COURS DE MASTER 1 : THÉORIE DES NOMBRES

OLIVIER BRINON

Table des matières

1. Rappels et compléments d'algèbre commutative

Conventions. Dans tout le cours, les anneaux sont supposés (commutatifs et) unitaires. Par définition, un morphisme d'anneaux $f\colon A \to B$ vérifie $f(1_A) = 1_B$. On utilisera fréquemment le résultat suivant :

Théorème 1.0.1. (Krull). Soient A un anneau et $I \subset A$ un idéal strict [a]. Il existe $\mathfrak{m} \subset A$ maximal tel que $I \subset \mathfrak{m}$.

a. *I.e.* tel que $I \neq A$.

1.1. Propriétés de finitude.

Soient A un anneau et M un A-module.

Définition 1.1.1. (1) On dit que M est de **type fini** s'il est engendré par une famille finie : il existe $\{m_i\}_{1\leqslant i\leqslant r} \subset M$ tel que $M = \sum_{i=1}^{r} Am_i$.
(2) On dit que M est **nœthérien** si tous ses sous-modules sont de type fini.
(3) On dit que A est **nœthérien** s'il l'est en tant que A-module.
(4) Un anneau principal est un anneau *intègre* dont tout idéal est monogène.

Remarque 1.1.2. (1) Un A-module nœthérien est de type fini, mais la réciproque est fausse (trouver un contre-exemple).
(2) Les sous-A-modules de A ne sont autres que ses idéaux : A est nœthérien si ses idéaux sont de type fini.

Exemples 1.1.3. (1) Tout anneau principal est nœthérien : c'est le cas des corps, de $\mathbf{Z}$.
(2) si K est un corps, un K-espace vectoriel est nœthérien si et seulement s'il est de dimension finie.
(3) $\mathbf{Q}$ est un anneau nœthérien, mais il n'est pas nœthérien comme $\mathbf{Z}$-module.
(4) Si K est un corps et I un ensemble infini, l'anneau de polynômes $K\big[X_i\big]_{i\in I}$ n'est pas nœthérien (exercice).
(5) Les anneaux $\mathscr{C}^\infty(\mathbf{R},\mathbf{R}) \subset \mathscr{C}^0(\mathbf{R},\mathbf{R}) \subset \mathscr{F}(\mathbf{R},\mathbf{R})$ ne sont pas nœthériens.

Proposition 1.1.4. Propriétés équivalentes :
(i) M est nœthérien ;
(ii) toute suite croissante de sous-modules de M est stationnaire ;
(iii) tout sous-ensemble non vide de sous-modules de M admet un élément maximal (pour l'inclusion).

Démonstration. (i) $\Rightarrow$ (ii). La réunion est un sous-module de type fini, donc égale à l'un des sous-modules.
(ii) $\Rightarrow$ (iii). Soit $\mathscr{E}$ un tel ensemble. S'il n'a pas d'élément maximal, on peut construire une suite strictement croissante (pour l'inclusion) d'éléments de $\mathscr{E}$, ce qui contredit (ii).
(iii) $\Rightarrow$ (ii). Soient $N \subset M$ un sous-module et $\mathscr{E}$ l'ensemble des sous-modules de type fini de N. Comme $\{0\} \in \mathscr{E}$, on a $\mathscr{E} \neq \varnothing$: d'après (iii), $\mathscr{E}$ admet un élément maximal N_0. Si $N_0 \neq N$, soient $x \in N\backslash N_0$ et $N' = N_0 + Ax \subset N \in \mathscr{E}$. Comme $N_0 \subsetneq N'$, cela contredit la maximalité de N_0 : on a $N_0 = N$ et N est de type fini. □

Proposition 1.1.5. Soit $N \subseteq M$ un sous-module. Alors M est nœthérien si et seulement si N et M/N le sont : la « catégorie » des A-modules nœthériens est stable par sous-module, quotient et extension (en particulier par somme directe finie).

Démonstration. Si M est nœthérien, alors N est de type fini. Par ailleurs, si N' est un sous-A-module de M/N, on a $N' = \widetilde{N}/N$ avec $\widetilde{N} = \pi^{-1}(N')$ (où $\pi\colon M \to M/N$ est la projection canonique). Comme M est nœthérien, $\widetilde{N}$ est de type fini, c'est *a fortiori* de cas de $N' = \widetilde{N}/N$, et M/N est nœthérien.

Supposons N et M/N nœthériens. Soit $(M_n)_{n\in\mathbf{N}}$ une suite croissante de sous-A-modules de M. On dispose des suites croissantes $(M_n \cap N)_{n\in\mathbf{N}}$ et $((N+M_n)/N)_{n\in\mathbf{N}}$ de sous-A-modules de N et de M/N respectivement. Comme ces derniers sont nœthériens, ces suites sont stationnaires : il existe $n_0 \in \mathbf{N}$ tel que pour $n \geqslant n_0$, on a $M_n \cap N = M_{n_0} \cap N$ et $(N+M_n)/N = (N+M_{n_0})/N$ *i.e.* $N + M_n = N + M_{n_0}$. Si $m \in M_n$, il existe donc $x \in N$ et $y \in M_{n_0} \subseteq M_n$ tels que $m = x + y$. Comme $x = y - m \in N \cap M_n = N \cap M_{n_0}$, on a $m \in M_{n_0}$, d'où $M_n \subseteq M_{n_0}$ *i.e.* $M_n = M_{n_0}$. Le A-module M est donc nœthérien. □

Corollaire 1.1.6. Si A est nœthérien, M est nœthérien si et seulement s'il est type fini.

Démonstration. Si M est de type fini, on dispose d'un morphisme surjectif $f\colon A^r \to M$. Comme A est nœthérien, il en est de même de A^r, et de son quotient $M \simeq A^r/\mathsf{Ker}(f)$. □

Théorème 1.1.7. (Hilbert). Si A est nœthérien, alors $A[X]$ est nœthérien.

Démonstration. Soit $I \subseteq A[X]$ un idéal. Pour $n \in \mathbf{N}$, notons J_n l'ensemble des coefficients dominants des éléments de I qui sont de degré n. Comme I est un idéal de $A[X]$, l'ensemble J_n est un idéal de A. En outre, si $n \leqslant m$ et $a \in J_n$ (de sorte qu'il existe $P \in I$ de degré n de coefficient dominant égal à a), alors $a \in J_m$ (car a est le coefficient dominant du polynôme $X^{m-n}P$). La suite d'idéaux $(J_n)_{n\in\mathbf{N}}$ est donc croissante. Comme A est nœthérien, cette suite est stationnaire : soit $d \in \mathbf{N}$ tel que $n \geqslant d \Rightarrow J_n = J_d$. Comme A est nœthérien, l'idéal J_d est de type fini : choisissons $\alpha_1, \ldots, \alpha_r$ des générateurs de J_d, ce sont les coefficients dominants de $P_1, \ldots, P_r \in J_d$ respectivement. Par ailleurs, si $A[X]_{<d}$ désigne le sous-A-module de $A[X]$ constitué du polynôme nul et des polynômes de degré $< d$, posons $M = I \cap A[X]_{<d}$. Comme $A[X]_{<d}$ est un A module de type fini, il est nœthérien (*cf* corollaire 1.1.6), de sorte que M est de type fini : soient $Q_1, \ldots, Q_s$ des générateurs de M. On a bien sûr

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

Montrons l'inclusion réciproque. Si $P \in I$ est de degré $n \geqslant d$, son coefficient dominant a appartient à J_d, de sorte qu'il existe $a_1, \ldots, a_r \in A$ tels que $a = a_a\alpha_1 + \cdots + a_r\alpha_r$. Le polynôme $P - \sum_{i=1}^{r} a_i X^{n-d} P_i \in I$ est de degré $< n$: quitte à soustraire à P un élément de $\alpha_1 A[X] + \cdots + \alpha_r A[X]$, on peut supposer que $\deg(P) < d$. Mais alors $P \in M = I \cap A[X]_{<d}$, et $P \in Q_1 A[X] + \cdots + Q_s A[X]$, ce qui prouve que $P \in \alpha_1 A[X] + \cdots + \alpha_r A[X] + Q_1 A[X] + \cdots + Q_s A[X]$. Ainsi, l'idéal I est de type fini, et $A[X]$ est nœthérien. □

Définition 1.1.8. Une **A-algèbre** est la donnée d'un anneau B muni d'un morphisme d'anneaux $f\colon A \to B$.

Une A-algèbre B est automatiquement munie d'une structure de A-module, la loi externe étant donnée par :

$$\begin{aligned} A \times B &\to B \\ (a, b) &\mapsto f(a)b \end{aligned}$$

Exemples 1.1.9. (1) Tout anneau est de façon unique une $\mathbf{Z}$-algèbre.

(2) L'anneau de polynômes $A[X]$ est une A-algèbre de la façon évidente.

(3) Si L/K est une extension de corps, alors L est une K-algèbre.

Remarque 1.1.10. Si B est une A-algèbre (via $f\colon A \to B$) et M un B-module, alors M hérite d'une structure de A-module par la loi externe

$$\begin{aligned} A \times M &\to M \\ (a, m) &\mapsto f(a)m \end{aligned}$$

Définition 1.1.11. (1) Si $X \subset B$, la **sous-A-algèbre de B engendrée par X** est la plus petite sous-A-algèbre de B contenant X. Si $X = \{b_1, \dots, b_r\}$, c'est l'ensemble, noté $A[b_1, \dots, b_r]$, des éléments de la forme

$$P(b_1, \dots, b_r) = \sum_{\underline{n}=(n_1,\dots,n_r)\in\mathbf{N}^r} f(a_{\underline{n}}) b_1^{n_1} \cdots b_r^{n_r}$$

pour $P = \sum_{\underline{n}=(n_1,\dots,n_r)\in\mathbf{N}^r} a_{\underline{n}} X_1^{n_1} \cdots X_r^{n_r} \in A[X_1, \dots, X_r]$.

(2) On dit que B est une A-algèbre de **type fini** si elle est engendrée, *comme A-algèbre* par une partie finie, *i.e.* s'il existe $b_1, \dots, b_r \in B$ tels que $B = A[b_1, \dots, b_r]$.

