if $f \in \mathcal{O}_K[X_1,\ldots,X_n]$ and $\delta(f) \leqslant \delta(g)$ for all the forms g that are K-equivalent to f. Of course, replacing f by an appropriate F-equivalent form, we may assume that f is reduced.
Let $r \in \mathbf{Z}_{\geqslant 0}$ be minimal such that $f \equiv f_1(L_1,\ldots,L_r) \mod \pi\mathcal{O}_K[X_1,\ldots,X_n]$ (where π denotes a uniformizer of K), where $f_1 \in \mathcal{O}_K[Y_1,\ldots,Y_r]$ and $L_1,\ldots,L_r \in \mathcal{O}_K[X_1,\ldots,X_n]$ are linearly independent linear forms. We have of course $r \leqslant n$. Also, $L_1,\ldots,L_r$ are the first components of an unimodular map $M \in \mathsf{GL}_n(\mathcal{O}_K)$, so that $g := f\circ M^{-1}$ is reduced as well: replacing f by g, we may assume that $L_i = X_i$, *i.e.* that $f(X_1,\ldots,X_n) \equiv f_1(X_1,\ldots,X_r) \mod \pi\mathcal{O}_K[X_1,\ldots,X_n]$. This implies that the form $f' = \pi^{-1}f(\pi X_1,\ldots,\pi X_r,X_{r+1},\ldots,X_n)$ has coefficients in $\mathcal{O}_K$. Moreover, as Δ is homogeneous of degree $n2^{n-1}$ in the variables of f, we have

$$\Delta(f') = \pi^{-n2^{n-1}}\Delta(f(\pi X_1,\ldots,\pi X_r,X_{r+1},\ldots,X_n))$$

$$\text{and}\quad \Delta(f(\pi X_1,\ldots,\pi X_r,X_{r+1},\ldots,X_n)) = \pi^{3r2^{n-1}}\Delta(f).$$

The last equality follows from the fact that multiplying the variables $X_1,\ldots,X_r$ by π has the effect of multiplying $\binom{r+2}{3}$ coefficients by π^3 (namely those $X_iX_jX_k$ such that $1\leqslant i\leqslant j\leqslant k\leqslant r$), $\binom{r+1}{2}(n-r)$ coefficients by π^2 (those $X_iX_jX_k$ such that $1\leqslant i\leqslant j\leqslant r<k\leqslant n$) and $r\binom{n-r+1}{2}$ coefficients by π (those $X_iX_jX_k$ such that $1\leqslant i\leqslant r<j\leqslant k\leqslant n$), so that the mean scaling on the $\binom{n+2}{3}$ coefficients of f is

$$\tfrac{1}{\binom{n+2}{3}}\Big(3\tbinom{r+2}{3}+2\tbinom{r+1}{2}(n-r)+r\tbinom{n-r+1}{2}\Big) = \tfrac{3r}{n}$$

so that the effect on $\Delta(f)$ is multiplication by $\pi^{\frac{3r}{n}n2^{n-1}} = \pi^{3r2^{n-1}}$ since Δ is homogeneous of degree $n2^{n-1}$. Put together, this implies that $\Delta(f') = \pi^{(3r-n)2^{n-1}}\Delta(f)$, so that

$$\delta(f') = \delta(f) + (3r-n)2^{n-1}.$$

As f is reduced, we have $\delta(f)\leqslant\delta(f')$, so that $3r\geqslant n$: if $n\geqslant 10$, we have $r\geqslant 4$. By Chevalley-Warning theorem (*cf* theorem 7.1.2), the reduction of f_1 modulo π represents 0 (because it has 4 variables and degree 3 over the finite field κ_K): there exists $(b_1,\ldots,b_r)\in\mathcal{O}_K^r\backslash\pi\mathcal{O}_K^r$ such that $f_1(b_1,\ldots,b_r)\in\pi\mathcal{O}_K$. We may of course assume $b_1 = 1$. Replacing f by the unimodularly equivalent

$$f(X_1,X_2+b_2X_1,\ldots,X_r+b_rX_r,X_{r+1},\ldots,X_n)\in\mathcal{O}_K[X_1,\ldots,X_n]$$

(this is still reduced), we may assume that $(b_1,\ldots,b_r) = (1,0,\ldots,0)$. Then

$$f(1,0,\ldots,0)\equiv f_1(b_1,\ldots,b_r) \mod \pi\mathcal{O}_K$$

so that $f(1,0,\ldots,0)\in\pi\mathcal{O}_K$. This shows that the coefficient of X_1^3 in f belongs to $\pi\mathcal{O}_K$. We thus have

$$f\equiv X_1^2L+X_1Q+C \mod \pi\mathcal{O}_K[X_1,\ldots,X_n]$$

where $L,Q,C\in\mathcal{O}_K[X_2,\ldots,X_r]$ are homogeneous of degres 1, 2 and 3 respectively. By minimality of r, we cannot have $(L,Q)\equiv(0,0) \mod \pi\mathcal{O}_K[X_2,\ldots,X_r]$ (otherwise we could replace f_1 by C).

First case. If $L\notin\pi\mathcal{O}_K[X_2,\ldots,X_r]$, there exists $i\in\{2,\ldots,r\}$ such that $\frac{\partial L}{\partial X_i}\in\mathcal{O}_K^\times$. As Q and C are homogeneous of degree $\geqslant 2$, we have $\frac{\partial Q}{\partial X_i}(1,0,\ldots,0) = \frac{\partial C}{\partial X_i}(1,0,\ldots,0) = 0$, so that

$$\tfrac{\partial f}{\partial X_i}(1,0,\ldots,0) = \tfrac{\partial L}{\partial X_i}\in\mathcal{O}_K^\times.$$

Second case. If $L\in\pi\mathcal{O}_K[X_2,\ldots,X_r]$, there exists $\mathbf{d} = (d_2,\ldots,d_r)\in\mathcal{O}_K^{r-1}$ such that $Q(\mathbf{d})\notin\pi\mathcal{O}_K$, *i.e.* $Q(\mathbf{d})\in\mathcal{O}_K^\times$. Put $\mathbf{x} = (-C(\mathbf{d}),d_2Q(\mathbf{q}),\ldots,d_rQ(\mathbf{d}),0,\ldots,0)\in\mathcal{O}_K^n$. We have $\mathbf{x}\notin\pi\mathcal{O}_K^n$ since $(d_2Q(\mathbf{q}),\ldots,d_rQ(\mathbf{d}) = Q(\mathbf{d})\mathbf{d}\notin\pi\mathcal{O}_K^{r-1}$. We have

$$f(\mathbf{x})\equiv C(\mathbf{d})^2\underbrace{L(Q(\mathbf{d})\mathbf{d})}_{Q(\mathbf{d})L(\mathbf{d})}-C(\mathbf{d})\underbrace{Q(Q(\mathbf{d})\mathbf{d})}_{=Q(\mathbf{d})^3}+\underbrace{C(Q(\mathbf{d})\mathbf{d})}_{=Q(\mathbf{d})^3C(\mathbf{d})} \mod \pi\mathcal{O}_K$$

since L (resp. Q, resp. C) is homogeneous of degree 1 (resp. 2, resp. 3). As $\mathsf{L}(\mathbf{d}) \in \pi\mathcal{O}_K$, this shows that $f(\mathbf{x}) \in \pi\mathcal{O}_K$. On the other hand, we have $\frac{\partial f}{\partial X_1} \equiv 2X_1L + Q \mod \pi\mathcal{O}_K[X_1, \ldots, X_n]$, so that

$$\tfrac{\partial f}{\partial X_1}(\mathbf{x}) \equiv -2C(\mathbf{d})Q(\mathbf{D})L(\mathbf{d}) + Q(\mathbf{d})^3 \mod \pi\mathcal{O}_K$$

which implies that $\frac{\partial f}{\partial X_1}(\mathbf{x}) \in \mathcal{O}_K^\times$ since $L(\mathbf{d}) \in \pi\mathcal{O}_K$ and $Q(\mathbf{d}) \in \mathcal{O}_K^\times$.

In any case we can apply Newton's lemma to find a nonzero solution of $f = 0$, which concludes the proof when $\mathsf{V}(f)$ is non-singular.

• Proof of the general case. As Δ is a nonzero homogeneous form of degree $n2^{n-1}$ in the $\binom{n+2}{2}$ variables of f, it cannot vanish on any neighborhood of a point in $\mathscr{H}_{n,2}$: we can find a sequence of non-singular forms $(f_k)_{k\in\mathbf{Z}_{\geqslant 0}}$ that converges coefficientwise to f. By the non-singular case proved above, for each $k \in \mathbf{Z}_{\geqslant 0}$, we can find $\mathbf{x}_k \in K^n\backslash\{0\}$ such that $f_k(\mathbf{x}_k) = 0$. As f_k is homogeneous, we can multiply $\mathbf{x}_k$ by an appropriate power of π and assume that

$$\mathbf{x}_k \in \mathscr{K} := \bigcup_{i=1}^{n} \{\mathbf{x} \in \mathcal{O}_K^r\,;\, x_i \in \mathcal{O}_K^\times\}.$$

As $\mathscr{K}$ is compact as a finite union of compact sets, the sequence $(\mathbf{x}_k)_{k\in\mathbf{Z}_{\geqslant 0}}$ has an accumulation point: we may assume it converges to some $\mathbf{a} \in \mathscr{K}$ (so in particular $\mathbf{a} \neq 0$. By continuity of f, we have $f(\mathbf{a}) = 0$ and f represents 0. □

Remark 7.4.35. (1) The bound 10 is optimal. In fact, if p is a prime, $K/\mathbf{Q}_p$ a finite extension and $n \in \mathbf{Z}_{>0}$, it is easy to construct a homogeneous polynomial in n^2 variables and of degree n that does not represent 0, as follows (*cf* [3, p.58]). Let $q = \#\kappa_K$. After the choice of a $\mathbf{F}_q$-basis of $\mathbf{F}_{q^n}$, the norm $\mathsf{N}_{\mathbf{F}_{q^n}/\mathbf{F}_q} \colon \mathbf{F}_{q^n} \to \mathbf{F}_q$ provides an homogeneous polynomial $\mathbf{F}_q[X_1, \ldots, X_n]$ of degree n which does not represent 0 (we have $\mathsf{N}_{\mathbf{F}_{q^n}/\mathbf{F}_q}(x) = 0 \Rightarrow x = 0$). We may lift it coefficient-wise to get a degree n homogeneous polynomial $g \in \mathcal{O}_K[X_1, \ldots, X_n]$ such for all for all $\mathbf{x} \in \mathcal{O}_K^n$, we have $g(\mathbf{x}) \in \pi\mathcal{O}_K \Rightarrow \mathbf{x} \in \pi\mathcal{O}_K$. Put

$$f(X_1, \ldots, X_{n^2}) = \sum_{i=0}^{n-1} \pi^i g(X_{in+1}, \ldots X_{in+n-1}) \in \mathcal{O}_K[X_1, \ldots, X_{n^2}]$$

If f represents 0, there exists a primitive vector $\mathbf{x} = (x_1, \ldots, x_{n^2}) \in \mathcal{O}_K^{n^2}\backslash\pi\mathcal{O}_K^{n^2}$ such that $f(\mathbf{x}) = 0$. This implies that $g(x_1, \ldots, x_n) \in \pi\mathcal{O}_K$, so that $x_1, \ldots, x_n \in \pi\mathcal{O}_K$, hence $g(x_1, \ldots, x_n) \in \pi^n\mathcal{O}_K$. This implies that $\pi g(x_{n+1}, \ldots, x_{2n}) \in \pi^2\mathcal{O}_K$, so that $x_{n+1}, \ldots, x_{2n} \in \pi\mathcal{O}_K$. A straightforward induction thus shows that $x_i \in \pi\mathcal{O}_K$ for all $i \in \{1, \ldots, n^2\}$, which is a contradiction.
(2) Heath-Brown has shown (*cf* [11]) that a *non-singular* cubic form in $n \geqslant 10$ variables with rational coefficients represents 0 in $\mathbf{Q}$.

7.5. Exercises.

Exercise 7.5.1. Let V be a $\mathbf{F}_q$-scheme of finite type. Show that Dwork's theorem is equivalent to the existence of algebraic complex numbers $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ such that $\#V(\mathbf{F}_{q^k}) = \sum\limits_{i=1}^{r} \alpha_i^k - \sum\limits_{j=1}^{s} \beta_j^k$ for all $k \in \mathbf{Z}_{>0}$.

Exercise 7.5.2. Assume V is such that $\mathsf{Z}_V(T) = \frac{1+aT+qT^2}{(1-T)(1-qT)}$ (this holds when V is an elliptic curve). Show that $\#V(\mathbf{F}_q)$ determines $\#V(\mathbf{F}_{q^k})$ for all $k \in \mathbf{Z}_{>0}$.

Exercise 7.5.3. Find the Zeta functions of the following schemes V over $\mathbf{F}_q$:
(1) the 3-dimensional hypersurface defined by $XY - ZT = 0$;
(2) the projective curve in $\mathbf{P}^2_{\mathbf{F}_q}$ with inhomogeneous equation:
(i) $XY = 0$;
(ii) $XY(X + Y + 1) = 0$;
(iii) $X^2 - Y^2 = 1$;
(iv) $Y^2 = X^3$;
(v) $Y^2 = X^3 + X^2$;
(3) $V = \mathsf{GL}_d$ and $V = \mathsf{SL}_d$ over $\mathbf{F}_q$ for $d \in \mathbf{Z}_{>0}$.

Exercise 7.5.4. Let V be a geometrically irreducible smooth projective variety of dimension d over $\mathbf{F}_q$. Show that the Riemann hypothesis for $\mathsf{Z}_V(T)$ implies that $\#V(\mathbf{F}_{q^n}) = q^{dn} + \mathsf{O}(q^{(d-1/2)n})$. Conversely, assuming that $d = 1$, $\mathsf{Z}_V(T) = \frac{P(T)}{(1-T)(1-qT)}$ and the functional equation, show that the Riemann hypothesis for $\mathsf{Z}_V(T)$ follows from this estimate.

Exercise 7.5.5. Let $P(X,Y,Z) = 3X^3 + 4Y^3 + 5Z^3$.
(1) Show that the equation $P(x,y,z) = 0$ has a non zero solution in $\mathbf{F}_p^3$ for all prime p.
(2) Deduce that the equation $P(x,y,z) = 0$ has a non zero solution in $\mathbf{Z}_p^3$ for all prime p.

Exercise 7.5.6. Let $P(X,Y,Z) = X^4 - 2Y^2 - 17Z^4$.
(1) Show that the equation $P(x,y,z) = 0$ has a non-zero solution in $\mathbf{Z}_p^3$ for all prime p.
(2) Show that the equation $P(x,y,z) = 0$ has no non-zero solution in $\mathbf{Q}^3$

Exercise 7.5.7. Let p be an odd prime and $K/\mathbf{Q}_p$ a finite extension. Assume $f = \sum\limits_{1=1}^{n} a_i X_i^2 \in K[X_1, \ldots, X_n]$ is a quadratic form of rank n.
(1) Show that if $a_i \in \mathcal{O}_K^\times$ for at least three indices $i \in \{1, \ldots, n\}$, then f represents 0.
(2) Show that if $n \geqslant 5$, then f represents 0.

Exercise 7.5.8. Does the quadratic form $x^2 + y^2 + z^2 - 7t^2$ represent 0 over $\mathbf{Q}$?

Exercise 7.5.9. Let p be a prime, $f = a_1x_1^2 + \cdots + a_nx_n^2$ and $g = b_1x_1^2 + \cdots + b_mx_m^2$ be two diagonal non-singular quadratic forms with coefficients in $\mathbf{Q}_p$. Show that $\varepsilon_p(f \oplus g) = \varepsilon_p(f)\varepsilon_p(g)(\mathsf{disc}(f), \mathsf{disc}(g))_p$.

Exercise 7.5.10. Determine all the elements of $\mathbf{Q}_7$ represented by the quadratic form $3x^2 + 7y^2$.

Exercise 7.5.11. Let $f = 5X^2 - 7Y^2$.
(1) Does the form f represent 0 in $\mathbf{Q}$?
(2) Show that the form f represents a nonzero rational integer a in $\mathbf{Q}$ if and only if $(a, 35)_p = (5, -7)_p$ for all odd prime p.
(3) Assuming $a \in \mathbf{Z}\backslash\{0\}$ is squarefree, characterize by conditions on Legendre symbols those a that can be represented by f in $\mathbf{Q}$, distinguishing the following four cases:

(i) $\mathsf{gcd}(a, 35) = 1$;
(ii) $5 \mid a$ and $7 \nmid a$;
(iii) $7 \mid a$ and $5 \nmid a$;
(iv) $35 \mid a$.

8. The Kronecker-Weber Theorem

8.1. **The statements.** What follows is taken from [25, Chapter 14]. In what follows, if $n \in \mathbf{Z}_{>0}$, ζ_n will denote a (any) primitive n-th root of unity. If F ia a field whose characteristic does not divide n, the extension $F(\zeta_n)/F$ is Galois (field of decomposition of $X^n - 1$). If $\sigma \in \mathsf{Gal}(F(\zeta_n)/F)$, there exists a unique $\chi(\sigma) \in (\mathbf{Z}/n\mathbf{Z})^\times$ such that $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$, and σ is entirely determined by $\chi(\sigma)$, so that the map

$$\begin{aligned}\chi\colon \mathsf{Gal}(F(\zeta_n)/F) &\to (\mathbf{Z}/n\mathbf{Z})^\times\\ \sigma &\mapsto \chi(\sigma)\end{aligned}$$

is an injective group homomorphism. In particular, the extension $F(\zeta_n)/F$ is abelian.
Class field theory is devoted in classifying abelian extensions of a given field. A classical consequence of global class field theory is the follow result:

Theorem 8.1.1. (Kronecker-Weber). Let $K/\mathbf{Q}$ be a finite abelian extension. Then there exists $n \in \mathbf{Z}_{>0}$ such that $K \subset \mathbf{Q}(\zeta_n)$.

Instead of using class field theory, we will deduce it from its local counterpart:

Theorem 8.1.2. Let p be a prime number and $K/\mathbf{Q}_p$ a finite abelian extension. Then there exists $n \in \mathbf{Z}_{>0}$ such that $K \subset \mathbf{Q}_p(\zeta_n)$.

8.2. **Preliminaries.**

8.2.1. *Abelian extensions.*

Proposition 8.2.2. Any subextension of an abelian extension is abelian. Any composite of finitely many abelian extensions is an abelian extension.

Proof. Let K be a field.
- Let L/K be an abelian extension. If M is a subextension of L/K, the group $\mathsf{Gal}(L/M)$ is a subgroup of the abelian group $\mathsf{Gal}(L/K)$: it is abelian as well, and normal in $\mathsf{Gal}(L/K)$, so that M/K is Galois, with group $\mathsf{Gal}(M/K) \simeq \mathsf{Gal}(L/K)/\mathsf{Gal}(L/M)$, which is abelian. This shows that L/M and M/K are abelian.
- Let L/K be an algebraic extension and L_1, L_2 subextensions of L/K such that L_1/K and L_2/K are abelian. Then L_2 is the field of decomposition of some separable polynomial $P(X) \in K[X]$ over K, so that L_1L_2 is the field of decomposition of P over L_1. This implies that the extension L_1L_2/L_1 is separable (even Galois): as L_1/K is separable, this shows that L_1L_2/K is separable. On the other hand, if $\sigma\colon L_1L_2 \to \overline{L}$ is a morphism of K-algebras (where $\overline{L}$ is an algebraic closure of L), we have $\sigma(L_1) = L_1$ and $\sigma(L_2) = L_2$ (since L_1 and L_2 are Galois over K), hence $\sigma(L_1L_2) = L_1L_2$, *i.e.* L_1L_2/K is normal, thus Galois. The restrictions to L_1 and L_2 induce a group homomorphism

$$\mathsf{Gal}(L_1L_2/K) \to \mathsf{Gal}(L_1/K) \times \mathsf{Gal}(L_2/K)$$

which is injective since if $\sigma \in \mathsf{Gal}(L_1L_2/K)$ induces the identity on L_1 and L_2, then $\sigma = \mathsf{Id}_{L_1L_2}$. This implies that $\mathsf{Gal}(L_1L_2/K)$ identifies with a subgroup of the abelian group $\mathsf{Gal}(L_1/K) \times \mathsf{Gal}(L_2/K)$: it is abelian as well. By induction, this extends to the composite of finitely many abelian extensions. □

Proposition 8.2.3. Let L/K be an abelian extension of number fields, $\mathfrak{p} \subset \mathcal{O}_K$ a nonzero prime ideal and $\mathfrak{P} \subset \mathcal{O}_L$ a prime ideal lying above $\mathfrak{p}$. Then

$$\{\sigma \in \mathsf{Gal}(L/K)\,;\, \sigma(\mathfrak{P}) \subset \mathfrak{P}\}$$

$$\{\sigma \in \mathsf{Gal}(L/K)\,;\, (\forall x \in \mathcal{O}_L)\, \sigma(x) \in x + \mathfrak{P}\}$$

are subgroup of $\mathsf{Gal}(L/K)$ that do not depend of $\mathfrak{P}$: we denote them $D_{\mathfrak{P}}(L/K)$ and $I_{\mathfrak{p}}(L/K)$ respectively, and call them the *decomposition* and the *inertia* group of L/K at $\mathfrak{p}$ respectively.

Proof. The set $\{\sigma \in \mathsf{Gal}(L/K)\,;\, \sigma(\mathfrak{P}) \subset \mathfrak{P}\}$ is the stabilizer of $\mathfrak{P}$ for the action of $\mathsf{Gal}(L/K)$ on the set of prime ideals dividing $\mathfrak{p}$: this is a subgroup of $\mathsf{Gal}(L/K)$. As the action is transitive, those stabilizers are all conjugate, hence equal since $\mathsf{Gal}(L/K)$ is abelian. This shows the statements for $D_{\mathfrak{p}}(L/K)$. The analogue for $I_{\mathfrak{p}}(L/K)$ follow. □

8.2.4. *Cyclotomic extensions of* $\mathbf{Q}$.

Proposition 8.2.5. The minimal polynomial of ζ_n over $\mathbf{Q}$ is the cyclotomic polynomial

$$\Phi_n(X)=\prod_{k\in(\mathbf{Z}/n\,\mathbf{Z})^\times}(X-\zeta_n^k).$$

Proof. We have $X^n-1=\prod\limits_{d\mid n}\Phi_d(X)$: a straightforward induction (starting with $\Phi_1(X)=X-1$) implies that $\Phi_n(X)\in\mathbf{Z}[X]$ for all $n\in\mathbf{Z}_{>0}$. We have to prove that $\Phi_n(X)$ is irreducible over $\mathbf{Q}$, *i.e.* over $\mathbf{Z}$ (its content is 1). Assume we can write $\Phi_n(X)=P(X)Q(X)$ with $P,Q\in\mathbf{Q}[X]$ monic and P irreducible. Write $P=\frac{1}{a}\widetilde{P}$ and $Q=\frac{1}{b}\widetilde{Q}$ with $a,b\in\mathbf{Z}_{>0}$ and $\widetilde{P},\widetilde{Q}\in\mathbf{Z}[X]$ with content 1: we have $\widetilde{P}\widetilde{Q}=ab\Phi_n$. Taking contents we have $ab=1$, *i.e.* $a=b=1$, so that $P,Q\in\mathbf{Z}[X]$. Replacing ζ_n by another primitive n-th root of unity, we may assume that $P(\zeta_n)=0$, and P is the minimal polynomial of ζ_n over $\mathbf{Q}$.
Let p be a prime not dividing n. As ζ_n^p is a primitive n-th root of unity, we have $\Phi_n(\zeta_n^p)=0$. Assume that $P(\zeta_n^p)\neq0$, so that $Q(\zeta_n^p)=0$. As P is the minimal polynomial of ζ_n over $\mathbf{Q}$, we have $P(X)\mid Q(X^p)$: write $Q(X^p)=P(X)U(X)$. We have $U(X)\in\mathbf{Z}[X]$ since P is monic. Modulo p, this gives $\overline{Q}(X)^p=\overline{P}(X)\overline{U}(X)$ in $\mathbf{F}_p[X]$. If $\alpha\in\overline{\mathbf{F}}_p$ is a root of $\overline{P}$, we have $Q(\alpha)=0$. This implies that $X-\alpha\mid\gcd(\overline{P}(X),\overline{Q}(X))$, so that $(X-\alpha)^2\mid\overline{P}(X)\overline{Q}(X)=\overline{\Phi}_n(X)$, whence $(X-\alpha)^2\mid X^n-1$ in $\overline{\mathbf{F}}_p[X]$. This contradicts the fact that the polynomial X^n-1 is separable in $\mathbf{F}_p[X]$ (since $p\nmid n$). We thus have $P(\zeta_n^p)=0$. A straightforward induction implies that for any $k\in\mathbf{Z}_{>0}$ prime to n, we have $P(\zeta_n^k)=0$, so that $\Phi_n(X)\mid P(X)$, *i.e.* $\Phi_n=P$ is irreducible over $\mathbf{Q}$. □

Remark 8.2.6. If p is a prime integer and $e\in\mathbf{Z}_{>0}$, we have

$$\Phi_{p^e}(X)=\Phi_p(X^{p^{e-1}})=X^{(p-1)p^{e-1}}+X^{(p-2)p^{e-1}}+\cdots+X^{p^{e-1}}+1=\tfrac{X^{p^e}-1}{X^{p^{e-1}}-1},$$

and one can show directly the irreducibility of Φ_{p^e} over $\mathbf{Z}$ using the Eisenstein criterion.

Proposition 8.2.7. If p is a prime number and $e\in\mathbf{Z}_{>0}$. The ring of integers of $\mathbf{Q}(\zeta_{p^e})$ is $\mathbf{Z}[\zeta_{p^e}]$ and $\left|d_{\mathbf{Q}(\zeta_{p^e})}\right|=p^{p^{e-1}(pe-e-1)}=\frac{p^{e\varphi(p^e)}}{p^{\frac{\varphi(p^e)}{p-1}}}$.

Proof. Put $\zeta=\zeta_{p^e}$ and $K=\mathbf{Q}(\zeta_{p^e})$ for short.