(3) On dit que B est une A-algèbre **finie** si elle est engendrée, *comme A-module* par une partie finie, *i.e.* s'il existe $b_1, \dots, b_r \in B$ tels que $B = \sum_{i=1}^{r} Ab_i$.

Remarque 1.1.12. (1) Si B est une A-algèbre finie, alors elle est de type fini (on a $\sum_{i=1}^{r} Ab_i \subseteq A[b_1, \dots, b_r]$), mais la réciproque est fausse : l'anneau de polynômes $A[X]$ est une A-algèbre de type fini (engendrée par $\{X\}$), mais pas finie.

(2) Transitivité. Si B est une A-algèbre finie et M un B-module de type fini, alors M est un A-module de type fini. En effet, si $B = \sum_{i=1}^{r} Ab_i$ et $M = \sum_{j=1}^{s} Bm_j$, on a $M = \sum_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant s}} Ab_i m_j$. En particulier, une B-algèbre finie est aussi finie sur A.

Corollaire 1.1.13. Soient A un anneau nœthérien et B une A-algèbre de type fini. Alors B est un anneau nœthérien.

Démonstration. Comme B est de type fini, il existe $b_1, \dots, b_r \in B$ tels que $B = A[b_1, \dots, b_r]$, si bien qu'on dispose du morphisme de A-algèbres surjectif $f\colon A[X_1, \dots, X_r] \to B$ défini par $f(X_i) = b_i$ pour $i \in \{1, \dots, r\}$. Comme A est nœthérien, il en est de même de $A[X_1, \dots, X_r]$ (en appliquant r fois le théorème 1.1.7), donc de son quotient $B \simeq A[X_1, \dots, X_r]/\mathsf{Ker}(f)$. □

Définition 1.1.14. Soient M un A-module et $m \in M$. On pose $\mathsf{ann}_A(m) = \{a \in A,\ am = 0\}$. C'est un idéal de A, appelé **idéal annulateur** de m. On dit que m est de **torsion** si $\mathsf{ann}_A(m) \neq \{0\}$, *i.e.* s'il existe $a \in A\backslash\{0\}$ tel que $am = 0$. On note M_{tors} l'ensemble des éléments de M qui sont de torsion. On dit que M est **sans torsion** si $M_{\mathsf{tors}} = \{0\}$.
On pose $\mathsf{ann}_A(M) = \{a \in A,\ (\forall m \in M)\ am = 0\} = \bigcap_{m\in M} \mathsf{ann}_A(m)$. C'est un idéal de A, appelé **idéal annulateur** de M. On en déduit une structure de $A/\mathsf{ann}_A(M)$-module sur M. Remarquons que M peut-être de torsion même si $\mathsf{ann}_A(M) = \{0\}$: par exemple, on a $\mathsf{ann}_{\mathbf{Z}}(\mathbf{Q}/\mathbf{Z}) = \{0\}$.

Proposition 1.1.15. Supposons A intègre et soit M un A-module. Alors M_{tors} est un sous-A-module de M et le A-module quotient M/M_{tors} est sans torsion.

Démonstration. Si $m_1, m_2 \in M_{\mathsf{tors}}$ et $\alpha \in A$, il existe $a_1, a_2 \in A\backslash\{0\}$ tels que $a_1 m_1 = 0$ et $a_2 m_2 = 0$. Comme A est intègre, on a $a_1 a_2 \neq 0$ et $a_1 a_2(m_1 + \alpha m_2) = 0$ implique $m_1 + \alpha m_2 \in M_{\mathsf{tors}}$.

Soit $m \in M$ dont l'image $m + M_{\mathsf{tors}}$ est de torsion dans M/M_{tors} : il existe $a \in A\backslash\{0\}$ tel que $am + M_{\mathsf{tors}} = M_{\mathsf{tors}}$ *i.e.* $am \in M_{\mathsf{tors}}$. Il existe donc $b \in A\backslash\{0\}$ tel que $b(am) = 0$. Comme A est intègre, on a $ab \neq 0$, et $m \in M_{\mathsf{tors}}$. □

Remarque 1.1.16. (1) Ce qui précède tombe en défaut si A n'est pas supposé intègre. Par exemple, si $A = M = \mathbf{Z} \times \mathbf{Z}$, alors $M_{\mathsf{tors}} = \mathbf{Z} \times \{0\} \cup \{0\} \times \mathbf{Z}$ n'est pas un sous-module de M.
(2) Un A-module libre est sans torsion, mais la réciproque est fausse en général (elle est valide dans le cas des modules de type fini sur un anneau principal, *cf* corollaire 1.5.12).

1.2. **Anneaux principaux, factoriels.** Soit A un anneau *intègre*.

Définition 1.2.1. Soit $a \in A\backslash\{0\}$.
(1) On dit que $a \in A$ est **irréductible** si $a \notin A^\times$ et
$$(\forall (b,c) \in A^2)\ a = bc \Rightarrow b \in A^\times \text{ ou } c \in A^\times$$
(2) On dit que $a \in A$ est **premier** si l'idéal principal aA est premier.
(3) On dit que $a, a' \in A\backslash\{0\}$ sont **associés** si $aA = a'A$. Cela définit une relation d'équivalence sur $A\backslash\{0\}$.

Remarque 1.2.2. (1) Un élément irréductible est donc par définition un élément minimal de $A\backslash(\{0\} \cup A^\times)$ pour la relation de divisibilité.
(2) Un élément premier est toujours irréductible. En effet, si $a \in A$ est premier et $a = bc$ avec $b, c \in A$, on a $bc \in aA$ qui est premier : on a $b \in aA$ ou $c \in aA$, disons $b \in aA$. On a donc $b = ad$ avec $d \in A$, et alors $a = adc$. Comme A est intègre, on a $cd = 1$ et $c \in A^\times$.
(3) Deux éléments $a, a' \in A\backslash\{0\}$ sont associés si et seulement si $(\exists u \in A^\times)\, a' = au$.

Définition 1.2.3. On dit que A est **factoriel** si tout élément $a \in A\backslash\{0\}$ peut s'écrire
$$a = up_1p_2\cdots p_r$$
avec $u \in A^\times$ et $p_1, \ldots, p_r$ irréductibles et si cette écriture est unique dans le sens suivant : si $a = vq_1q_2\ldots q_s$ avec $v \in A^\times$ et $q_1, \ldots, q_s$ irréductibles, alors $r = s$ et quitte à renuméroter les q_i, on a $p_iA = q_iA$ pour tout $i \in \{1, \ldots, r\}$.
Une telle écriture s'appelle une **décomposition en facteurs irréductibles** de a.

Exemples 1.2.4. (1) Un corps est factoriel (tout élément non nul est inversible).
(2) Tout anneau principal est factoriel (*cf* proposition 1.2.12).
(3) On peut montrer (exercice) que le sous-anneau $\mathbf{Z}[i\sqrt{5}] = \{x + iy\sqrt{5} \in \mathbf{C},\ x, y \in \mathbf{Z}\}$ de $\mathbf{C}$ n'est pas factoriel, parce que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles, les unités sont 1 et -1, mais que $2.3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ (*i.e.* on n'a pas unicité de la décomposition de 6).

Dans la pratique, si A est factoriel, on se fixe une famille de représentants $\mathscr{P} = \{p_\lambda\}_{\lambda\in\Lambda}$ des classes des éléments irréductibles. Tout élément $a \in A\backslash\{0\}$ s'écrit alors de façon unique
$$a = u\prod_{\lambda\in\Lambda} p_\lambda^{n_\lambda}$$
avec $u \in A^\times$ et $(n_\lambda)_{\lambda\in\Lambda}$ une famille d'entiers presque tous nuls (*i.e.* tous nuls sauf un nombre *fini*).

Définition 1.2.5. Soit p un élément irréductible de A. Il existe un unique $\lambda \in \Lambda$ tel que $pA = p_\lambda A$. La multiplicité n_λ s'appelle la **valuation** [a] de a en p. On la note $v_p(a)$. On pose $v_p(0) = +\infty$.

a. Elle ne dépend que de p et pas du choix de $\mathscr{P}$.

Proposition 1.2.6. (Propriétés des valuations). Supposons A factoriel et soient $a, b \in A$. On a
(1) $v_p(ab) = v_p(a) + v_p(b)$;
(2) $a \mid b$ si et seulement si pour tout $p \in A$ irréductible, on a $v_p(a) \leqslant v_p(b)$;
(3) $a \in A^\times$ si et seulement si pour tout $p \in A$ irréductible, on a $v_p(a) = 0$.
(4) $v_p(a + b) \geqslant \inf\{v_p(a), v_p(b)\}$ avec égalité si $v_p(a) \neq v_p(b)$.

Démonstration. (1)-(3) résultent immédiatement des définitions et de l'unicité de la décomposition en facteurs irréductibles. Pour (4), on si $v = \inf\{v_p(a), v_p(b)\}$, on a $p^v \mid a$ et $p^v \mid b$ donc $p^v \mid a + b$, et donc $v_p(a + b) \geqslant v$. Supposons $v_p(a) \neq v_p(b)$: quitte à échanger a et b, on a $v = v_p(a) < v_p(b)$. On peut écrire $a = p^v a'$ avec $p \nmid a'$ et $b = p^v b'$ avec $p \mid b'$, de sorte que $a + b = p^v(a' + b')$ et $p \nmid a' + b'$: on a $v_p(a + b) = v$. □

Proposition 1.2.7. Soient A un anneau factoriel et $p \in A\backslash\{0\}$. Alors p est irréductible si et seulement si p est premier.

Démonstration. Si p est irréductible et $p \mid ab$, on a $v_p(a) + v_p(b) = v_p(ab) \geqslant 1$ et donc $v_p(a) \geqslant 1$ ou $v_p(b) \geqslant 1$ *i.e.* $p \mid a$ ou $p \mid b$. Réciproquement un élément premier est toujours irréductible. □

Remarque 1.2.8. En fait, on peut montrer qu'un anneau intègre est factoriel si et seulement s'il est nœthérien et tout élément irréductible est premier.