- We certainly have $\mathbf{Z}[\zeta]\subset\mathcal{O}_K$. We have $\Phi_{p^e}(1)=\Phi_p(1)=p$, so that $\prod\limits_{k\in(\mathbf{Z}/p^e\,\mathbf{Z})^\times}(1-\zeta^k)=p$. If $k\in(\mathbf{Z}/p^e\,\mathbf{Z})^\times$, we have $\frac{1-\zeta^k}{1-\zeta}\in\mathbf{Z}[\zeta]$. As ζ^k is also a primitive p^e-th root of unity, we also have $\frac{1-\zeta}{1-\zeta^k}\in\mathbf{Z}[\zeta]$, so that $\frac{1-\zeta^k}{1-\zeta}\in\mathbf{Z}[\zeta]^\times$. What precedes thus imply that $p=u(1-\zeta)^{(p-1)p^{e-1}}$ with $u\in\mathbf{Z}[\zeta]^\times$. If $\pi=1-\zeta$ was invertible in A, so would be $p=u\pi^{\varphi(p^r)}$, implying that p would be invertible in $\mathbf{Z}$ (since $\mathbf{Z}$ is integrally closed), which is not: π is not invertible in $\mathcal{O}_K$.
- We have $\mathsf{N}_{K/\mathbf{Q}}(1-\zeta)=\prod\limits_{\substack{1\leqslant k<p^r\\ \gcd(k,p)=1}}(1-\zeta)=\Phi_{p^e}(1)=p$. If $m\in\{1,\ldots,e-1\}$, the element ζ^{p^m} is a primitive p^{e-m}-th root of unity, so that $\mathsf{N}_{\mathbf{Q}(\zeta^{p^m})/\mathbf{Q}}\left(1-\zeta^{p^m}\right)=p$ by what precedes. This implies

$$\mathsf{N}_{K/\mathbf{Q}}\left(1-\zeta^{p^m}\right)=\mathsf{N}_{K/\mathbf{Q}(\zeta^{p^m})}\left(\mathsf{N}_{\mathbf{Q}(\zeta^{p^m})/\mathbf{Q}}\left(1-\zeta^{p^m}\right)\right)=p^{[K:\mathbf{Q}(\zeta^{p^m})]}$$

As $[K:\mathbf{Q}]=\varphi(p^e)=p^{e-1}(p-1)$ and $\left[\mathbf{Q}\left(\zeta^{p^m}\right):\mathbf{Q}\right]=p^{e-m-1}(p-1)$, we have $\left[K:\mathbf{Q}\left(\zeta^{p^m}\right)\right]=p^m$, so that

$$\mathsf{N}_{K/\mathbf{Q}}\left(1-\zeta^{p^m}\right)=p^{p^m}$$

We have $\Phi'_{p^e}(X)=\sum\limits_{\substack{1\leqslant k<p^e\\ \gcd(k,p)=1}}\prod\limits_{\substack{1\leqslant j<p^e\\ \gcd(j,p)=1\\ j\neq k}}\left(X-\zeta^j\right)$, so $\Phi'_{p^e}(\zeta)=\prod\limits_{\substack{1<k<p^e\\ \gcd(k,p)=1}}(\zeta-\zeta^k)=\zeta^{\varphi(p^e)-1}\prod\limits_{\substack{1<k<p^e\\ \gcd(k,p)=1}}(1-\zeta^{k-1})$ and

$$\mathsf{N}_{K/\mathbf{Q}}\left(\Phi'_{p^e}(\zeta)\right)=\mathsf{N}_{K/\mathbf{Q}}(\zeta)^{\varphi(p^e)-1}\prod_{\substack{1<k<p^e\\ \gcd(k,p)=1}}\mathsf{N}_{K/\mathbf{Q}}\left(1-\zeta^{k-1}\right)$$

As $\zeta\in\mathcal{O}_K^\times$, we have $\mathsf{N}_{K/\mathbf{Q}}(\zeta)\in\{\pm1\}$. As $\mathsf{N}_{K/\mathbf{Q}}\left(1-\zeta^{k-1}\right)=p^{p^{v_p(k-1)}}$ by what precedes, we have thus $\mathsf{N}_{K/\mathbf{Q}}\left(\Phi'_{p^e}(\zeta)\right)=\pm p^c$, where $c=\sum\limits_{\substack{1<k<p^e\\ \gcd(k,p)=1}}p^{v_p(k-1)}$. An integer $k\in\{2,\ldots,p^e-1\}$ satisfies $v_p(k-1)\geqslant r$ if and only if $k=1+p^rx$ with $x\in\{1,\ldots,p^{e-r}-1\}$ if $r\in\{1,\ldots,e-1\}$ and $x\in\{1,\ldots,p^e-2\}$ if $r=0$: there are $p^{e-r}-1$ (resp. p^e-2) such integers. This implies that there are $p^e-p^{e-1}-1$ (resp. $p^{e-r}-p^{e-r-1}$) integers $k\in\{2,\ldots,p^e-1\}$ such that $v_p(k-1)=0$ (resp. such that $v_p(k-1)=r$). Among

those k such that $v_p(k-1)=0$, there are $p^{e-1}-1$ that are divisible by p. This implies that we have $c=p^e-p^{e-1}-1-(p^{e-1}-1)+\sum\limits_{r=1}^{e-1}p^r(p^{e-r}-p^{e-r-1})=e(p^e-p^{e-1})-p^{e-1}$ *i.e.* $c=p^{e-1}(pe-e-1)$.
We have[49]

$$\mathrm{D}\left(1,\zeta,\cdots,\zeta^{\varphi(p^e)-1}\right)=(-1)^{\frac{\varphi(p^e)(\varphi(p^e)-1)}{2}}\,\mathsf{N}_{K/\mathbf{Q}}\left(\Phi'_{p^e}(\zeta)\right)=\pm p^c$$

If $(x_1,\dots,x_{\varphi(p^r)})$ is a $\mathbf{Z}$-basis of $\mathcal{O}_K$, we have

$$\mathrm{D}\left(1,\zeta,\cdots,\zeta^{\varphi(p^e)-1}\right)=[\mathcal{O}_K:\mathbf{Z}[\zeta]]^2\,\mathrm{D}(x_1,\dots,x_{\varphi(p^e)})$$

and $[\mathcal{O}_K:\mathbf{Z}[\zeta]]^2|p^c$, so that $\#(\mathcal{O}_K/\mathbf{Z}[\zeta])=[\mathcal{O}_K:\mathbf{Z}[\zeta]]$ is a power of p (*cf* corollary 2.6.5).
• We have $p\mathcal{O}_K=\pi^{\varphi(p^r)}\mathcal{O}_K$, so $p\,\mathbf{Z}\subseteq\mathbf{Z}\cap\pi\mathcal{O}_K$. As $p\,\mathbf{Z}$ is maximal in $\mathbf{Z}$ and $1\notin\pi\mathcal{O}_K$ (because π is not invertible in $\mathcal{O}_K$), we have in fact $\mathbf{Z}\cap\pi\mathcal{O}_K=p\,\mathbf{Z}$. As the extension $\mathbf{Z}\subset\mathcal{O}_K$ is integral and $p\,\mathbf{Z}$ is maximal in $\mathbf{Z}$, the ideal $\pi\mathcal{O}_K$ is maximal in $\mathcal{O}_K$. As $p\mathcal{O}_K=\pi^{\varphi(p^r)}\mathcal{O}_K$, there is a filtration

$$p\mathcal{O}_K=\pi^{\varphi(p^e)}\mathcal{O}_K\subset\pi^{\varphi(p^e)-1}\mathcal{O}_K\subset\cdots\subset\pi\mathcal{O}_K\subset\mathcal{O}_K$$

where the $\mathcal{O}_K/\pi\mathcal{O}_K$-vector space $\pi^m\mathcal{O}_K/\pi^{m+1}\mathcal{O}_K$ has dimension 1 for all $m\in\{0,\dots,\varphi(p^r)-1\}$. We thus have $\#(\mathcal{O}_K/p\mathcal{O}_K)=\left(\#(\mathcal{O}_K/\pi\mathcal{O}_K)\right)^{\varphi(p^r)}$. As $\#(\mathcal{O}_K/p\mathcal{O}_K)=p^{\varphi(p^e)}$ (since $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank $\varphi(p^e)$), whence $\#(\mathcal{O}_K/\pi\mathcal{O}_K)=p$: the natural map $\mathbf{Z}/p\,\mathbf{Z}\to\mathcal{O}_K/\pi\mathcal{O}_K$ is an isomorphism.
• This implies that $\mathcal{O}_K=\mathbf{Z}+\pi\mathcal{O}_K$, *i.e.* $\mathcal{O}_K=\mathbf{Z}[\zeta]+\pi\mathcal{O}_K$. If $k\in\mathbf{Z}_{>0}$ and $\mathcal{O}_K=\mathbf{Z}[\zeta]+\pi^k\mathcal{O}_K$, we thus have $\mathcal{O}_K=\mathbf{Z}[\zeta]+\pi^k(\mathbf{Z}[\zeta]+\pi\mathcal{O}_K)=\mathcal{O}_K=\mathbf{Z}[\zeta]+\pi^{k+1}\mathcal{O}_K$: by induction, we deduce $\mathcal{O}_K=\mathbf{Z}[\zeta]+\pi^k\mathcal{O}_K$ for all $k\in\mathbf{Z}_{>0}$. In particular, we have $\mathcal{O}_K=\mathbf{Z}[\zeta]+\pi^{\varphi(p^e)c}\mathcal{O}_K$, *i.e.* $\mathcal{O}_K=\mathbf{Z}[\zeta]+p^c\mathcal{O}_K$. As $\#(\mathcal{O}_K/\mathbf{Z}[\zeta])\mid p^c$, we have $p^c\mathcal{O}_K\subseteq\mathbf{Z}[\zeta]$, so that $\mathcal{O}_K\,\mathbf{Z}[\zeta]$.
• As $[\mathcal{O}_K:\mathbf{Z}[\zeta]]=1$, we deduce that $|d_K|=p^c=p^{p^{e-1}(pe-e-1)}$. □

Lemma 8.2.8. Let K and L be number fields such that $[KL:\mathbf{Q}]=[K:\mathbf{Q}][L:\mathbf{Q}]$ and $\mathsf{gcd}(d_K,d_L)=1$. Then $\mathcal{O}_{KL}=\mathcal{O}_K\mathcal{O}_L$ and $d_{LK}=d_K^{[L:\mathbf{Q}]}d_L^{[K:\mathbf{Q}]}$.

Proof. • We have of course $\mathcal{O}_K\mathcal{O}_L\subset\mathcal{O}_{KL}$. Let $(x_1,\dots,x_n)$ (resp. $(y_1,\dots,y_m)$) be a basis of $\mathcal{O}_K$ (resp. $\mathcal{O}_L$) over $\mathbf{Z}$. Then $K=\bigoplus\limits_{i=1}^{n}\mathbf{Q}\,x_i$ and $L=\bigoplus\limits_{j=1}^{m}\mathbf{Q}\,y_j$, so $KL=\sum\limits_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}}\mathbf{Q}\,x_iy_j$. As $[KL:\mathbf{Q}]=[K:\mathbf{Q}][L:\mathbf{Q}]=nm$ by hypothesis, this implies that $(x_iy_j)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}}$ is a basis of KL over $\mathbf{Q}$. Now let $\alpha\in\mathcal{O}_{KL}$: we can write $\alpha=\sum\limits_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}}\lambda_{i,j}x_iy_j$ with $(\lambda_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}}\in\mathbf{Q}^{nm}$. Let $\delta\in\mathbf{Z}_{>0}$ be the lcm of the denominators of the $\lambda_{i,j}$: we have $\delta\alpha=\sum\limits_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}}a_{i,j}x_iy_j$ where $a_{i,j}=\delta\lambda_{i,j}\in\mathbf{Z}$ and δ is prime to $\mathsf{gcd}_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}}(a_{i,j})$. For $i\in\{1,\dots,n\}$, put $\alpha_i=\sum\limits_{j=1}^{m}a_{i,j}y_j\in\mathcal{O}_L$: we have $\delta\alpha=\sum\limits_{i=1}^{n}\alpha_ix_i$.
Let $\sigma\colon K\to\mathbf{C}$ be a field homomorphism. Let θ be a primitive element for L, so that $L=\mathbf{Q}(\theta)$, and $KL=K(\theta)$. By hypothesis, we have $[K(\theta):K]=[KL:K]=\frac{[KL:\mathbf{Q}]}{[K:\mathbf{Q}]}=[L:\mathbf{Q}]=[\mathbf{Q}(\theta):\mathbf{Q}]$. This means that the degree of θ over K is equal to that over $\mathbf{Q}$, so that the minimal polynomial of θ over K is equal to that over $\mathbf{Q}$ (without the degree assumption, we only know that the former divides the latter). By the isomorphism extension theorem, there exists a unique field homomorphism $\widehat{\sigma}\colon KL\to\mathbf{C}$ that extends σ and such that $\widehat{\sigma}(\theta)=\theta$, implying $\widehat{\sigma}_{|L}=\mathsf{Id}_L$. We thus have $\delta\widehat{\sigma}(\alpha)=\sum\limits_{i=1}^{n}\alpha_i\sigma(x_i)$. The collection of those equalities for all $\sigma\in I:=\mathsf{Hom}_{\mathbf{Q}\text{-alg}}(K,\mathbf{C})$ provides a Cramer linear system $\delta Y=XM$ where $X=(\alpha_1,\dots,\alpha_n)\in\mathcal{O}_L^n$, $Y=(\widehat{\sigma}(\alpha))_{\sigma\in I}\in\mathcal{O}_{KL}^n$ and $M=(\sigma(x_i))_{\substack{1\leqslant i\leqslant n\\\sigma\in I}}\in\mathsf{M}_n(\mathcal{O}_K)$. Multiplying on the right by the transpose $\widetilde{M}\in\mathsf{M}_n(\mathcal{O}_K)$ of the adjugate matrix of M, we get $\delta Y\widetilde{M}=\det(M)X$. As $(x_1,\dots,x_n)$ is a basis of $\mathcal{O}_K$ over $\mathbf{Z}$, there exists a column vector $V\in\mathbf{Z}^n$ such that $XV=1$, so that $\delta Y\widetilde{M}V=\det(M)$. As $d_K=\det(M)^2$ (*cf* proposition 1.10.22), this shows that $\delta\det(M)Y\widetilde{M}V=d_K$, hence $\delta\mid d_K$. Symmetrically, we have $\delta\mid d_L$: as $\mathsf{gcd}(d_K,d_L)=1$, we have $\delta=1$, and $\alpha=\sum\limits_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}}a_{i,j}x_iy_j\in\mathcal{O}_K\mathcal{O}_L$, showing the equality $\mathcal{O}_{KL}=\mathcal{O}_K\mathcal{O}_L$.