Définition 1.2.9. Soient A un anneau factoriel [a] et $a, b \in A\backslash\{0\}$. On appelle **pgcd** (plus grand commun diviseur) –resp. **ppcm** (plus petit commun multiple)– de a et b un plus grand minorant –resp. un plus petit majorant– de $\{a, b\}$ pour la relation de divisiblité. On les note $\mathsf{pgcd}(a, b)$ et $\mathsf{ppcm}(a, b)$ respectivement. On dit que a et b sont **premiers entre eux** si $\mathsf{pgcd}(a, b) = 1$.

a. Cette définition garde un sens dans un anneau intègre quelconque, mais en général, le pgcd et le ppcm de deux éléments n'existent pas.

Remarque 1.2.10. Rigoureusement, $\mathsf{pgcd}(a, b)$ et $\mathsf{ppcm}(a, b)$ sont définis à multiplication par une unité près : ce sont les idéaux qu'ils engendrent qui sont bien définis.

Cette définition affirme implicitement l'existence du pgcd et du ppcm. En fait, étant donnés $a, b \in A$, de décompositions en facteurs irréductibles

$$a = u \prod_{\lambda \in \Lambda} p_\lambda^{n_\lambda} \qquad b = v \prod_{\lambda \in \Lambda} p_\lambda^{m_\lambda}$$

alors on a

$$\mathsf{pgcd}(a, b) = \prod_{\lambda \in \Lambda} p_\lambda^{\min\{n_\lambda, m_\lambda\}} \qquad \mathsf{ppcm}(a, b) = \prod_{\lambda \in \Lambda} p_\lambda^{\max\{n_\lambda, m_\lambda\}}.$$

En d'autres termes, pour tout $p \in A$ irréductible, on a $v_p(\mathsf{pgcd}(a, b)) = \min\{v_p(a), v_p(b)\}$ et $v_p(\mathsf{ppcm}(a, b)) = \max\{v_p(a), v_p(b)\}$. On remarque qu'on a $\mathsf{pgcd}(a, b)\,\mathsf{ppcm}(a, b)A = abA$.

Par induction, on peut facilement étendre la définition et parler du pgcd et du ppcm d'une famille *finie* d'éléments non nuls.

Proposition 1.2.11. Lemme de Gauss. Soient A un anneau factoriel et $a, b, c \in A\backslash\{0\}$ tels que $\mathsf{pgcd}(a, b) = 1$. Si $a \mid bc$, alors $a \mid c$.

Démonstration. Si $p \in A$ est irréductible et divise a, on a $v_p(b) = 0$ vu que $p \nmid b$ (a et b étant premiers entre eux). On a donc $v_p(a) \leqslant v_p(bc) = v_p(c)$. Comme c'est vrai pour tout p premier divisant a, on a $a \mid c$ (*cf* proposition 1.2.6 (2)). □

Proposition 1.2.12. Tout anneau principal est factoriel.

Lemme 1.2.13. Soit A un anneau intègre dans lequel élément irréductible est premier (*cf* proposition 1.2.7). Alors *si* un élément admet une décomposition en facteur irréductibles, cette dernière est unique (au sens de la définition 1.2.3).

Démonstration. Soit $a = up_1p_2 \cdots p_r$, avec $u \in A^\times$ et $p_1, \ldots, p_r$ des éléments irréductibles. Soit en outre $a = vq_1q_2 \cdots q_s$, avec $v \in A^\times$ et $q_1, \ldots, q_s$ des éléments irréductibles, une autre décomposition en facteur irréductibles.

Quitte à échanger les deux écritures, on peut supposer $r \leqslant s$. On procède par récurrence sur r. Si $r = 0$, alors $a = u \in A^\times$: le produit $vq_1q_2 \cdots q_s$ est inversible donc chacun de ses facteurs l'est, et on a nécessairement $s = 0$. Supposons $r \geqslant 1$. Comme p_1 est irréductible et divise le produit $vq_1q_2 \cdots q_s$, il divise l'un des facteurs (puisqu'il est premier). Comme v est inversible, il n'est pas divisible par p_1 qui ne l'est pas : quitte à renuméroter les q_i, on peut supposer $p_1 \mid q_1$ *i.e.* $p_1A = q_1A$. En divisant a par p_1, on se ramène au cas $r - 1$, ce qui permet de conclure. □

Démonstration de la proposition 1.2.12. Soient A un anneau principal et $a_0 \in A\backslash\{0\}$. Supposons que a_0 n'admet pas de décomposition en facteurs irréductibles. Alors a_0 n'est pas irréductible : il s'écrit $a_0 = a_1b_1$ avec $a_1, b_1 \in A\backslash(\{0\} \cup A^\times)$. Si a_1 et b_1 admettent tous les deux une décomposition en facteurs irréductiles, il en est de même de leur produit a_0, ce qui n'est pas : quitte à échanger a_1 et b_1, on peut supposer que a_1 n'admet pas de décomposition en facteurs irréductibles. On peut appliquer de nouveau ce raisonnement avec a_1 à la place de a_0 : on construit ainsi pas récurrence deux suites $(a_n)_{n \in \mathbf{N}}$ et $(b_n)_{n \in \mathbf{N}_{>0}}$ d'éléments de $A\backslash(\{0\} \cup A^\times)$ telles que pour tout $n \in \mathbf{N}$, on a

$a_n = a_{n+1}b_{n+1}$. La suite d'idéaux $(a_nA)_{n\in\mathbf{N}}$ est croissante (car $a_{n+1} \mid a_n$ pour tout $n \in \mathbf{N}$). Elle est donc stationnaire (car A est nœthérien) : il existe $n \in \mathbf{N}$ tel que $a_nA = a_{n+1}A$. Comme on a $a_n = a_{n+1}b_{n+1}$, cela implique $b_{n+1} \in A^\times$, ce qui est contradictoire.

Pour achever la preuve, il suffit (en vertu du lemme 1.2.13) de montrer que tout élément irréductible est premier. Soit $p \in A$ irréductible. Soit $\mathfrak{m} \subseteq A$ un idéal maximal de A contenant p (théorème de Krull, ou en utilisant le fait que A est nœthérien). Comme A est principal, il existe $a \in A$ avec $\mathfrak{m} = aA$, et $p \in \mathfrak{m} \Rightarrow (\exists b \in A)\ p = ab$. Comme p est irréductible, on a $b \in A^\times$ (car $a \notin A^\times$ vu que $\mathfrak{m} = aA \neq A$). Ainsi $pA = \mathfrak{m}$ est maximal. □

Remarque 1.2.14. Si A est un anneau principal, on a une autre caractérisation du pgcd et du ppcm de deux éléments $a, b \in A$. On a $\mathsf{pgcd}(a,b)A = aA + bA$ et $\mathsf{ppcm}(a,b)A = aA \cap bA$. Montrons-le pour le pgcd (la preuve pour le ppcm est analogue). Comme A est principal, il existe $d \in A$ tel que $aA + bA = dA$. Comme $x \in A$ divise a et b si et seulement si $aA \subseteq xA$ et $bA \subseteq xA$ *i.e.* $dA \subseteq xA$, on a bien $\mathsf{pgcd}(a,b) = d$.

Il ne faut pas croire que cette caractérisation est valable dans tout anneau factoriel. Par exemple, on peut montrer que $\mathbf{Q}[X,Y]$ est factoriel. Comme X et Y sont irréductibles et premiers entre eux, on a $\mathsf{pgcd}(X,Y) = 1$, bien que $X\,\mathbf{Q}[X,Y] + Y\,\mathbf{Q}[X,Y] \neq \mathbf{Q}[X,Y]$ (c'est l'idéal des polynômes qui s'annulent en $(0,0)$). Bien sûr, cela vient du fait que l'anneau $\mathbf{Q}[X,Y]$ n'est pas principal.

Exemples 1.2.15. Si K est un corps et $n \in \mathbf{N}_{>1}$, l'anneau $K[X_1, \ldots, X_n]$ est factoriel (*cf* théorème 1.2.27) mais pas principal (*cf* remarque précédente). De même, l'anneau $\mathbf{Z}[X]$ est factoriel (*cf loc. cit.*) mais pas principal (l'idéal engendré par 2 et X n'est pas principal).

Proposition 1.2.16. Si A est principal, ses idéaux premiers non nuls sont maximaux.

Démonstration. Soit $\mathfrak{p} \subseteq A$ premier non nul. D'après le théorème de Krull (théorème 1.0.1), il existe $\mathfrak{m} \subset A$ maximal tel que $\mathfrak{p} \subseteq \mathfrak{m}$. Comme A est principal, on a $\mathfrak{p} = pA$ et $\mathfrak{m} = aA$: on a $p = ab$ avec $b \in A$. Comme p est premier donc irréductible, on a $b \in A^\times$ (car $a \notin A^\times$ vu que $\mathfrak{m}$ est maximal), ce qui implique que $\mathfrak{p} = \mathfrak{m}$ est maximal. □

Définition 1.2.17. Soit A un anneau intègre.

- Un *stathme euclidien* est une application $\phi\colon A\backslash\{0\} \to \mathbf{N}$ telle que si $a, b \in A\backslash\{0\}$ sont tels que b divise a, alors $\phi(b) \leqslant \phi(a)$. Cette application sert de « mesure » pour la division euclidienne. Le stathme euclidien ϕ est dit *total* s'il est en fait à valeurs dans $\mathbf{N}_{>0}$.
- Un stathme euclidien ϕ définit une *division euclidienne* si pour tout $(a,b) \in A \times A\backslash\{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ et ($r = 0$ ou $\phi(r) < \phi(b)$). L'élément q s'appelle alors le **quotient** et r le **reste** de la division.
- Un anneau est un anneau *euclidien* si et seulement s'il admet un stathme euclidien définissant une division euclidienne.

Remarque 1.2.18. Si A est un anneau euclidien, il n'y a pas unicité d'un stathme euclidien sur A. En outre, on ne requiert pas l'unicité du quotient et du reste.

Exemples 1.2.19. Tout corps est un anneau euclidien. L'anneau $\mathbf{Z}$ est euclidien, avec le stathme donné par $\phi(a) = |a|$ (valeur absolue). Dans ce cas, la division est la division euclidienne habituelle (on a unicité –au signe près– dans ce cas). Si K est un corps, l'anneau de polynômes $K[X]$ est euclidien, avec le stathme donné par $\phi(P) = \deg(P)$ si $P \neq 0$, et $\phi(0) = 0$. Là encore, la division est la division euclidienne habituelle et elle est unique.

L'anneau $\mathbf{Z}[i] = \{a + ib \in \mathbf{C},\ a, b \in \mathbf{Z}\}$ des *entiers de Gauss* est euclidien, muni du stathme donné par $\phi(a + ib) = a^2 + b^2$.

Proposition 1.2.20. Tout anneau euclidien est principal.

Démonstration. Soient A un anneau euclidien, $\phi\colon A\backslash\{0\} \to \mathbf{N}$ un stathme euclidien et $I \subseteq A$ un idéal. Montrons que I est principal. On peut supposer $I \neq 0$. Dans ce cas, $\phi(I\backslash\{0\})$ est une partie non vide de $\mathbf{N}$, elle admet donc un plus petit élément : Soit $b \in I\backslash\{0\}$ un élément tel que $\phi(b)$ est minimal. On a bien sûr $bA \subseteq I$. Réciproquement, soit $a \in I$. Comme ϕ est euclidien, il existe $q, r \in A$ tels que $a = qb + r$ et $r = 0$ ou $\phi(r) < \phi(b)$. Supposons $r \neq 0$: on a $\phi(r) < \phi(b)$. Mais

$r = a - qb \in I$, et comme $r \neq 0$, on a $\phi(b) \leqslant \phi(r)$ par minimalité de $\phi(b)$, ce qui est contradictoire. On a donc en fait $r = 0$, et $a = qb \in bA$. Ainsi $I = bA$ est principal. □

Remarque 1.2.21. Il existe des anneaux qui sont principaux, mais pas euclidiens.

Corollaire 1.2.22. Soit K un corps, les anneaux $\mathbf{Z}$ et $K[X]$ sont principaux, donc factoriels (*cf* proposition 1.2.12).

Si $f\colon A \to B$ est un morphisme d'anneaux, il induit un morphisme d'anneaux $A[X] \to B[X]$. Si A est un sous-anneau de B, alors $A[X]$ est naturellement un sous-anneau de $B[X]$.

Définition 1.2.23. Soient A un anneau factoriel et $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]\backslash\{0\}$. Le **contenu** de P est

$$c(P) = \mathsf{pgcd}\{a_i/\ a_i \neq 0\}.$$

Lemme 1.2.24. Soient A un anneau factoriel et $P, Q \in A[X]\backslash\{0\}$. Alors $c(PQ) = c(P)c(Q)$.

Remarque 1.2.25. Le pgcd étant défini à multiplication par une unité près, on devrait plutôt écrire $c(PQ)A = c(P)c(Q)A$. Dans ce qui suit, on commettra systématiquement cet abus pour ne pas alourdir la rédaction.

Démonstration. On peut déjà écrire $P = c(P)\widetilde{P}$ et $Q = c(Q)\widetilde{Q}$ avec $c(\widetilde{P}) = 1$ et $c(\widetilde{Q}) = 1$: on a $PQ = c(P)c(Q)\widetilde{P}\widetilde{Q}$. Quitte à remplacer P et Q par $\widetilde{P}$ et $\widetilde{Q}$ respectivement, on peut supposer $c(P) = 1$ et $c(Q) = 1$, et il s'agit de prouver que $c(PQ) = 1$.

Supposons au contraire qu'il existe $p \in A$ premier tel que $p \mid c(PQ)$. Si on note $\overline{P}$ et $\overline{Q}$ les images dans $(A/pA)[X]$ de P et Q respectivement, cela implique que $\overline{PQ} = 0$ dans $(A/pA)[X]$. Mais comme p est premier, l'anneau A/pA est intègre : il en est de même de l'anneau $(A/pA)[X]$. On a donc $\overline{P} = 0$ ou $\overline{Q} = 0$, et donc $p \mid c(P)$ ou $p \mid c(Q)$, ce qui contredit $c(P) = 1$ et $c(Q) = 1$. □

Proposition 1.2.26. Supposons A factoriel. Soient $K = \mathsf{Frac}(A)$ et $P \in A[X]$ tel que $c(P) = 1$. Alors P est irréductible dans $A[X]$ si et seulement si P est irréductible dans $K[X]$.

Démonstration. Si P est irréductible dans $K[X]$ et $P = Q_1Q_2$ avec $Q_1, Q_2 \in A[X]$. Comme P est irréductible dans $K[X]$, quitte à échanger Q_1 et Q_2, le polynôme Q_1 est constant d'où $Q_1 = c(Q_1)$. Mais d'après le lemme 1.2.24, on a $1 = c(P) = c(Q_1)c(Q_2)$, donc $Q_1 \in A^\times$. Ainsi P est irréductible dans $A[X]$.

Réciproquement, supposons P irréductible dans $A[X]$ et $P = Q_1Q_2$ avec $Q_1, Q_2 \in K[X]$. Il existe $a_1, a_2 \in A\backslash\{0\}$ tels que $a_1Q_1 \in A[X]$ et $a_2Q_2 \in A[X]$. On a alors $a_1a_2 = c(a_1a_2P) = c(a_1Q_1)c(a_2Q_2)$ d'après le lemme 1.2.24, vu que $c(P) = 1$. Si on écrit $a_1Q_1 = c(a_1Q_1)\widetilde{Q}_1$ et $a_2Q_2 = c(a_2Q_2)\widetilde{Q}_2$ avec $\widetilde{Q}_1, \widetilde{Q}_2 \in A[X]$, on a donc $a_1a_2P = c(a_1Q_1)\widetilde{Q}_1c(a_2Q_2)\widetilde{Q}_2 = a_1a_2\widetilde{Q}_1\widetilde{Q}_2$ soit $P = \widetilde{Q}_1\widetilde{Q}_2$ (l'anneau A est intègre). Comme P est irréductible dans $A[X]$, quitte à échanger $\widetilde{Q}_1$ et $\widetilde{Q}_2$, on peut supposer $\widetilde{Q}_1 \in A^\times$. On a alors $Q_1 \in K^\times$ et P est irréductible dans $K[X]$. □

Théorème 1.2.27. Soit A un anneau factoriel. Alors l'anneau $A[X]$ est factoriel [a].

a. Il est facile de voir que la réciproque est vraie.

Démonstration. • Si $p \in A$ est irréductible, le polynôme constant p est irréductible dans $A[X]$. En effet, l'anneau A/pA est intègre : il en est de même de $A[X]/pA[X] \simeq (A/pA)[X]$ et p est premier donc irréductible dans $A[X]$.

• Si $P \in A[X]$ est de degré $\geqslant 1$ et irréductible, alors $c(P) = 1$. En effet, on peut écrire $P = c(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$, ce qui donne une factorisation non triviale si $c(P)$ est non inversible.

• Existence d'une décomposition en facteurs irréductibles. Soit $P \in A[X]\backslash\{0\}$. On peut écrire $P = c(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$ de contenu égal à 1. Comme A est factoriel, on peut décomposer $c(P)$ en facteurs irréductibles et il suffit de montrer qu'on peut décomposer $\widetilde{P}$: on peut supposer $c(P) = 1$. Si $P \in A$, on a alors $P = 1$: on peut supposer $\deg(P) \geqslant 1$. Soit K le corps des fractions de A. Comme l'anneau $K[X]$ est factoriel (*cf* corollaire 1.2.22), on peut écrire $P = P_1P_2\cdots P_r$

avec $P_i \in K[X]$ irréductible pour $i \in \{1,\dots,r\}$. Pour tout $i \in \{1,\dots,r\}$, soit $a_i \in A\backslash\{0\}$ tel que $a_iP_i \in A[X]$, et $\widetilde{P}_i = c(a_iP_i)^{-1}(a_iP_i) \in A[X]$. Comme $\widetilde{P}_i$ est de contenu 1 et irréductible dans $K[X]$ (car P_i l'est), il est irréductible dans $A[X]$ d'après la proposition 1.2.26. On a $a_1a_2\cdots a_r = c(a_1P_1)\cdots c(a_rP_r)$ en vertu du lemme 1.2.24, vu que $c(P) = 1$. On a donc la décomposition en facteurs irréductibles $P = \widetilde{P}_1\widetilde{P}_2\cdots\widetilde{P}_r$.
• Unicité de la décomposition en facteurs irréductibles. Soient $P \in A[X]\backslash\{0\}$ et $P = P_1P_2\cdots P_r$ et $P = Q_1Q_2\cdots Q_s$ deux décompostions en facteurs irréductibles dans $A[X]$. Quitte à renuméroter les P_i (resp. les Q_j), il existe $r_0 \leqslant r$ (resp. $s_0 \leqslant s$) tel que $P_i \in A\backslash\{0\}$ pour $i \leqslant r_0$ et $\deg(P_i) > 0$ pour $r_0 < i \leqslant r$ (resp. $Q_j \in A\backslash\{0\}$ pour $j \leqslant s_0$ et $\deg(Q_j) > 0$ pour $s_0 < j \leqslant s$). D'après la remarque faite plus haut, on a alors $c(P_i) = c(Q_j) = 1$ pour $r_0 < i \leqslant r$ et $s_0 < j \leqslant s$. En prenant le contenu de l'égalité $P_1P_2\cdots P_r = Q_1Q_2\cdots Q_s$, il vient donc $P_1P_2\cdots P_{r_0} = Q_1Q_2\cdots Q_{s_0}$, qui est une égalité de deux décompostions en facteurs irréductibles dans A. Ce dernier étant factoriel, on a $r_0 = s_0$, et quitte à renuméroter, on peut supposer $P_iA = Q_iA$ pour tout $i \in \{1,\dots,r_0\}$. En divisant P par $P_1P_2\cdots P_{r_0}$, il vient $P_{r_0+1}\cdots P_rA[X] = Q_{r_0+1}\cdots Q_sA[X]$. C'est une décomposition en facteurs irréductibles dans $K[X]$, qui est factoriel : on a $r = s$ et quitte à renuméroter, on peut supposer $P_iK[X] = Q_iK[X]$ pour $i \in \{r_0+1,\dots,r\}$. Mais comme $c(P_i) = c(Q_i) = 1$, on a en fait $P_iA[X] = Q_iA[X]$ pour $i \in \{r_0+1,\dots,r\}$. □

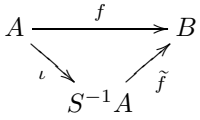
Remarque 1.2.28. (1) Au cours de la preuve, on a vu qu'une famille de représentants des éléments irréductibles de $A[X]$ est donnée par la réunion d'une famille de représentants des éléments irréductibles de A et d'une famille de polynômes de $A[X]$ de contenu 1 qui forment une famille de représentants des éléments irréductibles de $K[X]$.
(2) En général, il n'est pas vrai que A factoriel implique $A[\![X]\!]$ factoriel. C'est cependant vrai si A est suffisament « régulier ». C'est le cas par exemple lorsque A est un corps. On a un unique élément irréductible (à une unité près bien sûr) : X. En effet, toute série formelle non nulle s'écrit $f = a_nX^n + a_{n+1}X^{n+1} + \cdots$ avec $a_n \in A\backslash\{0\} = A^\times$. L'élément $u = a_n + a_{n+1}X + a_{n+2}X^2\cdots \in A[\![X]\!]$ est inversible, et on a $f = uX^n$ (l'unicité est évidente).