[49] This is the formula $\mathrm{D}(1,x,x^2,\dots,x^{n-1})=(-1)^{\frac{n(n-1)}{2}}\mathsf{N}_{F(x)/F}(P'_{x,F}(x))$ for x separable of degree n over F.

- Keeping the preceding notation, $(x_iy_j)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}}$ is a basis of $\mathcal{O}_{KL}$ over $\mathbf{Z}$. By proposition 1.10.24, we have

$$\begin{aligned} d_{KL} &= \mathrm{D}(x_iy_j)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}} = \mathrm{D}(x_1,\dots,x_n)^{[L:K]}\,\mathsf{N}_{K/\mathbf{Q}}(\mathrm{D}(y_1,\dots,y_m)) \\ &= d_K^{[KL:K]}\,\mathsf{N}_{K/\mathbf{Q}}(d_L) = d_K^{[L:\mathbf{Q}]}d_L^{[K:\mathbf{Q}]} \end{aligned}$$

since $[KL:K]=[L:\mathbf{Q}]$ by hypothesis, and $\mathsf{N}_{K/\mathbf{Q}}(d_L)=d_L^{[K:\mathbf{Q}]}$ because $d_L\in\mathbf{Q}$. □

Remark 8.2.9. A reformulation of the second statement is $\frac{\ln(d_{KL})}{[KL:\mathbf{Q}]}=\frac{\ln(d_K)}{[K:\mathbf{Q}]}+\frac{\ln(d_L)}{[L:\mathbf{Q}]}$.

Theorem 8.2.10. Let $n\in\mathbf{Z}_{>0}$. The ring of integers of $\mathbf{Q}(\zeta_n)$ is $\mathbf{Z}[\zeta_n]$ and $\left|d_{\mathbf{Q}(\zeta_n)}\right| = \frac{n^{\varphi(n)}}{\prod\limits_{p\mid n}p^{\frac{\varphi(n)}{p-1}}}$.

Proof. Write $n=\prod\limits_{i=1}^{r}p_i^{e_i}$. We proceed by induction on $r\in\mathbf{N}$, the cases $r=0$ being trivial, and $r=1$ being proposition 8.2.7. Assume $r>1$, and put $m=\prod\limits_{i=1}^{r-1}p_i^{e_i}$, so that $n=mp_r^{e_r}$ and $\mathsf{gcd}(m,p^{e_r})$. Put $K=\mathbf{Q}(\zeta_m)$ and $L=\mathbf{Q}(\zeta_{p_r^{e_r}})$. We have $KL=\mathbf{Q}(\zeta_n)$ (since $\zeta_m\zeta_{p_r^{e_r}}$ is a primitive n-th root of unity because $\mathsf{gcd}(m,p^{e_r})=1$). This implies that

$$[KL:\mathbf{Q}]=\varphi(n)=\varphi(m)\varphi(p_r^{e_r})=[K:\mathbf{Q}][L:\mathbf{Q}]$$

(again because $\mathsf{gcd}(m,p^{e_r})=1$). Moreover, the induction hypothesis implies that the prime dividing d_K (resp. d_L) are $p_1,\dots,p_{r-1}$ (resp. p_r), so that $\mathsf{gcd}(d_K,d_L)=1$. This shows that one may apply lemma 8.2.8, so that $\mathcal{O}_{\mathbf{Q}(\zeta_n)}=\mathcal{O}_K\mathcal{O}_L=\mathbf{Z}[\zeta_m]\,\mathbf{Z}[\zeta_{p_r^{e_r}}]=\mathbf{Z}[\zeta_n]$ and

$$d_{\mathbf{Q}(\zeta_n)}=d_K^{[L:\mathbf{Q}]}d_L^{[K:\mathbf{Q}]}=\pm\left(\frac{m^{\varphi(m)}}{\prod\limits_{p\mid m}p^{\frac{\varphi(m)}{p-1}}}\right)^{\varphi(p_r^{e_r})}\frac{p_r^{e_r\varphi(p_r^{e_r})\varphi(m)}}{p_r^{\frac{\varphi(p_r^{e_r})}{p_r-1}\varphi(m)}}=\pm\frac{n^{\varphi(n)}}{\prod\limits_{p\mid n}p^{\frac{\varphi(n)}{p-1}}}$$

since $\varphi(m)\varphi(p_r^{e_r})=\varphi(n)$. □

Corollary 8.2.11. The prime that ramify in $\mathbf{Q}(\zeta_n)$ are precisely those dividing n.

Proof. This follows from corollary 2.6.6. □

8.2.12. *Ramification of cyclotomic extensions of* $\mathbf{Q}_p$. Let p be a prime and $n\in\mathbf{Z}_{>0}$. Write $n=p^en'$ with $n'\in\mathbf{Z}_{>0}$ prime to p. Let $f\in\mathbf{Z}_{>0}$ be the order of p in $(\mathbf{Z}/n'\mathbf{Z})^\times$ (so that f is the least positive integer such that $n'\mid p^f-1$, and $f\mid\varphi(n')$).

Proposition 8.2.13. The absolute ramification index of $\mathbf{Q}_p(\zeta_n)$ is $\varphi(p^e)$, and its residual degree is f. In particular, we have $[\mathbf{Q}_p(\zeta_n):\mathbf{Q}_p]\mid\varphi(n)$, with equality if and only if p is a generator of $(\mathbf{Z}/n'\mathbf{Z})^\times$.

Proof. • As $p\nmid n'$, the polynomial $X^{n'}-1$ is separable over $\mathbf{F}_p[X]$: so is the cyclotomic polynomial $\Phi_{n'}(X)$. If $\alpha\in\overline{\mathbf{F}}_p$ is a root of $\Phi_{n'}$, the order of α in the multiplicative group $\overline{\mathbf{F}}_p^\times$ is n': if $i\in\mathbf{Z}_{>0}$, we have $\alpha^{p^i}=\alpha\Leftrightarrow\alpha^{p^i-1}=1\Leftrightarrow n'\mid p^i-1\Leftrightarrow f\mid i$. This implies that the field of decomposition of $\Phi_{n'}$ is $\mathbf{F}_{p^f}$. The roots of $\Phi_{n'}$ lift uniquely into roots of $\Phi_{n'}$ in $\mathbf{Q}_{p^f}$ (which is the unique unramified subextension of $\overline{\mathbf{Q}}_p/\mathbf{Q}_p$ lifting $\mathbf{F}_{p^f}/\mathbf{F}_p$, *cf* theorem 3.8.7). This implies that $\mathbf{Q}_p(\zeta_{n'})\subset\mathbf{Q}_{p^f}$. As the image of $\zeta_{n'}$ in $\kappa_{\mathbf{Q}_p(\zeta_{n'})}$ generates $\mathbf{F}_{p^f}$, we also have

$$f=[\mathbf{F}_{p^f}:\mathbf{F}_p]\leqslant[\kappa_{\mathbf{Q}_p(\zeta_{n'})}:\mathbf{F}_p]\leqslant[\mathbf{Q}_p(\zeta_{n'}):\mathbf{Q}_p]\leqslant[\mathbf{Q}_{p^f}:\mathbf{Q}_p]=f$$

we have $\mathbf{Q}_p(\zeta_{n'})=\mathbf{Q}_{p^f}$ so $[\mathbf{Q}_p(\zeta_{n'}):\mathbf{Q}_p]=f$ and $\mathbf{Q}_p(\zeta_{n'})/\mathbf{Q}_p$ is unramified.

- We have $\Phi_{p^e}(X)=\Phi_p(X^{p^{e-1}})$, so $\Phi_{p^e}(X+1)=\Phi_p((X+1)^{p^{e-1}})\equiv\Phi_p(X^{p^{e-1}}+1)\mod p\,\mathbf{Z}[X]$. As $\Phi_p(Y+1)=\frac{(Y+1)^p-1}{Y}\equiv Y^{p-1}\mod p\,\mathbf{Z}[Y]$, we have $\Phi_{p^e}(X+1)\equiv X^{(p-1)p^{e-1}}\mod p\,\mathbf{Z}[X]$. Moreover, we have $\Phi_{p^e}(1)=\Phi_p(1)=p$. This implies that the $\Phi_{p^e}(X+1)\in\mathbf{Q}_{p^f}[X]$ is an Eisenstein polynomial: it is irreducible, and $[\mathbf{Q}_{p^f}(\zeta_{p^e}):\mathbf{Q}_{p^f}]=\deg(\Phi_{p^e}(X+1))=\varphi(p^e)$. This also implies that the extension $\mathbf{Q}_{p^f}(\zeta_{p^e})/\mathbf{Q}_{p^f}$ is totally ramified, with uniformizer $\zeta_{p^e}-1$ (so that $v_p(\zeta_{p^e}-1)=\frac{1}{\varphi(p^e)}=\frac{1}{p^{e-1}(p-1)}$).
- We have $\mathbf{Q}_p(\zeta_{n'},\zeta_{p^e})=\mathbf{Q}_p(\zeta_n)$ (as $\mathsf{gcd}(p,n')=1$, the element $\zeta_{n'}\zeta_{p^e}$ is a primitive n-th root of unity). This implies that $\mathbf{Q}_p(\zeta_n)=\mathbf{Q}_{p^f}(\zeta_{p^e})$, showing that the ramification index of $\mathbf{Q}_p(\zeta_n)/\mathbf{Q}_p$ is $\varphi(p^e)$ and that its residual degree is f. In particular, we have $[\mathbf{Q}_p(\zeta_n):\mathbf{Q}_p]=\varphi(p^e)f$. As f is the order of p in the group $(\mathbf{Z}/n'\mathbf{Z})^\times$, we have $f\mid\#(\mathbf{Z}/n'\mathbf{Z})^\times=\varphi(n')$, hence $[\mathbf{Q}_p(\zeta_n):\mathbf{Q}_p]\mid\varphi(p^e)\varphi(n')=\varphi(n)$, with equality if and only if p generates $(\mathbf{Z}/n'\mathbf{Z})^\times$. □

Corollary 8.2.14. Under the assumptions of proposition 8.2.13, the inertia subgroup of $\mathbf{Q}_p(\zeta_n)/\mathbf{Q}_p$ is isomorphic to $(\mathbf{Z}/p^e\mathbf{Z})^\times$.

Proof. This follows from the discussion in paragraph 8.1 applied to $F = \mathbf{Q}_{p^f}$, using the irreducibility of Φ_{p^e} over $\mathbf{Q}_{p^f}$. □

Remark 8.2.15. As a special case of last proposition, we have $\mathbf{Q}_{p^f} = \mathbf{Q}_p(\zeta_{p^f-1})$.

8.2.16. *The field* $\mathbf{Q}_p(\zeta_p)$.

Lemma 8.2.17. $\mathbf{Q}_p(\zeta_p) = \mathbf{Q}_p\left((-p)^{\frac{1}{p-1}}\right)$.

Proof. We have $\Phi_p(X+1) = \frac{(X+1)^p-1}{X} = X^{p-1} + \sum\limits_{i=1}^{p-1}\binom{p}{i}X^{i-1}$, so $(\zeta_p-1)^{p-1} = -\sum\limits_{i=1}^{p-1}\binom{p}{i}(\zeta_p-1)^{i-1}$, hence $(\zeta_p-1)^{p-1} \equiv -p \mod p(\zeta_p-1)\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$, *i.e.* $u := \frac{(\zeta_p-1)^{p-1}}{-p} \equiv 1 \mod (\zeta_p-1)\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$. As $(\zeta_p-1)\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$ is the maximal ideal of $\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$, we have $u \in \mathcal{O}_{\mathbf{Q}_p(\zeta_p)}^\times$. Moreover, a straightforward induction implies that $u^{p^i} \equiv 1 \mod p^i(\zeta_p-1)\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$. This shows that the sequence $\left(u^{-1+p+p^2+\cdots+p^n}\right)_{n\in\mathbf{Z}_{\geqslant 0}}$ converges to some element $u_1 \in \mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$, such that $u_1^{p-1} = u$. We have $u_1 \in \mathcal{O}_{\mathbf{Q}_p(\zeta_p)}^\times$, and $(\zeta_p-1)^{p-1} = -pu_1^{p-1}$, *i.e.* $\alpha = \frac{\zeta_p-1}{u_1} \in \mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$ is a root of $X^{p-1}+p$. As the latter is an Eisenstein polynomial, the inclusion $\mathbf{Q}_p(\alpha) \subset \mathbf{Q}_p(\zeta_p)$ is a equality. □

Remark 8.2.18. The extension $\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p$ is totally tamely ramified of degree $p-1$: we knew *a priori* that there exists a uniformizer ϖ of $\mathbf{Q}_p$ such that $\mathbf{Q}_p(\zeta_p) = \mathbf{Q}_p\left(\varpi^{\frac{1}{p-1}}\right)$ (*cf* theorem 3.8.28).

Let $v\colon \mathbf{Q}_p(\zeta_p)^\times \to \mathbf{Z}$ be the normalized valuation, so that $v(\pi) = 1$ where $\pi = \zeta_p - 1$, and

$$U = \{x \in \mathcal{O}_{\mathbf{Q}_p(\zeta_p)}\,;\, x \equiv 1 \mod \pi\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}\}$$

the group of principal units. As the residue field of $\mathbf{Q}_p(\zeta_p)$ is $\mathbf{F}_p$, we have

$$\mathbf{Q}_p(\zeta_p)^\times \simeq \pi^{\mathbf{Z}} \times \mu_{p-1} \times U.$$

Lemma 8.2.19. We have $U^p := \{u^p\,;\, u \in U\} = \left\{x \in \mathcal{O}_{\mathbf{Q}_p(\zeta_p)}\,;\, x \equiv 1 \mod \pi^{p+1}\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}\right\}$.

Proof. • Let $u \in U$. As the residue field of $\mathbf{Q}_p(\zeta_p)$ is $\mathbf{F}_p$, we have $\mathcal{O}_{\mathbf{Q}_p(\zeta_p)} = \mathbf{Z} + \pi\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$: we can write $u \equiv 1 - n\pi \mod \pi^2\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$ with $n \in \mathbf{Z}_{\geqslant 0}$. As $\zeta_p^n = (1+\pi)^n \equiv 1 + n\pi \mod \pi^2\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$, we have thus $\zeta_p^n u \equiv 1 \mod \pi^2\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$: write $\zeta_p^n u = 1 + \pi^2 y$ with $y \in \mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$. Raising to the p-th power, we get

$$u^p = 1 + \sum_{i=1}^{p-1}\binom{p}{i}\pi^{2i}y^i + \pi^{2p}y^p \equiv 1 \mod \pi^{p+1}\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$$

since $\binom{p}{i} \in p\mathcal{O}_{\mathbf{Q}_p(\zeta_p)} = \pi^{p-1}\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$ for $i \in \{1,\ldots,p-1\}$ (because $v(p) = p-1 = v(\pi^{p-1})$), and $p+1 \leqslant 2p$.
• Conversely, let $x \in 1 + \pi^{p+1}\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$. Write $x = 1 + \pi^{p+1}z$ with $z \in \mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$: we have to show that x is the p-th power of some $u \in U$. We have

$$\left(\sum_{n=0}^{\infty}\binom{1/p}{n}X^n\right)^p = 1 + X$$

in $\mathbf{Q}[\![X]\!]$. If $n \in \mathbf{Z}_{\geqslant 0}$, we have

$$\binom{1/p}{n} = \frac{1}{n!}\frac{1}{p}\left(\frac{1}{p}-1\right)\left(\frac{1}{p}-2\right)\cdots\left(\frac{1}{p}-n+1\right) = \frac{(1-p)(1-2p)\cdots(1-(n-1)p)}{n!p^n}$$

This implies that $v_p\left(\binom{1/p}{n}\right) = -n - v_p(n!) = -n - \frac{n-s(n)}{p-1}$, where $s(n)$ denotes the sum of the digits of n written in base p. In particular, we have $v\left(\binom{1/p}{n}(\pi^{p+1}z)^n\right) \geqslant (p+1)n - (p-1)\left(n + \frac{n-s(n)}{p-1}\right) = n + s(n) \geqslant n$. This implies that the series

$$u = \sum_{n=0}^{\infty}\binom{1/p}{n}\left(\pi^{p+1}z\right)^n$$

converges in $\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$, and that $u^p = 1 + \pi^{p+1}z = x$, as required. □

8.3. **Proof of Kronecker-Weber Theorem.**

8.3.1. *Reduction of theorem 8.1.1 to theorem 8.1.2 for all p.* Assume that theorem 8.1.2 holds for every prime p and let $K/\mathbf{Q}$ be an abelian extension. Let Σ be the set of primes p that ramify in $K/\mathbf{Q}$ (*i.e.* such that $p \mid d_K$, *cf* corollary 2.6.6). If $p \in \Sigma$ and $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal lying over p, denote by $\widehat{K}_{\mathfrak{p}}$ the completion of K with respect to $\mathfrak{p}$. The extension $\widehat{K}_{\mathfrak{p}}/\mathbf{Q}_p$ is abelian, and its Galois group identifies the decomposition subgroup

$$D_p(K/\mathbf{Q}) = \{\sigma \in \mathsf{Gal}(K/\mathbf{Q})\,;\, \sigma(\mathfrak{p}) = \mathfrak{p}\} \leqslant \mathsf{Gal}(K/\mathbf{Q})$$

(*cf* propositions 3.5.15 and 8.2.3). By theorem 8.1.2, there exists $n_p \in \mathbf{Z}_{>0}$ such that $\widehat{K}_{\mathfrak{p}} \subset \mathbf{Q}_p(\zeta_{n_p})$. Put $e_p = v_p(n_p)$ and $n = \prod\limits_{p\in\Sigma} p^{e_p}$: it is enough to prove that $K \subset \mathbf{Q}(\zeta_n)$.

Put $L = K(\zeta_n) = \mathbf{Q}(\zeta_n)K$: the extension $L/\mathbf{Q}$ is abelian since $K/\mathbf{Q}$ and $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ are (*cf* proposition 8.2.2). Let $\mathfrak{P} \subset \mathcal{O}_L$ be a prime ideal lying over $\mathfrak{p}$, and $\widehat{L}_{\mathfrak{P}}$ the completion of L with respect to $\mathfrak{P}$. We have the diagram of fields:

$$\begin{tikzcd}
& \widehat{L}_{\mathfrak{P}} \arrow[dl, dash] \arrow[dr, dash] & \\
\widehat{K}_{\mathfrak{p}} \arrow[dr, dash] & & \mathbf{Q}_p(\zeta_n) \arrow[dl, dash] \\
& \mathbf{Q}_p &
\end{tikzcd}$$

As $\widehat{L}_{\mathfrak{P}} = \mathbf{Q}_p(\zeta_n)\widehat{K}_{\mathfrak{p}}$, the extension $\widehat{L}_{\mathfrak{P}}/\mathbf{Q}_p$ is unramified if and only if $\widehat{K}_{\mathfrak{p}}$ and $\mathbf{Q}_p(\zeta_n)$ are (*cf* corollaries 3.8.9 and 3.8.11). This implies that the primes p that ramify in L are precisely those in Σ (since the prime that ramify in $\mathbf{Q}(\zeta_n)$ are the elements of Σ by corollary 8.2.11).

For $p \in \Sigma$, we have $\widehat{K}_{\mathfrak{p}} \subset \mathbf{Q}_p(\zeta_{n_p})$, so that

$$\mathbf{Q}_p(\zeta_{p^{e_p}}) \subset \widehat{L}_{\mathfrak{P}} \subset \mathbf{Q}_p(\zeta_{n_p}, \zeta_n) = \mathbf{Q}_p(\zeta_{p^{e_p}n'})$$

for some $n' \in \mathbf{Z}_{>0}$ prime to p. Let $I_p = I_p(L/\mathbf{Q})$ be the inertia group of $L/\mathbf{Q}$ at p. By corollary 8.2.14, we have

$$I_p \simeq \mathsf{Gal}(\mathbf{Q}_p(\zeta_{p^{e_p}})/\mathbf{Q}_p) \simeq (\mathbf{Z}/p^{e_p}\mathbf{Z}_p)^\times$$

Let $I \leqslant \mathsf{Gal}(L/\mathbf{Q})$ be the subgroup generated by all the I_p for $p \in \Sigma$. As $\mathsf{Gal}(L/\mathbf{Q})$ hence I is abelian, the natural map $\prod\limits_{p\in\Sigma} I_p \to I$ is a surjective group homomorphism, so that

$$\#I \leqslant \prod_{p\in\Sigma} \#I_p = \prod_{p\in\Sigma} \varphi(p^{e_p}) = \varphi(n) = [\mathbf{Q}(\zeta_n) : \mathbf{Q}].$$

Let $F \subset \mathbf{Q}(\zeta_n)$ be the field fixed by I. The primes ramified in F are ramified in L: they belong to Σ. As we killed the ramification at p by taking invariants under I_p for all $p \in \Sigma$, this implies that $F/\mathbf{Q}$ is nowhere ramified, *i.e.* that $|d_F| = 1$. Minkowski bound $\sqrt{|d_F|} \geqslant \big(\frac{\pi}{4}\big)^d \frac{d^d}{d!}$ (where $d = [F : \mathbf{Q}]$) implies that $F = \mathbf{Q}$, so that

$$[L : \mathbf{Q}] = [L : F] = \#I \leqslant [\mathbf{Q}(\zeta_n) : \mathbf{Q}].$$

As $\mathbf{Q}(\zeta_n) \subset L$, this implies $L = \mathbf{Q}(\zeta_n)$, hence $K \subset \mathbf{Q}(\zeta_n)$.

8.3.2. *Proof of theorem 8.1.2.* Let $K/\mathbf{Q}_p$ be an abelian extension. We can write $\mathsf{Gal}(K/\mathbf{Q}_p) = \prod\limits_{i=1}^{r} G_i$ where G_i is cyclic of prime power order. Then $K = K_1 \cdots K_r$ where K_i is the field fixed by $\prod\limits_{\substack{1\leqslant j\leqslant r\\ j\neq i}} G_j$. As the composite of finitely many cyclotomic extensions is again a cyclotomic extension, it is enough to show that each K_i is included in a cyclotomic extension of $\mathbf{Q}_p$: we are reduced to the case where $\mathsf{Gal}(K/\mathbf{Q}_p) \simeq \mathbf{Z}/q^m\mathbf{Z}$ is cyclic of prime power order.

Case where $p \neq q$. Let T be the maximal unramified subextension of $K/\mathbf{Q}_p$. If $f = [T : \mathbf{Q}_p]$, then T is the unique unramified subextension of $\overline{\mathbf{Q}}_p$ lifting $\mathbf{F}_{p^f}/\mathbf{F}_p$, *i.e.* $T = \mathbf{Q}_{p^f} = \mathbf{Q}_p(\zeta_{p^f-1})$, *cf* remark 8.2.15. As $[K : \mathbf{Q}_p] = q^m$ and $p \neq q$, the degree of the totally ramified extension K/T is of the form $e = q^r$ with $r \in \{0, \ldots, m\}$, whence prime to p: it is tamely ramified. By theorem 3.8.28, there exists a uniformizer π of $T = \mathbf{Q}_{p^f}$ such that $K = \mathbf{Q}_{p^f}\big(\pi^{\frac{1}{e}}\big)$. As π and p are uniformizers of $\mathbf{Q}_{p^f}$, there exists $u \in \mathbf{Z}_{p^f}^\times$ such that $\pi = -up$. As u is a unit and $p \neq q$, the extension $\mathbf{Q}_{p^f}\big(u^{\frac{1}{e}}\big)/\mathbf{Q}_{p^f}$ is unramified: so is

$\mathbf{Q}_{p^f}\big(u^{\frac{1}{e}}\big)/\mathbf{Q}_p$. By remark 8.2.15 again, we have $\mathbf{Q}_{p^f}\big(u^{\frac{1}{e}}\big) = \mathbf{Q}_p(\zeta_M)$ for some $M \in \mathbf{Z}_{>0}$ prime to p. Note that in $K(\zeta_M) = \mathbf{Q}_{p^f}\big(\pi^{\frac{1}{e}}, u^{\frac{1}{e}}\big)$, we have $\Big(\frac{\pi^{\frac{1}{e}}}{u^{\frac{1}{e}}}\Big)^e = -p$, so that $(-p)^{\frac{1}{e}} \in K(\zeta_M)$.

$$\begin{tikzcd}[column sep=small]
 & K(\zeta_M) \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \mathbf{Q}_p(\zeta_M) \arrow[dl, dash] \\
 & \mathbf{Q}_p &
\end{tikzcd}$$

Being the composite of the abelian extensions $K/\mathbf{Q}_p$ and $\mathbf{Q}_p(\zeta_M)/\mathbf{Q}_p$, the extension $K(\zeta_M)/\mathbf{Q}_p$ is abelian: so is its subextension $\mathbf{Q}_p\big((-p)^{\frac{1}{e}}\big)/\mathbf{Q}_p$ (*cf* proposition 8.2.2). In particular, it is Galois, hence contains the conjugates of $(-p)^{\frac{1}{e}}$ over $\mathbf{Q}_p$: we have $\zeta_e \in \mathbf{Q}_p\big((-p)^{\frac{1}{e}}\big)$. Moreover, the extension $\mathbf{Q}_p\big((-p)^{\frac{1}{e}}\big)/\mathbf{Q}_p$ is totally ramified: so is its subextension $\mathbf{Q}_p(\zeta_e)/\mathbf{Q}_p$. By proposition 8.2.13, this implies that $e = q^r \mid p-1$ (recall that $p \neq q$), so that $(-p)^{\frac{1}{e}} \in \mathbf{Q}_p\big((-p)^{\frac{1}{p-1}}\big) = \mathbf{Q}_p(\zeta_p)$ (*cf* lemma 8.2.17), *i.e.*

$$\pi^{\frac{1}{e}} = (-p)^{\frac{1}{e}} u^{\frac{1}{e}} \in \mathbf{Q}_p(\zeta_M, \zeta_p) = \mathbf{Q}_p(\zeta_{Mp}).$$

Finally, we have $K \subset \mathbf{Q}_p(\zeta_{Mp})$, finishing the proof in that case.