1.3. **Localisation.** Soit A un anneau.

Définition 1.3.1. Une partie $S \subset A$ est dite **multiplicative** si $1 \in S$ et S est stable par multiplication. Par commodité, on requiert en outre que $0 \notin S$.

Exemples 1.3.2. (1) $A^\times$.
(2) Si $f \in A$, l'ensemble $\{f^n\}_{n\in\mathbf{N}}$.
(3) Si $\mathfrak{p} \subset A$ est un idéal premier, $A\backslash\mathfrak{p}$.

Proposition 1.3.3. Soit $S \subset A$ une partie multiplicative. Il existe une A-algèbre $A \xrightarrow{\iota} S^{-1}A$, unique à isomorphisme près, ayant la propriété universelle suivante : si $f\colon A \to B$ est un morphisme d'anneaux tel que $(\forall s \in S)\ f(s) \in B^\times$, alors il existe un morphisme d'anneaux $\widetilde{f}\colon S^{-1}A \to B$ unique tel que $f = \widetilde{f} \circ \iota$.



Démonstration. Munissons l'ensemble $A \times S$ de la relation binaire $\sim$ définie par

$$(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow (\exists t \in S)\ t(a_1s_2 - a_2s_1) = 0$$

Il est facile (mais un peu fastidieux) de vérifier que c'est une relation d'équivalence. On note $S^{-1}A = (A \times S)/\sim$ l'ensemble quotient. Si $(a, s) \in A \times S$, on note $\frac{a}{s}$ son image dans $S^{-1}A$. Soient $(a_1, s_1), (a_2, s_2) \in A \times S$. Il est facile (mais un peu fastidieux) de vérifier que les éléments $\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{a_1s_2+a_2s_1}{s_1s_2}$ et $\frac{a_1}{s_1}.\frac{a_2}{s_2} := \frac{a_1a_2}{s_1s_2}$ ne dépendent que de $\frac{a_1}{s_1}$ et $\frac{a_2}{s_2}$, et que cela définit deux lois internes $+$ et $.$ sur $S^{-1}A$, qui en font un anneau commutatif d'unité $\frac{1}{1}$. Par ailleurs, l'application

$$\iota\colon A \to S^{-1}A$$
$$a \mapsto \tfrac{a}{1}$$

est un morphisme d'anneau. Observons que si $s \in S$, alors $\iota(s) = \frac{s}{1}$ est inversible dans $S^{-1}A$, d'inverse $\frac{1}{s}$.
Enfin, soit $f\colon A \to B$ un morphisme d'anneaux tel que $(\forall s \in S)\ f(s) \in B^\times$. On vérifie facilement que l'application

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

est un morphisme d'anneaux bien défini, et que c'est l'unique tel que $f = \widetilde{f} \circ \iota$. L'unicité de $(S^{-1}A, \iota)$ résulte de la propriété universelle. □

Définition 1.3.4. La A-algèbre $S^{-1}A$ s'appelle la **localisation** de A en S.

Remarque 1.3.5. (1) Par abus, si $a \in A$, on note encore a au lieu de $\iota(a)$ son image dans $S^{-1}A$.

(2) D'un certain point de vue, $S^{-1}A$ est la « plus petite » A-algèbre dans laquelle les éléments de S sont inversibles.

(3) Lorsque A est *intègre*, la relation binaire $\sim$ n'est autre que la relation « habituelle » $(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow a_1 s_2 = a_2 s_1$. Lorsque A n'est pas intègre, cette dernière n'est plus une relation d'équivalence (pourquoi ?), et il est nécessaire de rajouter le « t ».

(4) On a $\mathsf{Ker}(\iota) = \{a \in A,\ (\exists s \in S)\ sa = 0\}$. En particulier, ι est injective dès que A est intègre.

(5) À moins que A soit factoriel, on n'a pas de notion de « fraction irréductible ».

Exemples 1.3.6. (1) Supposons A intègre (c'est le seul cas qu'on rencontrera dans la suite du cours). Alors $A\backslash\{0\}$ est multiplicative ($\{0\}$ est premier), et $(A\backslash\{0\})^{-1}A = \mathsf{Frac}(A)$ est le **corps des fractions** de A. Par exemple, on a $\mathsf{Frac}(\mathbf{Z}) = \mathbf{Q}$, $\mathsf{Frac}(K[X]) = K(X)$ si K est un corps).

Si maintenant $S \subset A$ est une partie multiplicative quelconque, la propriété universelle fournit un morphisme injectif $S^{-1}A \to \mathsf{Frac}(A)$: les localisations de A s'identifient à des sous-anneaux de $\mathsf{Frac}(A)$.

(2) Si $f \in A$, on note $A_{(f)}$ le localisé de A par rapport à la partie multiplicative $\{f^n\}_{n\in\mathbf{N}}$. Par exemple, $\mathbf{Z}_{(10)}$ n'est autre que l'anneau des nombres décimaux.

(3) Si $\mathfrak{p} \subset A$ est un idéal premier, on note $A_\mathfrak{p}$ le localisé de A par rapport à la partie multiplicative $A\backslash\mathfrak{p}$. Lorsque A est intègre et $\mathfrak{p} = \{0\}$, on retrouve $\mathsf{Frac}(A)$.

(4) Exercice : trouver des parties multiplicatives $S \subset \mathbf{Z}$ autres que $\mathbf{Z}\backslash\{0\}$ telles que $S^{-1}\mathbf{Z} = \mathbf{Q}$.

Définition 1.3.7. Si $S \subset A$ est une partie multiplicative et M un A-module, on définit la localisation $S^{-1}M$ de M par rapport à S de façon analogue à $S^{-1}A$: c'est l'ensemble quotient de $M \times S$ par la relation d'équivalence $(m_1, s_1) \sim (m_2, s_2) \Leftrightarrow (\exists t \in S)\ t(m_1 s_2 - m_2 s_1) = 0$. C'est un $S^{-1}A$-module avec les lois interne et externes données par $\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{m_1 s_2 + m_2 s_1}{s_1 s_2}$ et $\frac{a}{s}.\frac{m}{s'} := \frac{am}{ss'}$. Par ailleurs, un morphisme $f\colon M \to N$ de A-modules induit un morphisme $f_S\colon S^{-1}M \to S^{-1}N$ de $S^{-1}A$-modules (en posant $f_S\big(\frac{m}{s}\big) = \frac{f(m)}{s}$ pour tout $m \in M$ et $s \in S$).

En particulier, si I est un idéal de A, c'est un sous-A-module de A : on dispose de l'idéal $S^{-1}I$ de $S^{-1}A$.

Proposition 1.3.8. (1) On a $\big(\mathrm{Id}_M\big)_S = \mathrm{Id}_{S^{-1}M}$.
(2) Si $f\colon M \to M'$ et $g\colon M' \to M''$ sont A-linéaires alors $(g \circ f)_S = g_S \circ f_S$.
(3) $M \subseteq N$, alors $S^{-1}M \subseteq S^{-1}N$ et $S^{-1}(N/M) \simeq S^{-1}N/S^{-1}M$.
(4) Si $f\colon M \to N$ est A-linéaire, on a $\mathsf{Ker}(f_S) = S^{-1}\,\mathsf{Ker}(f)$ et $\mathsf{Coker}(f_S) = S^{-1}\,\mathsf{Coker}(f)$.

Démonstration. (3) Le composé $M \subseteq N \xrightarrow{\iota} S^{-1}N$ s'étend en $i\colon S^{-1}M \to S^{-1}N$ (par $S^{-1}A$-linéarité). Soit $x \in S^{-1}M$: écrivons $x = \frac{m}{s}$ avec $m \in M$ et $s \in S$. Si $i(x) = 0$, il existe $t \in S$ tel que $tm = 0$ dans $M \subseteq N$, ce qui implique que $x = \frac{m}{s} = 0$ dans $S^{-1}M$: l'application i est injective. On la voit comme une inclusion $S^{-1}M \subseteq S^{-1}N$.
La projection canonique $\pi\colon N \to N/M$ induit le morphisme $S^{-1}A$-linéaire $S^{-1}N \xrightarrow{\pi_S} S^{-1}(N/M)$. Il est surjectif : si $x \in S^{-1}(N/M)$ il existe $\overline{n} \in N/M$ et $s \in S$ tel que $x = \frac{\overline{n}}{s}$. Soit $n \in N$ relevant $\overline{n}$: on a $\pi_S\big(\frac{n}{s}\big) = x$. Bien entendu, on a $S^{-1}M \subseteq \mathsf{Ker}(\pi_S)$. Réciproquement, si $x =$

$\frac{n}{s} \in \mathsf{Ker}(\pi_S)$ (avec $n \in N$ et $s \in S$), on a $\frac{\pi(n)}{s} = 0$ dans $S^{-1}(N/M)$: il existe $t \in S$ tel que $t\pi(n) = \pi(tn) = 0$ dans N/M, *i.e.* $tn \in M$, soit encore $x = \frac{tn}{ts} \in S^{-1}M$. Ainsi $\mathsf{Ker}(\pi_S) = S^{-1}M$ et $S^{-1}N/S^{-1}M \xrightarrow{\sim} S^{-1}(N/M)$.
(4) Résulte de (3). □

Proposition 1.3.9. Soit $S \subset A$ est une partie multiplicative. Si A est nœthérien, il en est de même de $S^{-1}A$.

Démonstration. Soit I un idéal de $S^{-1}A$. Posons $J = I \cap A := \iota^{-1}(I)$: c'est un idéal de A. Comme ce dernier est nœthérien, J est de type fini $J = \sum_{i=1}^{r} A\alpha_i$. Soit $x = \frac{a}{s} \in I$, alors $sx = a \in I$, donc $a \in J$, ce qui implique que $x \in \sum_{i=1}^{r} \frac{1}{s}\iota(A\alpha_i)$ et donc $I \subseteq \sum_{i=1}^{r} S^{-1}A\iota(\alpha_i)$. C'est en fait une égalité, et I est de type fini. □

Notation. On note $\mathsf{Spec}(A)$ l'ensemble des idéaux premiers de A. On l'appelle le **spectre** de A.

Proposition 1.3.10. Soit $S \subset A$ est une partie multiplicative. Les applications

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

sont des bijections croissantes inverses l'une de l'autre.

Démonstration. Soit $\mathfrak{p} \in \mathsf{Spec}(A)$ tel que $\mathfrak{p} \cap S = \varnothing$. On a $S^{-1}A/S^{-1}\mathfrak{p} \simeq S^{-1}(A/\mathfrak{p})$ (*cf* proposition 1.3.8). Notons $\overline{S}$ l'image de S dans $A/\mathfrak{p}$: comme $\mathfrak{p} \cap S = \varnothing$, on a $0 \notin \overline{S}$, et $\overline{S}$ est une partie multiplicative de $A/\mathfrak{p}$. Comme $A/\mathfrak{p}$ est intègre, il en est de même du localisé $S^{-1}(A/\mathfrak{p}) = \overline{S}^{-1}(A/\mathfrak{p}) \subset \mathsf{Frac}(A/\mathfrak{p})$, de sorte que $S^{-1}\mathfrak{p}$ est premier dans $S^{-1}A$.
Inversement, si $\mathfrak{q} \in \mathsf{Spec}(S^{-1}A)$, alors $A/\iota^{-1}(\mathfrak{q}) \hookrightarrow S^{-1}A/\mathfrak{q}$ est intègre : on a $\mathfrak{q} \cap A \in \mathsf{Spec}(A)$. Si $s \in (\mathfrak{q} \cap A) \cap S$, alors $s \in \mathfrak{q}$. Comme s est inversible dans $S^{-1}A$, on a donc $\mathfrak{q} = S^{-1}A$, ce qui n'est pas : on a $(\mathfrak{q} \cap A) \cap S = \varnothing$.
Soit $\mathfrak{p} \in \mathsf{Spec}(A)$ tel que $\mathfrak{p} \cap S = \varnothing$. On a bien sûr $\mathfrak{p} \subseteq S^{-1}\mathfrak{p} \cap A$. Réciproquement, soit $a \in S^{-1}\mathfrak{p} \cap A$: on peut écrire $a = \frac{\alpha}{s}$ avec $\alpha \in \mathfrak{p}$ et $s \in S$. Comme $sa = \alpha \in \mathfrak{p}$ et $s \notin \mathfrak{p}$ (car $\mathfrak{p} \cap S = \varnothing$), on a $a \in \mathfrak{p}$, ce qui prouve l'égalité $\mathfrak{p} = S^{-1}\mathfrak{p} \cap A$.
Soit $\mathfrak{q} \in \mathsf{Spec}(S^{-1}A)$. On a bien sûr $S^{-1}(\mathfrak{q} \cap A) \subseteq \mathfrak{q}$. Réciproquement, soit $x \in \mathfrak{q}$: écrivons $x = \frac{a}{s}$ avec $a \in A$ et $s \in S$. On a $sx = a \in \mathfrak{q} \cap A$, et donc $x = \frac{a}{s} \in S^{-1}(\mathfrak{q} \cap A)$, ce qui prouve l'égalité $\mathfrak{q} = S^{-1}(\mathfrak{q} \cap A)$. □

Remarque 1.3.11. On a donc $\mathsf{Spec}(S^{-1}A) \subseteq \mathsf{Spec}(A)$. Il se trouve que l'ensemble $\mathsf{Spec}(A)$ peut être muni d'une structure d'espace topologique (et même de bien plus...) et que la bijection de la proposition 1.3.10 est un homéomorphisme. De ce point de vue, la localisation de l'anneau A induit une « localisation » de l'espace $\mathsf{Spec}(A)$, ce qui explique la terminologie.

Définition 1.3.12. Un anneau **local** est un anneau n'ayant qu'un seul idéal maximal.

Exemples 1.3.13. (1) Un corps est un anneau local.
(2) Si K est un corps, l'anneau des séries formelles $K[\![X]\!]$ est local, d'idéal maximal $XK[\![X]\!]$.
(3) Exercice : A est local si et seulement si $A\backslash A^\times$ est un idéal [1] : c'est alors l'idéal maximal de A.

1. Si A est local d'idéal maximal $\mathfrak{m}$, on a bien sûr $\mathfrak{m} \subseteq A\backslash A^\times$, et si $a \in A\backslash A^\times$, l'idéal aA est strict : il est contenu dans un idéal maximal en vertu du théorème de Krull (théorème 1.0.1), donc $a \in \mathfrak{m}$, ce qui prouve l'égalité $\mathfrak{m} = A\backslash A^\times$. Réciproquement, si $\mathfrak{m} := A\backslash A^\times$ est un idéal, et si I est un idéal propre de A, on a $I \cap A^\times = \varnothing$, *i.e.* $I \subseteq \mathfrak{m}$ et $\mathfrak{m}$ contient *tous* les idéaux de A.

Corollaire 1.3.14. Si $\mathfrak{p} \in \mathsf{Spec}(A)$, alors $\mathsf{Spec}(A_\mathfrak{p}) = \{\mathfrak{q}A_\mathfrak{p},\ \mathfrak{q} \in \mathsf{Spec}(A),\ \mathfrak{q} \subseteq \mathfrak{p}\}$. En particulier, $A_\mathfrak{p}$ est un anneau local [a] d'idéal maximal $\mathfrak{p}A_\mathfrak{p}$.

a. La terminologie est bien faite, là encore...

Démonstration. L'égalité résulte de l'équivalence $\mathfrak{q} \cap (A \backslash \mathfrak{p}) = \varnothing \Leftrightarrow \mathfrak{q} \subseteq \mathfrak{p}$ et de la proposition 1.3.10. Les bijections de *loc. cit.* étant croissantes (au sens de l'inclusion), les éléments maximaux se correspondent, ce qui achève la preuve. □

Lemme 1.3.15. Soit M un A-module. Alors $M = \{0\}$ si et seulement si $M_\mathfrak{m} = \{0\}$ pour tout idéal maximal $\mathfrak{m} \subset A$.

Démonstration. Supposons $M_\mathfrak{m} = \{0\}$ pour tout idéal maximal $\mathfrak{m} \subset A$. Soit $m \in M$. Posons $I = \{a \in A,\ am = 0\}$: c'est un idéal de A. Supposons $I \neq A$: d'après le théorème de Krull (théorème 1.0.1), il existe $\mathfrak{m} \subset A$ maximal tel que $I \subseteq \mathfrak{m}$. Comme $m = \frac{m}{1}$ est nul dans $M_\mathfrak{m}$, il existe $t \in A \backslash \mathfrak{m}$ tel que $tm = 0$ dans M, *i.e.* $t \in I$. On a donc $t \in I \backslash \mathfrak{m}$ contradiction : $I = A$ et $m = 0$. □

Proposition 1.3.16. Principe local-global. Soient M un A-module et M', M'' deux sous-modules de M. Alors $M' \subseteq M''$ (resp. $M' = M''$) si et seulement si pour tout idéal maximal $\mathfrak{m}$ de A, on a $M'_\mathfrak{m} \subseteq M''_\mathfrak{m}$ (resp. $M'_\mathfrak{m} = M''_\mathfrak{m}$) dans $M_\mathfrak{m}$.

Démonstration. Si $M' \subseteq M''$, on sait déjà que $M'_\mathfrak{m} \subseteq M''_\mathfrak{m}$ pour tout idéal maximal $\mathfrak{m}$ de A (proposition 1.3.8 (3)). Réciproquement, supposons $M'_\mathfrak{m} \subseteq M''_\mathfrak{m}$ pour tout idéal maximal $\mathfrak{m}$ de A. Posons $\overline{M} = M/M''$ et $\pi \colon M \to \overline{M}$ la projection canonique. On dispose de $\pi(M') \subseteq \overline{M}$. Par hypothèse, on a $\pi(M')_\mathfrak{m} = \{0\}$ (parce que $M'_\mathfrak{m} \subseteq M''_\mathfrak{m}$ a une image nulle dans $\overline{M}_\mathfrak{m} = M_\mathfrak{m}/M''_\mathfrak{m}$, *cf* proposition 1.3.8 (3)) pour tout idéal maximal $\mathfrak{m}$ de A. D'après le lemme 1.3.15, cela implique $\pi(M') = \{0\}$ dans $\overline{M}$, *i.e.* $M' \subseteq M''$. □

Remarque 1.3.17. Un exemple important du résultat précédent est le suivant : si I et J sont deux idéaux de A, on a $I \subset J$ si et seulement si $I_\mathfrak{m} \subseteq J_\mathfrak{m}$ pour tout idéal maximal $\mathfrak{m}$ de A.

Définition 1.3.18. (1) Soit K un corps. Une **valuation discrète** sur K est une application $v \colon K \to \mathbf{R} \cup \{+\infty\}$ telle que
- $(\forall x, y \in K)\ v(xy) = v(x) + v(y)$ (cela implique $v(1) = 0$) ;
- $(\forall x, y \in K)\ v(x + y) \geqslant \min(v(x), v(y))$;
- $v(K^\times)$ est un sous-groupe discret de $\mathbf{R}$ (donc de la forme $\alpha\,\mathbf{Z}$ avec $\alpha \neq 0$).