Case where $p = q \neq 2$. The extension $K_u := \mathbf{Q}_p(\zeta_{p^{p^m}-1})/\mathbf{Q}_p$ is unramified and cyclic of degree p^m (*cf* remark 8.2.15). On the other hand, the extension $\mathbf{Q}_p(\zeta_{p^{m+1}})/\mathbf{Q}_p$ is totally ramified, with Galois group isomorphic to $(\mathbf{Z}/p^{m+1}\mathbf{Z})^\times$, hence cyclic (since $p \neq 2$). Let K_r be its subfield fixed by the subgroup of order $p-1$: the extension $K_r/\mathbf{Q}_p$ is totally ramified and cyclic of degree p^m. This implies that $[K_uK_r] = p^{2m}$ (since the ramification index of $K_uK_r/\mathbf{Q}_p$ is at least $[K_r : \mathbf{Q}_p] = p^m$ and the residual degree at least $[K_u : \mathbf{Q}_p] = p^m$). By proposition 8.2.2, the extension $K_uK_r/\mathbf{Q}_p$ is abelian. As the group homomorphism

$$\mathsf{Gal}(K_uK_r/\mathbf{Q}_p) \to \mathsf{Gal}(K_u/\mathbf{Q}_p) \times \mathsf{Gal}(K_r/\mathbf{Q}_p)$$

(given by the restrictions) is injective, it is an isomorphism by cardinality, so that

$$\mathsf{Gal}(K_uK_r/\mathbf{Q}_p) \simeq (\mathbf{Z}/p^m\mathbf{Z})^2.$$

Assume $K \not\subset K_uK_r$. As above, the group homomorphism given by the restrictions

$$\mathsf{Gal}(KK_uK_r/\mathbf{Q}_p) \to \mathsf{Gal}(K_uK_r/\mathbf{Q}_p) \times \mathsf{Gal}(K/\mathbf{Q}_p) \simeq (\mathbf{Z}/p^m\mathbf{Z})^3$$

is injective: let H be its image. By the invariant factors decomposition (*cf* theorem 1.4.13), we have

$$H \simeq (\mathbf{Z}/p^{m_1}\mathbf{Z}) \times (\mathbf{Z}/p^{m_2}\mathbf{Z}) \times (\mathbf{Z}/p^{m_3}\mathbf{Z})$$

for unique integers $m_1 \geqslant m_2 \geqslant m_3$. As H is killed by p^m, we have $m_i \leqslant m$ for all $i \in \{1,2,3\}$. As the restriction $\mathsf{Gal}(KK_uK_r/\mathbf{Q}_p) \to \mathsf{Gal}(K_uK_r/\mathbf{Q}_p) \simeq (\mathbf{Z}/p^m\mathbf{Z})^2$ is surjective, we have $\dim_{\mathbf{F}_p}(p^{m-1}H) \geqslant 2$, so that $m_1 = m_2 = m$. We have $m' := m_3 > 0$, otherwise we would have $[KK_uK_r : \mathbf{Q}_p] = p^{2m} = [K_uK_r : \mathbf{Q}_p]$, implying that $K \subset K_uK_r$ contradicting the hypothesis. This implies in particular that

$$\mathsf{Gal}(KK_uK_r/\mathbf{Q}_p) \simeq (\mathbf{Z}/p^m\mathbf{Z})^2 \times (\mathbf{Z}/p^{m'}\mathbf{Z})$$

has a quotient isomorphic to $(\mathbf{Z}/p\mathbf{Z})^3$: there exists a Galois subextension N of $KK_uK_r/\mathbf{Q}_p$ such that

$$\mathsf{Gal}(N/\mathbf{Q}_p) \simeq (\mathbf{Z}/p\mathbf{Z})^3.$$

This is impossible by lemma 8.3.4 below: we must have $K \subset K_uK_r \subset \mathbf{Q}_p(\zeta_{p^m}, \zeta_{p^{p^m}-1}) = \mathbf{Q}_p(\zeta_{p^{m+1}(p^{p^m}-1)})$, finishing the proof in that case.

Lemma 8.3.3. Let F be a field of characteristic different from p, $M = \mathbf{Q}_p(\zeta_p)$ and $L = M\big(a^{\frac{1}{p}}\big)$ with $a \in M^\times$. Let $\chi\colon \mathsf{Gal}(M/F) \to \mathbf{Z}/p\mathbf{Z}$ be the cyclotomic character. The following are equivalent:

(i) L/F is abelian;

(ii) $(\forall\sigma \in \mathsf{Gal}(M/F))\, \sigma(a) \equiv a^{\chi(\sigma)} \mod M^{\times p}$.

Note that $\mathbf{Z}/p\mathbf{Z}$ acts on $M^\times/M^{\times p}$, so that $a^{\chi(\sigma)} \mod M^{\times p}$ makes sense.

Proof. • Assume (i). Let $\sigma \in \mathsf{Gal}(M/F)$, and fix $\widehat{\sigma} \in \mathsf{Gal}(L/F)$ extending σ. If $\tau \in \mathsf{Gal}(L/M)$, there exists $c_\tau \in \mathbf{Z}/p\mathbf{Z}$ such that $\tau\big(a^{\frac{1}{p}}\big) = \zeta_p^{c_\tau} a^{\frac{1}{p}}$. As $\mathsf{Gal}(L/F)$ is abelian, we have

$$(\tau \circ \widehat{\sigma})\big(a^{\frac{1}{p}}\big) = (\widehat{\sigma} \circ \tau)\big(a^{\frac{1}{p}}\big) = \zeta_p^{c_\tau \chi(\sigma)} \widehat{\sigma}\big(a^{\frac{1}{p}}\big)$$

Let $k \in \mathbf{Z}$ mapping to $\chi(\sigma)$ in $\mathbf{Z}/p\mathbf{Z}$: we have $\tau\big(a^{\frac{k}{p}}\big) = \zeta_p^{kc_\tau} a^{\frac{k}{p}} = \zeta_p^{c_\tau\chi(\sigma)}\zeta_p^{kc_\tau} a^{\frac{k}{p}}$. Put $\alpha = \frac{\widehat{\sigma}\left(a^{\frac{1}{p}}\right)}{a^{\frac{k}{p}}} \in L^\times$. What precedes implies that $\tau(\alpha) = \alpha$. As this holds for all $\tau \in \mathsf{Gal}(L/M)$, we have $\alpha \in M^\times$: raising to the p-th power gives $\sigma(a) = \widehat{\sigma}(a) = a^k\alpha^p$, which precisely means that $\sigma(a) \equiv a^{\chi(\sigma)} \mod M^{\times p}$.

• Assume (ii). As $\mathsf{char}(F) \neq p$, the extensions L/M and M/F are separable: so is the extension L/F. If $\gamma \in \mathsf{Hom}_{K\text{-alg}}(L, \overline{F})$, we have $\gamma_{|M} \in \mathsf{Gal}(M/F)$. Fix $k \in \mathbf{Z}$ mapping to $\chi(\gamma_{|M})$ in $\mathbf{Z}/p\mathbf{Z}$. By hypothesis, there exists $\alpha \in M^\times$ such that $\gamma\big(a^{\frac{1}{p}}\big)^p = \gamma_{|M}(a) = a^k\alpha^p$: there exists $i \in \mathbf{Z}/p\mathbf{Z}$ such that

$$\gamma\big(a^{\frac{1}{p}}\big) = \zeta_p^i a^{\frac{k}{p}}\alpha \in L.$$

As $L = M\big(a^{\frac{1}{p}}\big)$, this implies that the extension L/F is normal, hence Galois. The result is obvious if $L = M$ (then $\mathsf{Gal}(L/F) = \mathsf{Gal}(M/F)$ is abelian): assume henceforth that $L \neq M$. The group $\mathsf{Gal}(L/M)$ is then cyclic of order p, generated by σ such that $\sigma\big(a^{\frac{1}{p}}\big) = \zeta_p a^{\frac{1}{p}}$. Let $\gamma \in \mathsf{Gal}(L/F)$: we have $\gamma\big(a^{\frac{1}{p}}\big) = \zeta_p^i a^{\frac{k}{p}}\alpha$ with $i \in \mathbf{Z}/p\mathbf{Z}$, $k \in \mathbf{Z}$ whose image in $\mathbf{Z}/p\mathbf{Z}$ is $\chi(\gamma)$ and $\alpha \in M$. Then

$$(\gamma\circ\sigma)\big(a^{\frac{1}{p}}\big) = \gamma\big(\zeta_p a^{\frac{1}{p}}\big) = \zeta_p^{\chi(\gamma)+i} a^{\frac{k}{p}}\alpha = \zeta_p^{k+i} a^{\frac{k}{p}}\alpha = \zeta_p^i\big(\zeta_p a^{\frac{1}{p}}\big)^k\alpha = \sigma\big(\zeta_p^i a^{\frac{k}{p}}\alpha\big) = (\sigma\circ\gamma)\big(a^{\frac{1}{p}}\big)$$

As $\gamma\circ\sigma$ and $\sigma\circ\gamma$ also coincide on M (because M/F is abelian) and $L = M\big(a^{\frac{1}{p}}\big)$, this shows that $\gamma\circ\sigma = \sigma\circ\gamma$, so that $\mathsf{Gal}(L/M)$ lies in the center of $\mathsf{Gal}(L/F)$. This implies that the quotient of $\mathsf{Gal}(L/F)$ by its center is a quotient of $\mathsf{Gal}(M/F)$, which cyclic (since it identifies with a subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$). The classical argument in group theory implies that $\mathsf{Gal}(L/F)$ is abelian. □

Lemma 8.3.4. If $p \neq 2$, there is no Galois extension $N/\mathbf{Q}_p$ such that $\mathsf{Gal}(N/\mathbf{Q}_p) \simeq (\mathbf{Z}/p\mathbf{Z})^3$.

Proof. Let $N/\mathbf{Q}_p$ be Galois and such that $\mathsf{Gal}(N/\mathbf{Q}_p) \simeq (\mathbf{Z}/p\mathbf{Z})^3$. The composite of the abelian extensions $N/\mathbf{Q}_p$ and $\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p$ is abelian: so is the extension $N(\zeta_p)/\mathbf{Q}_p(\zeta_p)$. As $[\mathbf{Q}_p(\zeta_p) : \mathbf{Q}_p] = p-1$ is prime to $[N : \mathbf{Q}_p] = p^3$, we have $[N(\zeta_p) : \mathbf{Q}_p] = (p-1)p^3$, so that $[N(\zeta_p) : \mathbf{Q}_p(\zeta_p)] = p^3$: the restriction map $\mathsf{Gal}(N(\zeta_p)/\mathbf{Q}_p(\zeta_p)) \to \mathsf{Gal}(N/\mathbf{Q}_p)$, which is an injective group homomorphism, is thus an isomorphism, *i.e.* $\mathsf{Gal}(N(\zeta_p)/\mathbf{Q}_p(\zeta_p)) \simeq (\mathbf{Z}/p\mathbf{Z})^3$. This implies that the extension $N(\zeta_p)/\mathbf{Q}_p(\zeta_p)$ is a Kummer extension: it corresponds to a subgroup $\Delta \leqslant \mathbf{Q}_p(\zeta_p)^\times/\mathbf{Q}_p(\zeta_p)^{\times p}$ such that $\Delta \simeq (\mathbf{Z}/p\mathbf{Z})^3$.

Let $a \in \Delta$, and $L = \mathbf{Q}_p\left(\zeta_p, a^{\frac{1}{p}}\right) \subset N(\zeta_p)$. As the extension $N(\zeta_p)/\mathbf{Q}_p$ is abelian, so is $L/\mathbf{Q}_p$: by lemma 8.3.3, we have $\sigma(a) \equiv a^{\chi(\sigma)} \mod \mathbf{Q}_p(\zeta_p)^{\times p}$ for all $\sigma \in \mathsf{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$. Using notations of section 8.2.16, we have $v(a) = v(\sigma(a))$ and $v\big(\mathbf{Q}_p(\zeta_p)^{\times p}\big) = p\mathbf{Z}$, so the image of $v(a)$ in $\mathbf{Z}/p\mathbf{Z}$ is equal to $\chi(\sigma)v(a)$ for all $\sigma \in \mathsf{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$. As $\chi(\mathsf{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)) = (\mathbf{Z}/p\mathbf{Z})^\times \neq \{1\}$ (because $p \neq 2$), this shows that $v(a) \in p\mathbf{Z}$, so that

$$a \in (\zeta_p - 1)^{p\mathbf{Z}} \times \mu_{p-1} \times U \subset (\zeta_p - 1)^{\mathbf{Z}} \times \mu_{p-1} \times U \simeq \mathbf{Q}_p(\zeta_p)^\times.$$

As a is defined modulo $\mathbf{Q}_p(\zeta_p)^{\times p}$, we may multiply a by a p-th power and assume that $v(a) = 0$. Similarly, as elements of μ_{p-1} are p-th powers of themselves, we may assume that $a \in U$. This implies that we may assume that

$$\Delta \leqslant U/U^p.$$

Let $a \in \Delta\backslash\{1\}$. As the residue field of $\mathbf{Q}_p(\zeta_p)$ is $\mathbf{F}_p$, we have $\mathcal{O}_{\mathbf{Q}_p(\zeta_p)} = \mathbf{Z} + \pi\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$: there exists $n \in \mathbf{Z}_{\geqslant 0}$ such that $a \equiv 1 - n\pi \mod \pi^2\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$. As $\zeta_p^n = (1+\pi)^n \equiv 1 + n\pi \mod \pi^2\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$, we have

$$u := \zeta_p^n a \equiv 1 \mod \pi^2\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$$

(*cf* proof of lemma 8.2.19). Let $\sigma \in \mathsf{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$ and $k_\sigma \in \mathbf{Z}$ lifting $\chi(\sigma) \in (\mathbf{Z}/p\mathbf{Z})^\times$: as above, we have $\sigma(a) \equiv a^{k_\sigma} \mod \mathbf{Q}_p(\zeta_p)^{\times p}$ (because $\mathbf{Q}_p\left(\zeta_p, a^{\frac{1}{p}}\right)/\mathbf{Q}_p$ is abelian, *cf* lemma 8.3.3). As $\sigma(a), a^{k_\sigma} \in U$, we have thus $\frac{\sigma(a)}{a^{k_\sigma}} \in U \cap \mathbf{Q}_p^{\times p} = U^p$, whence $\sigma(a) \equiv a^{k_\sigma} \mod U^p$ for all $\sigma \in \mathsf{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$. As the same congruence holds for ζ_p^n, we also have

$$(*) \qquad \sigma(u) \equiv u^{k_\sigma} \mod U^p$$

for all $\sigma \in \mathsf{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$. On the other hand, we can write $u \equiv 1 + c\pi^q \mod \pi^d\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$ with $c \in \mathbf{Z}\backslash p\mathbf{Z}$ and $d = v(u-1) \in \mathbf{Z}_{\geqslant 2}$ (recall that $u \neq 1$). We have

$$\begin{cases} \sigma(u) \equiv 1 + ck_\sigma^d\pi^d \mod \pi^{d+1}\mathcal{O}_{\mathbf{Q}_p(\zeta_p)} \\ u^{k_\sigma} \equiv 1 + ck_\sigma\pi^d \mod \pi^{d+1}\mathcal{O}_{\mathbf{Q}_p(\zeta_p)} \end{cases}$$

so $\frac{\sigma(u)}{u^{k_\sigma}} \equiv 1 + c(k_\sigma^d - k_\sigma)\pi^d \mod \pi^{d+1}\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$. By equation $(*)$, we also have $\frac{\sigma(u)}{u^{k_\sigma}} \in U^p$. By lemma 8.2.19, we have $U^p = \big\{x \in \mathcal{O}_{\mathbf{Q}_p(\zeta_p)}\,;\, x \equiv 1 \mod \pi^{p+1}\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}\big\}$: this implies that $d \geqslant p+1$ or $d \leqslant p$ and $c(k_\sigma^d - k_\sigma) \in \pi\mathcal{O}_{\mathbf{Q}_p(\zeta_p)}$.

In the first case, we have $u \in U^p$, whence $a \in \zeta_p^{\mathbf{Z}}$. In the second case, we have $c(k_\sigma^d - k_\sigma) \in p\,\mathbf{Z}$, so that $k_\sigma^d - k_\sigma \in p\,\mathbf{Z}$ (since $c \notin p\,\mathbf{Z}$), thus $\chi(\sigma)^d = \chi(\sigma)$ *i.e.* $\chi(\sigma)^{d-1} = 1$ in $(\mathbf{Z}/p\,\mathbf{Z})^\times$. As $\chi(\sigma)$ can take any value in $(\mathbf{Z}/p\,\mathbf{Z})^\times$ and the latter is cyclic of order $p-1$, this implies that $p-1 \mid d-1$. As $d \leqslant p$, this implies that $d = p$, so that u belongs to $\{x \in U\,;\, x \equiv 1 \mod \pi^p \mathcal{O}_{\mathbf{Q}_p(\zeta_p)}\}$. As the latter is the subgroup of U generated by $1 + \pi^p$, we see that in any case, we have

$$\Delta \subset \langle \zeta_p, 1 + \pi^p \rangle \subset U/U^p$$

As $\langle \zeta_p, 1 + \pi^p \rangle$ has dimension 2 seen as a sub-$\mathbf{F}_p$-vector space of U/U^p, we cannot have $\Delta \simeq (\mathbf{Z}/p\,\mathbf{Z})^3$, giving the contradiction.

Case where $p = q = 2$. The extension $K_u := \mathbf{Q}_2(\zeta_{2^{2^m}-1})/\,\mathbf{Q}_2$ is unramified and cyclic of degree 2^m (*cf* remark 8.2.15). On the other hand, the extension $K_r = \mathbf{Q}_2(\zeta_{2^{m+2}})/\,\mathbf{Q}_2$ is totally ramified, with Galois group isomorphic to $(\mathbf{Z}/2^{m+2}\,\mathbf{Z})^\times \simeq (\mathbf{Z}/2\,\mathbf{Z}) \times (\mathbf{Z}/2^m\,\mathbf{Z})$. This implies that $[K_uK_r : \mathbf{Q}_2] = 2^{2m+1}$ (since the ramification index of $K_uK_r/\,\mathbf{Q}_2$ is at least $[K_r : \mathbf{Q}_2] = 2^{m+1}$ and the residual degree at least $[K_u : \mathbf{Q}_2] = 2^m$). By proposition 8.2.2, the extension $K_uK_r/\,\mathbf{Q}_2$ is abelian. As the group homomorphism

$$\mathsf{Gal}(K_uK_r/\,\mathbf{Q}_2) \to \mathsf{Gal}(K_u/\,\mathbf{Q}_2) \times \mathsf{Gal}(K_r/\,\mathbf{Q}_2)$$

(given by the restrictions) is injective, it is an isomorphism by cardinality, so that

$$\mathsf{Gal}(K_uK_r/\,\mathbf{Q}_2) \simeq (\mathbf{Z}/2\,\mathbf{Z}) \times (\mathbf{Z}/2^m\,\mathbf{Z})^2.$$

Assume $K \not\subset K_uK_r$. The extension $KK_uK_r/\,\mathbf{Q}_2$ is abelian (*cf* proposition 8.2.2). The group homomorphism

$$\mathsf{Gal}(KK_uK_r/K_uK_r) \to \mathsf{Gal}(K/\,\mathbf{Q}_2) \simeq \mathbf{Z}/2^m\,\mathbf{Z}$$

induced by the restriction is injective, so $\mathsf{Gal}(KK_uK_r/K_uK_r) \simeq \mathbf{Z}/2^{m'}\,\mathbf{Z}$ for some $m' \in \{1, \ldots, m\}$. As $\mathsf{Gal}(KK_uK_r/\,\mathbf{Q}_2)$ is abelian, this implies that it has at most four generators, one of which has order 2, and contains $(\mathbf{Z}/2\,\mathbf{Z}) \times (\mathbf{Z}/2^m\,\mathbf{Z})^2$ as a *strict* subgroup. There are two possibilities:

$$\mathsf{Gal}(KK_uK_r/\,\mathbf{Q}_2) \simeq \begin{cases} (\mathbf{Z}/2\,\mathbf{Z}) \times (\mathbf{Z}/2^m\,\mathbf{Z})^2 \times (\mathbf{Z}/2^{m'}\,\mathbf{Z}) & \text{with } m' \geqslant 1 \\ \text{or} & \\ (\mathbf{Z}/2^m\,\mathbf{Z})^2 \times (\mathbf{Z}/2^{m'}\,\mathbf{Z}) & \text{with } m \geqslant m' \geqslant 2 \end{cases}.$$

It thus has a quotient has a quotient isomorphic to either $(\mathbf{Z}/2\,\mathbf{Z})^4$ or $(\mathbf{Z}/4\,\mathbf{Z})^3$: there exists a Galois subextension N of $KK_uK_r/\,\mathbf{Q}_2$ such that

$$\mathsf{Gal}(N/\,\mathbf{Q}_2) \simeq \begin{cases} (\mathbf{Z}/2\,\mathbf{Z})^4 \\ \text{or} \\ (\mathbf{Z}/4\,\mathbf{Z})^3 \end{cases}.$$

It remains to check that those two cases are impossible.

- The first case corresponds, by Kummer theory, to four linearly independent elements in $\mathbf{Q}_2^\times/\,\mathbf{Q}_2^{\times 2}$ (*i.e.* to four independent quadratic extensions of $\mathbf{Q}_2$). As

$$\mathbf{Q}_2^\times \simeq 2^{\mathbf{Z}} \times \{\pm 1\} \times U_1$$

where $U_1 = \{u \in \mathbf{Z}_2\,;\, u \equiv 1 \mod 4\,\mathbf{Z}_2\}$, and $U_1^2 = \{x \in \mathbf{Z}_2\,;\, x \equiv 1 \mod 8\,\mathbf{Z}_2\}$, the $\mathbf{F}_2$-vector space

$$\mathbf{Q}_2^\times/\,\mathbf{Q}_2^{\times 2} \simeq (\mathbf{Z}/2\,\mathbf{Z}) \times \{\pm 1\} \times U_1/U_1^2$$

has dimension 3,contradicting $\mathsf{Gal}(N/\,\mathbf{Q}_2) \simeq (\mathbf{Z}/2\,\mathbf{Z})^4$.

- Assume from now on that $\mathsf{Gal}(N/\,\mathbf{Q}_2) \simeq (\mathbf{Z}/4\,\mathbf{Z})^3$. Assume $i := \sqrt{-1} \notin N$: then $N(i)/\,\mathbf{Q}_2$ is abelian, and the natural map $\mathsf{Gal}(N(i)/\,\mathbf{Q}_2) \to \mathsf{Gal}(N/\,\mathbf{Q}_2) \times \mathsf{Gal}(\mathbf{Q}_2(i)/\,\mathbf{Q}_2) \simeq (\mathbf{Z}/4\,\mathbf{Z})^3 \times (\mathbf{Z}/2\,\mathbf{Z})$ is a group isomorphism, implying the existence of a subfield N' of $N(i)$ such that $\mathsf{Gal}(N'/\,\mathbf{Q}_2) \simeq (\mathbf{Z}/2\,\mathbf{Z})^4$, which is not possible by what precedes. This shows that $i \in N$. Let $f\colon \mathbf{Z}^3 \to \mathsf{Gal}(N/\,\mathbf{Q}_2)$ be a surjective group homomorphism inducing an isomorphism $\widetilde{f}\colon (\mathbf{Z}/4\,\mathbf{Z})^3 \xrightarrow{\sim} \mathsf{Gal}(N/\,\mathbf{Q}_2)$. The composite with the surjective group homomorphism $g\colon \mathsf{Gal}(N/\,\mathbf{Q}_2) \to \mathsf{Gal}(\mathbf{Q}_2(i)/\,\mathbf{Q}_2) \simeq \mathbf{Z}/2\,\mathbf{Z}$ provides a surjective group homomorphism $g \circ f\colon \mathbf{Z}^3 \to \mathbf{Z}/2\,\mathbf{Z}$. By the adapted basis theorem (*cf* theorem 1.4.11), there exists a $\mathbf{Z}$-basis (e_1, e_2, e_3) of $\mathbf{Z}^3$ such that $\mathsf{Ker}(g \circ f) = \mathbf{Z}\,e_1 \oplus \mathbf{Z}\,e_2 \oplus 2\,\mathbf{Z}\,e_3$. This implies that replacing f by its composite with the change of basis map, we may assume that (e_1, e_2, e_3) is the canonical basis, so that $\mathsf{Ker}(g \circ \widetilde{f}) = (\mathbf{Z}/4\,\mathbf{Z})^2 \oplus (2\,\mathbf{Z}/4\,\mathbf{Z})$. Let L denote the subfield of N corresponding to the subgroup $(\mathbf{Z}/4\,\mathbf{Z}) \times \{0\} \subset (\mathbf{Z}/4\,\mathbf{Z})^2 \oplus (2\,\mathbf{Z}/4\,\mathbf{Z})$. By construction, we have $\mathbf{Q}_2(i) \subset L$ and $\mathsf{Gal}(L/\,\mathbf{Q}_2) \simeq \mathbf{Z}/4\,\mathbf{Z}$. Let σ be a generator of $\mathsf{Gal}(L/\,\mathbf{Q}_2)$, so that σ^2 generates $\mathsf{Gal}(\mathbf{Q}_2(i)/\,\mathbf{Q}_2)$ and $\sigma(i) = -i$. We can write $L = \mathbf{Q}_2(i, \alpha)$ with $\alpha^2 \in \mathbf{Q}_2(i)$. As $L/\,\mathbf{Q}_2$ is Galois, we also have $L = \mathbf{Q}_2(i, \sigma(\alpha))$ and $\sigma(\alpha)^2 = \sigma(\alpha^2) \in \mathbf{Q}_2(i)$. This implies that $\sigma^2(\alpha)^2 = \sigma^2(\alpha^2) = \alpha^2$, so that $\sigma^2(\alpha) = \pm\alpha$. We cannot have $\sigma^2(\alpha) = \alpha$, otherwise $\alpha \in \mathbf{Q}_2(i)$ which is not: we have $\sigma^2(\alpha) = -\alpha$, whence