On dit que v est **normalisée** lorsque $v(K^\times) = \mathbf{Z}$.
(2) Un **anneau de valuation discrète** est un anneau principal ayant un et un seul idéal premier non nul. Un générateur de ce dernier s'appelle une **uniformisante** de A.

Remarque 1.3.19. Supposons A de valuation discrète. L'unique idéal premier non nul $\mathfrak{m}$ de A est donc maximal : A est local. Les élements de $\mathfrak{m}$ ne sont pas inversibles : comme $\mathfrak{m} \neq 0$, l'anneau A n'est pas un corps.

Proposition 1.3.20. Soient A un anneau de valuation discrète, $\mathfrak{m}$ son idéal maximal, π une uniformisante et $K = \mathsf{Frac}(A)$.
(1) Tout $a \in A \backslash \{0\}$ s'écrit de façon unique sous la forme $a = u\pi^{v(a)}$ avec $u \in A^\times$ et $v(a) \in \mathbf{N}$;
(2) les idéaux non nuls de A sont tous de la forme $\mathfrak{m}^i = \pi^i A$ (avec $i \in \mathbf{N}$) ;
(3) $\bigcap_{i \in \mathbf{N}} \mathfrak{m}^i = \{0\}$;
(4) l'application $v \colon A \backslash \{0\} \to \mathbf{N}$ se prolonge de façon unique en une valuation discrète normalisée $v \colon K \to \mathbf{Z} \cup \{+\infty\}$;
(5) $A = \{x \in K,\ v(x) \geqslant 0\}$.

Démonstration. (1) Comme A est principal, il est factoriel. Comme $\mathfrak{m} = \pi A$ est le seul idéal premier non nul, il n'y a (à multiplication par un élément inversible près) qu'un élément irréductible : c'est

π. Si $a \in A\backslash\{0\}$, sa décomposition en produit d'irréductibles est donc $a = u\pi^{v(a)}$ pù $u \in A^\times$ et $v(a) = v_\pi(a) \in \mathbf{N}$ est la valuation π-adique de a.
(2) Si $I \subseteq A$ est un idéal, il est principal : on a $I = aA$ avec $a \in A$. Si $I \neq \{0\}$, on a $a \neq 0$, et on peut écrire $a = u\pi^i$ avec $u \in A^\times$ et $i = v(a) \in \mathbf{N}$: on a alors $I = \pi^i A = \mathfrak{m}^i$.
(3) Si $a \in A\backslash\{0\}$, on a $a = u\pi^i$ avec $u \in A^\times$ et $i = v(a)$, donc $a \in \mathfrak{m}^i\backslash\mathfrak{m}^{i+1}$, et $a \notin \bigcap_{i\in\mathbf{N}} \mathfrak{m}^i$. Ainsi, on a $\bigcap_{i\in\mathbf{N}} \mathfrak{m}^i = \{0\}$.
(4) Si $x = \frac{a}{b} \in K$, avec $a \in A$ et $b \in A\backslash\{0\}$, on a nécessairement $v(x) = v(a) - v(b) \in \mathbf{Z} \cup \{+\infty\}$, ce qui prouve l'unicité. Si $x = \frac{a'}{b'}$ est une autre écriture, on a $ab' = a'b$ (car A est intègre), donc $v(a) + v(b') = v(a') + v(b)$ *i.e.* $v(a) - v(b) = v(a') - v(b')$, ce qui montre l'existence.
(5) On sait déjà que $(\forall a \in A)\ v(a) \in \mathbf{N} \cup \{+\infty\}$. Réciproquement, soit $x = \frac{a}{b} \in K$ avec $a \in A$ et $b \in A\backslash\{0\}$. On a $v(x) \geqslant 0 \Rightarrow v(a) \geqslant v(b) \Rightarrow b \mid a$ (*cf* proposition 1.2.6 (2)), donc $x \in A$. □

1.4. **Critères d'irréductibilité.** Dans toute cette section, A désigne un anneau *intègre*.

Proposition 1.4.1. Supposons A factoriel. Soient K son corps des fractions et $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ un polynôme de degré n. Soient $a, b \in A\backslash\{0\}$ premiers entre eux tels que a/b soit une racine de P. Alors $a \mid a_0$ et $b \mid a_n$.

Démonstration. On a $b^nP(a/b) = a_0b^n + a_1b^{n-1}a + a_2b^{n-2}a^2 + \cdots + a_{n-1}ba^{n-1} + a_na^n = 0$. On a donc $a \mid a_0b^n$. Comme $\mathsf{pgcd}(a, b) = 1$, le lemme de Gauss (*cf* proposition 1.2.11) implique $a \mid a_0$. Un raisonnement identique implique $b \mid a_n$. □

Exemple 1.4.2. Soit $P = 2X^3 - X^2 + X - 1 \in \mathbf{Z}[X]$. Si $x = a/b \in \mathbf{Q}$ est racine de P, avec $a, b \in \mathbf{Z}\backslash\{0\}$ premiers entre eux, alors $a \in \{\pm 1\}$ et $b \mid 2$. On vérifie que $1/2$ est racine de P et on a (par division euclidienne) $P = (2X - 1)(X^2 + X + 1)$. De même, si $x = a/b \in \mathbf{Q}$ est racine de $X^2 + X + 1$, avec $a, b \in \mathbf{Z}\backslash\{0\}$ premiers entre eux, alors $a, b \in \{\pm 1\}$ *i.e.* $x \in \{\pm 1\}$. Mais 1 et -1 ne sont pas racines, si bien que $X^2 + X + 1$ est irréductible dans $\mathbf{Q}[X]$, donc dans $\mathbf{Z}[X]$ (proposition 1.2.26).

Lemme 1.4.3. Soit $P \in A[X]$ unitaire et réductible. Alors il existe $P_1, P_2 \in A[X]$ unitaires tels que $P = P_1P_2$ et $\deg(P_1), \deg(P_2) < \deg(P)$.

Démonstration. Comme P est réductible, il s'écrit $P = P_1P_2$ avec $P_1, P_2 \in A[X]\backslash A^\times$. L'anneau A étant intègre, le coefficient dominant de P (c'est-à-dire 1) est le produit des coefficients dominants de P_1 et de P_2 : ces derniers sont inversibles, inverses l'un de l'autre. Comme $P_1 \notin A^\times$ et $P_2 \notin A^\times$, les polynômes P_1 et P_2 sont non constants : on a $\deg(P_1), \deg(P_2) < \deg(P)$. Quitte à diviser P_1 et P_2 par leurs coefficients dominants respectifs, on peut supposer P_1 et P_2 unitaires. □

Proposition 1.4.4. (Critère d'irréductibilité par réduction). Soient $I \subseteq A$ un idéal *strict* et $P \in A[X]$ un polynôme *unitaire*. Si l'image de P dans $(A/I)[X]$ ne se factorise pas en un produit de deux polynômes de degrés $< \deg(P)$, alors P est irréductible dans $A[X]$.

Démonstration. Supposons P réductible : on peut écrire $P = P_1P_2$ avec $P_1, P_2 \in A[X]$ unitaires et $\deg(P_1), \deg(P_2) < \deg(P)$ (lemme 1.4.3). Notons avec un barre l'image d'un élément de $A[X]$ dans $(A/I)[X]$: on a $\overline{P} = \overline{P_1}\,\overline{P_2}$ avec $\deg(\overline{P_1}) < \deg(\overline{P})$ $(= \deg(P)$ vu que P est unitaire) et $\deg(\overline{P_2}) < \deg(\overline{P})$, ce qui n'est pas, contradiction. □

Exemples 1.4.5. (1) Le polynôme $X^2 + X + 1 \in \mathbf{Z}[X]$ est irréductible, parce qu'il est unitaire et que son image modulo 2 est irréductible.
(2) Soit $P = X^2 + XY + 1 \in \mathbf{Q}[X, Y]$. On prend $A = \mathbf{Q}[Y]$ et $I = Y\,\mathbf{Q}[Y]$ l'idéal engendré par Y. On a $A/I = \mathbf{Q}$ et l'image (modulo I) de P dans $\mathbf{Q}[X]$ est $X^2 + 1$ (qui est irréductible, de degré 2 et n'ayant pas de racine dans le corps $\mathbf{Q}$). Le polynôme P est donc irréductible dans $\mathbf{Q}[X, Y]$.

Remarque 1.4.6. L'hypothèse P unitaire n'est pas superflue : si $P = (1 + X^2)(1 + Y) \in \mathbf{Q}[X, Y]$, alors P n'est pas irréductible, mais sa réduction modulo Y l'est (c'est $X^2 + 1 \in \mathbf{Q}[X]$). C'est parce que le terme dominant de P est X^2Y, qui n'est pas unitaire (que ce soit en la variable X ou en la variable Y). Il convient donc d'être soigneux.

Proposition 1.4.7. (Critère d'Eisenstein). Soient $\mathfrak{p} \subseteq A$ un idéal premier, $n \in \mathbf{N}_{>0}$ et $P = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n \in A[X]$ un polynôme unitaire. Supposons que $a_0, a_1, \ldots, a_{n-1} \in \mathfrak{p}$ mais $a_0 \notin \mathfrak{p}^2$. Alors P est irréductible.

Démonstration. Supposons P réductible : on peut écrire $P = P_1P_2$ avec $P_1, P_2 \in A[X]$ unitaires et $\deg(P_1), \deg(P_2) < \deg(P)$ (lemme 1.4.3). Posons $k = \deg(P_1)$: on a $0 < k < n$. Notons avec une barre l'image d'un élément de $A[X]$ dans $(A/\mathfrak{p})[X]$: on a $\overline{P} = X^n = \overline{P_1}\,\overline{P_2}$ dans $\mathsf{Frac}(A/\mathfrak{p})[X]$, qui est factoriel : cela implique $\overline{P_1} = X^k$ et $\overline{P_2} = X^{n-k}$ (on sait qu'ils sont unitaires parce que P_1 et P_2 le sont). Les termes constants de $\overline{P_1}$ et de $\overline{P_2}$ sont donc nuls. Ainsi, les termes constants de P_1 et de P_2 sont dans $\mathfrak{p}$. Le terme constant de P étant le produit des termes constants de P_1 et de P_2, il appartient à $\mathfrak{p}^2$, ce qui n'est pas : contradiction. □

Remarque 1.4.8. (1) Bien sûr, l'hypothèse $a_0 \notin \mathfrak{p}^2$ est cruciale, par exemple, le polynôme $X^2 - 4 = (X-2)(X-2) \in \mathbf{Z}[X]$ n'est pas irréductible (avec $\mathfrak{p} = 2\,\mathbf{Z}$).