$\sigma^3(\alpha) = -\sigma(\alpha)$. This implies that $\sigma^2\big(\frac{\sigma(\alpha)}{\alpha}\big) = \frac{\sigma(\alpha)}{\alpha}$, *i.e.* $\frac{\sigma(\alpha)}{\alpha} \in \mathbf{Q}_2(i)$: write $\sigma(\alpha) = (a+ib)\alpha$ with $a, b \in \mathbf{Q}_2$. Applying σ gives $-\alpha = \sigma^2(\alpha) = (a - ib)\sigma(\alpha)$: multiplying these equalities and dividing by $\alpha\sigma(\alpha)$ gives

$$a^2 + b^2 = -1.$$

Such an equality is impossible in $\mathbf{Q}_2$ (multiplying by the square of a common denominator gives a non trivial equality $x^2 + y^2 + z^2 = 0$ is $\mathbf{Z}_2$, which is already impossible modulo 8), giving a contradiction.
What precedes shows that the assumption $K \not\subset K_uK_r$ is absurd: we have $K \subset K_uK_r = \mathbf{Q}_2(\zeta_{2^{m+2}(2^{2^m}-1)})$, finishing the proof. □

9. Appendix

9.1. Zorn's lemma.

The axiom of choice (that we assume) is equivalent to the following:

Theorem 9.1.1. A partially ordered set in which every chain[50] has an upper bound contains at least one maximal element.

Remark 9.1.2. Considering opposite orders, we also have the dual statement: a partially ordered set in which every chain has an lower bound contains at least one minimal element.

9.2. Galois theory.

Let Ω/K a field extension, and L_1, L_2 sub-extensions. We have the following situation:

$$\begin{tikzcd}
 & \Omega \arrow[d, dash] & \\
 & L_1L_2 \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] \\
 & L_1 \cap L_2 \arrow[d, dash] & \\
 & K &
\end{tikzcd}$$

Proposition 9.2.1. Assume L_1/K is finite and Galois. The extensions L_1L_2/L_2 and $L_1/L_1 \cap L_2$ are finite and Galois, and the restriction map

$$\rho\colon\ \mathsf{Gal}(L_1L_2/L_2) \to \mathsf{Gal}(L_1/L_1 \cap L_2)$$

is a group isomorphism. In particular, we have $[L_1L_2 : L_2] = [L_1 : L_1 \cap L_2]$. If moreover L_2/K is finite, we have $[L_1L_2 : K] = \frac{[L_1:K][L_2:K]}{[L_1 \cap L_2:K]}$.

Proof. As L_1/K is finite and Galois, it is the splitting field, in Ω of a separable polynomial $P \in K[X]$: the field L_1L_2 is the splitting field, in Ω, of P seen as an element of $L_2[X]$. As P is separable, the extension L_1L_2/L_2 is Galois. Of course, $L_1/L_1 \cap L_2$ is Galois because L_1/K is. We thus have the group homomorphisme ρ.

If $\sigma \in \mathsf{Ker}(\rho)$, then σ induces the identity on L_1 and L_2, hence on L_1L_2: we have $\sigma = \mathsf{Id}_{L_1L_2}$, which shows the injectivity of ρ. Put $H = \mathsf{Im}(\rho)$. If $x \in L_1$ is fixed H, it is fixed by $\mathsf{Gal}(L_1L_2/L_2)$: it belongs to L_2, hence to $L_1 \cap L_2$. This shows that $L_1^H = L_1 \cap L_2$: Galois correspondance implies that $H = \mathsf{Gal}(L_1/L_1 \cap L_2)$, and ρ is surjective.

We have thus $\#\,\mathsf{Gal}(L_1L_2/L_2) = \#\,\mathsf{Gal}(L_1/L_1 \cap L_2)$, hence $[L_1L_2 : L_2] = [L_1 : L_1 \cap L_2]$.

If L_2/K is finite, we have

$$[L_1L_2 : K] = [L_1L_2 : L_2][L_2 : K] = [L_1 : L_1 \cap L_2][L_2 : K] = \tfrac{[L_1:K][L_2:K]}{[L_1 \cap L_2:K]} < +\infty.$$

□

Proposition 9.2.2. Assume L_1/K and L_2/K are finite and Galois. Then L_1L_2/K and $L_1 \cap L_2/K$ are finite and Galois, and the natural map (given by restrictions)

$$\psi\colon\ \mathsf{Gal}(L_1L_2/K) \to \mathsf{Gal}(L_1/K) \times \mathsf{Gal}(L_2/K)$$

is injective, with image $\{(\sigma_1, \sigma_2) \in \mathsf{Gal}(L_1/K) \times \mathsf{Gal}(L_2/K)\,;\, \sigma_{1|L_1 \cap L_2} = \sigma_{2|L_1 \cap L_2}\}$.

Proof. If $x \in L_1 \cap L_2$, the conjuguates of x over K all belong to L_1 (because L_1/K is normal). Similarly, they all belong to L_2: they lie in $L_1 \cap L_2$, and the extension $L_1 \cap L_2/K$ is normal. Being a sub-extension of the separable extension L_1/K, it is separable, which shows that $L_1 \cap L_2/K$ is Galois.

The fields L_1 and L_2 are splitting fields, in Ω, od separable polynomials P_1 and P_2: the field L_1L_2 is thus the splitting fields, in Ω, of the separable polynomial $\mathsf{lcm}(P_1, P_2)$, which shows that L_1L_2/K is Galois.

If $\sigma \in \mathsf{Ker}(\psi)$, then σ induces the identity on L_1 and L_2, hence on L_1L_2, so that $\sigma = \mathsf{Id}_{L_1L_2}$, which shows the injectivity of ψ. Of course we have

$$\mathsf{Im}(\psi) \leqslant H := \{(\sigma_1, \sigma_2) \in \mathsf{Gal}(L_1/K) \times \mathsf{Gal}(L_2/K)\,;\, \sigma_{1|L_1 \cap L_2} = \sigma_{2|L_1 \cap L_2}\}.$$

We know that

$$\mathsf{Gal}(L_2/K)/\,\mathsf{Gal}(L_2/L_1 \cap L_2) \xrightarrow{\sim} \mathsf{Gal}(L_1 \cap L_2/K).$$

[50] *I.e.* a totally ordered subset.

If $\sigma_1 \in \mathsf{Gal}(L_1/K)$, the restriction $\sigma_{1|L_1 \cap L_2} \in \mathsf{Gal}(L_1 \cap L_2/K)$ thus admits $[L_2 : L_1 \cap L_2]$ extensions to L_2. this implies that

$$\#H \leqslant \#\,\mathsf{Gal}(L_1/K)[L_2 : L_1 \cap L_2] = [L_1 : K][L_2 : L_1 \cap L_2] = \frac{[L_1 : K][L_2 : K]}{[L_1 \cap L_2 : K]}.$$

By proposition 9.2.1, we deduce $\#H \leqslant [L_1L_2 : K] = \#\,\mathsf{Gal}(L_1L_2/K)$. As ψ is injective, this is an equality, which shows that $\mathsf{Im}(\psi) = H$. □

Corollary 9.2.3. If L_1/K and L_2/K are finite and abelian, so is L_1L_2/K.

Proof. The group $\mathsf{Gal}(L_1/K) \times \mathsf{Gal}(L_2/K)$ is abelian: so is its sub-group

$$H := \{(\sigma_1, \sigma_2) \in \mathsf{Gal}(L_1/K) \times \mathsf{Gal}(L_2/K)\,;\, \sigma_{1|L_1 \cap L_2} = \sigma_{2|L_1 \cap L_2}\}.$$

As ψ induces an isomorphism $\mathsf{Gal}(L_1L_2/K) \xrightarrow{\sim} H$, the extension L_1L_2/K is abelian. □

References

[1] Y. Amice – *Ls nombres p-adiques*, Le mathématicien, vol. 14, Presses universitaires de France, 1975.

[2] J. Ax – "Zeros of polynomials over local fields - The Galois action", *Journal of Algebra* **15** (1970), p. 417–428.

[3] A. I. Borevich & I. R. Shafarevich – *Number theory*, Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20, Academic Press, New York-London, 1966.

[4] S. Bosch, U. Güntzer & R. Remmert – *Non-Archimedean analysis*, Grundlehren der Mathematischen Wissenschaften, vol. 261, Springer-Verlag, Berlin, 1984, A systematic approach to rigid analytic geometry.

[5] N. Bourbaki – *Éléments de mathématique. Algèbre commutative, chapitres 8 et 9*, Masson, 1983.

[6] T. Browning – "Local fields", `https://warwick.ac.uk/fac/sci/maths/people/staff/fbouyer/local_fieldstcc.pdf`, notes by Florian Bouyer.

[7] I. S. Cohen – "On non-Archimedean normed spaces", *Nederl. Akad. Wetensch., Proc.* **51** (1948), p. 693–698 = Indagationes Math. 10, 244–249.

[8] B. Dwork, G. Gerotto & F. Sullivan – *An introduction to G-functions*, Annals of Mathematics Studies, vol. 133, Princeton University Press, Princeton, NJ, 1994.

[9] Gelfand, I.M. and Kapranov, M. and Zelevinsky, A. – *Discriminants, Resultants, and Multidimensional Determinants*, Modern Birkhäuser Classics, Birkhäuser, 2008.

[10] A. Grothendieck – *Groupes de Barsotti-Tate et cristaux de Dieudonné*, Séminaire de Mathématiques Supérieures, vol. 45, Les Presses de l'Université de Montréal, 1974.

[11] D. R. Heath-Brown – "Cubic forms in ten variables", *Proceedings of the London Mathematical Society* **s3-47** (1983), no. 2, p. 225–257.

[12] M. Kashiwara & P. Schapira – *Sheaves on manifolds*, Grundlehren der Mathematischen Wissenschaften, vol. 292, Springer-Verlag, 1990.

[13] N. Koblitz – *p-adic numbers, p-adic analysis, and zeta-functions*, Graduate texts in mathematics, vol. 58, Springer-Verlag, 1977.

[14] D. J. Lewis – "Cubic homogeneous polynomials over p-adic number fields", *Annals of Mathematics* **56** (1952), no. 3, p. 473–478.

[15] Q. Liu – *Algebraic geometry and arithmetic curves*, Oxford graduate texts in mathematics, Oxford University Press, 2002.

[16] M. Matignon & M. Reversat – "Sous-corps fermés d'un corps valué", *Journal of Algebra* **90** (1984), no. 2, p. 491–515.

[17] H. Matsumura – *Commutative ring theory*, Cambridge university Press, 1986.

[18] W. H. Schikhof – *Ultrametric Calculus: An Introduction to p-Adic Analysis*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1985.

[19] J.-P. Serre – "Rationalité des fonctions ζ des variétés algébriques", in *Séminaire Bourbaki : années 1958/59 - 1959/60, exposés 169-204*, Séminaire Bourbaki, no. 5, Société mathématique de France, 1960, talk:198, p. 415–425.

[20] ———, *Corps locaux*, Publications de l'Institut de Mathématique de l'Université de Nancago, vol. VIII, Hermann, 1962.

[21] ———, *Algèbre locale, multiplicités*, Lecture notes in mathematics, vol. 11, Springer Verlag, 1965.

[22] ———, *Cours d'arithmétique*, Le Mathématicien, vol. 2, Presses Universitaires de France, 1977, Deuxième édition revue et corrigée.

[23] J.-P. Serre & J. Tate – "Good reduction of abelian varieties", *Annals of Mathematics. Second Series* **88** (1968), p. 492–517.

[24] T. Stacks project authors – "The stacks project", `https://stacks.math.columbia.edu`, 2018.

[25] L. Washington – *Introduction to cyclotomic fields*, second éd., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

Institut de Mathématiques de Bordeaux, Université Bordeaux, 351, cours de la Libération, 33405 Talence, France

Email address: `olivier.brinon@math.u-bordeaux.fr`