(2) Soient $\mathfrak{p} \subset A$ premier et $P = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + a_nX^n \in A[X]$ avec $a_n \notin \mathfrak{p}$, $a_0, a_1, \ldots, a_{n-1} \in \mathfrak{p}$ mais $a_0 \notin \mathfrak{p}^2$. Alors P n'est pas irréductible dans $A[X]$ en général : par exemple, $P = 2(X^2+3X+3) \in \mathbf{Z}[X]$ avec $\mathfrak{p} = 3\,\mathbf{Z}[X]$. Cependant, l'image de P dans $A_\mathfrak{p}[X]$ est un polynôme d'Eisenstein (on a $a_n \in A_\mathfrak{p}^\times$), de sorte que cette image est irréductible dans $A_\mathfrak{p}[X]$. Si A est factoriel, cela implique que P est irréductible dans $\mathsf{Frac}(A)[X]$.

Exemples 1.4.9. (1) Le polynôme $X^4 + 4X^3 + 6X^2 + 10$ est irréductible dans $\mathbf{Z}[X]$ (prendre $\mathfrak{p} = 2\,\mathbf{Z}$). Par contre, le critère ne s'applique pas au polynôme $X^5 - 4$ (qui est irréductible dans $\mathbf{Z}[X]$ cependant).

(2) Soit p un nombre premier et $\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbf{Z}[X]$ le p-ième polynôme cyclotomiques. Alors Φ_p est irréductible. Pour le montrer, on remarque que $\Phi_p = \frac{X^p-1}{X-1} \in \mathbf{Q}(X)$: on effectue le changement de variable $X = Y + 1$. On a alors $\Phi_p = \frac{(Y+1)^p-1}{Y}$ d'où

$$\Phi_p(Y+1) = Y^{p-1} + \tbinom{p}{1}Y^{p-2} + \tbinom{p}{2}Y^{p-3} + \cdots + \tbinom{p}{p-1}.$$

Comme $p \mid \binom{p}{k}$ pour tout $k \in \{1, \ldots, p-1\}$ et $\binom{p}{p-1} = p$ est non divisible par p^2, le critère d'Eisenstein s'applique (avec $\mathfrak{p} = p\,\mathbf{Z}$) et $\Phi_p(Y+1)$ est irréductible dans $\mathbf{Z}[Y]$: il en est de même de Φ_p.

(3) Le polynôme $X^3 + XY^2 + Y \in \mathbf{Z}[X, Y]$ est irréductible en vertu du critère d'Eisenstein (prendre $\mathfrak{p} = Y\,\mathbf{Z}[Y]$). Remarquons que dans ce cas, l'application de la proposition 1.4.4, (en quotientant par Y) ne permet pas de conclure.

1.5. **Modules de type fini sur les anneaux principaux.** On suppose désormais A principal. Par définition, A est intègre : on note K son corps des fractions. Rappelons que A est factoriel (proposition 1.2.12) : on dispose du pgcd et du ppcm. En outre, comme les idéaux de A sont engendrés par un élément, ils sont de type fini, *i.e.* A est nœthérien.

Dans ce qui suit, quand on écrit une matrice, les coefficients vides correspondent à des zéros. Si $n \in \mathbf{N}_{>0}$ et $a_1, \ldots, a_n \in A$, on pose

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

Par ailleurs, si $M = \big(m_{i,j}\big)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}} \in \mathsf{M}_{n\times m}(A)$, on note ${}^{\mathrm{T}}M = \big(m_{j,i}\big)_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} \in \mathsf{M}_{m\times n}(A)$ la matrice **transposée** de M.

Fixons une famille $(p_\lambda)_{\lambda\in\Lambda}$ de représentants des éléments irréductibles de A. Tout élément $a \in A\backslash\{0\}$ admet une décomposition unique en facteurs irréductibles :

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

où $u \in A^\times$ et $(n_\lambda)_{\lambda\in\Lambda}$ est une famille d'entiers presque tous nuls (*i.e.* tous nuls sauf un nombre fini). On pose alors

$$\ell(a) = \sum_{\lambda\in\Lambda} n_\lambda \in \mathbf{N}$$

qu'on appelle **longueur** de a. Ce n'est autre que le nombre de facteurs irréductibles de a (par exemple, on a $\ell(a) = 0 \Leftrightarrow a \in A^\times$ et $\ell(a) = 1$ si et seulement si A est irréductible).
Si $M = [m_{i,j}]_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} \in \mathsf{M}_{n\times m}(A)\backslash\{0\}$, on pose

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

Définition 1.5.1. (1) Si $n \in \mathbf{N}_{>0}$ on pose $\mathsf{GL}_n(A) = \{M \in \mathsf{M}_n(A),\ \det(M) \in A^\times\}$. D'après les formules de Cramer, c'est le groupe des éléments inversibles de $\mathsf{M}_n(A)$ (prendre garde que $\det(A) \neq 0$ est insuffisant si A n'est pas un corps). On pose $\mathsf{SL}_n(A) = \{M \in \mathsf{M}_n(A),\ \det(M) = 1\}$. C'est un sous-groupe de $\mathsf{GL}_n(A)$.

(2) Si $\sigma \in \mathfrak{S}_n$ est une permutation, on pose $P_\sigma = \big(\delta_{\sigma(i),j}\big)_{1\leqslant i,j\leqslant n} \in \mathsf{M}_n(A)$ (où $\delta_{i,j}$ est le symbole de Kronecker). On a $\det(P_\sigma) = (-1)^{\varepsilon(\sigma)}$ (où $\varepsilon(\sigma)$ désigne la signature de σ), de sorte que $P_\sigma \in \mathsf{GL}_n(A)$. Posons $\widetilde{P}_\sigma = \mathsf{diag}\big(1,\dots,1,(-1)^{\varepsilon(\sigma)}\big)P_\sigma \in \mathsf{SL}_n(A)$.

Si $M \in \mathsf{M}_{n\times m}(A)$, la matrice $P_\sigma M$ est l'élément de $\mathsf{M}_{n\times m}(A)$ dont la i-ième ligne est la $\sigma(i)$-ième ligne de M. De même, si $\gamma \in \mathfrak{S}_m$ est une permutation, la matrice MP_γ est déduite de M en permutant les colonnes suivant γ. En multipliant M par $\widetilde{P}_\sigma$ à gauche (resp. par $\widetilde{P}_\gamma$ à droite), on permute les lignes suivant σ (resp. les colonnes suivant γ) et on multiplie la dernière ligne (resp. colonne) par $(-1)^{\varepsilon(\sigma)}$ (resp. $(-1)^{\varepsilon(\gamma)}$).

Proposition 1.5.2. Soient $n \in \mathbf{N}_{\geqslant 2}$ et $a_1,\dots,a_n$ des éléments de A qui engendrent l'idéal A. Alors il existe une matrice dans $\mathsf{SL}_n(A)$ dont la première colonne est ${}^{\mathrm{T}}(a_1,\dots,a_n)$.

Démonstration. Posons $X = {}^{\mathrm{T}}(a_1,\dots,a_n)$. Il s'agit de prouver l'existence d'une matrice $M \in \mathsf{M}_n(A)$ de déterminant 1 telle que $M^{-1}X = {}^{\mathrm{T}}(1,0,\dots,0)$. On procède par récurrence sur $n \geqslant 2$.

Cas $n = 2$. Comme $A = Aa_1 + Aa_2$, il existe $u, v \in A$ tels que $va_1 - ua_2 = 1$. La matrice $M = \begin{pmatrix} a_1 & u \\ a_2 & v \end{pmatrix}$ répond alors à la question.

Cas $n > 2$. Soit $dA = \mathsf{pgcd}(a_2,\dots,a_n)$ et $b_2,\dots,b_n \in A$ tels que $db_i = a_i$ pour $i \in \{2,\dots,n\}$. On a $\mathsf{pgcd}(b_2,\dots,b_n) = A$: par hypothèse de récurence, il existe $M_1' \in \mathsf{M}_{n-1}(A)$ de déterminant 1 telle que $M_1'^{-1}Y = {}^{\mathrm{T}}(1,0,\dots,0)$ où $Y = {}^{\mathrm{T}}(b_2,\dots,b_n)$. Soit alors

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

On a $\det(M_1) = \det(M_1') = 1$ et $M_1^{-1\mathrm{T}}X = {}^{\mathrm{T}}(a_1,d,0,\dots,0)$. On est ramenés au cas $n = 2$: comme $\mathsf{pgcd}(a_1,d) = A$, il existe $M_2' \in \mathsf{M}_2(A)$ inversible avec $M_2^{-1\mathrm{T}}(a_1,d) = {}^{\mathrm{T}}(1,0)$. Soit alors

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

où $\mathrm{I}_{n-2} \in \mathsf{M}_{n-2}(A)$ désigne la matrice identité. On a $\det(M_2) = \det(M_2') = 1$ et $M_2^{-1}M_1^{-1}X = {}^{\mathrm{T}}(1,0,\dots,0)$. Soit $M = M_1M_2$. On a $\det(M) = 1$ et $M^{-1}X = {}^{\mathrm{T}}(1,0,\dots,0)$, ce qu'on voulait. □

Remarque 1.5.3. Cette preuve fournit une procédure effective pour construire la matrice si on sait traiter le cas $n = 2$ (par exemple pour $A = \mathbf{Z}$ ou, plus généralement, A un anneau euclidien).

Définition 1.5.4. Si $n, m \in \mathbf{N}_{>0}$, on fait agir $\mathsf{SL}_n(A) \times \mathsf{SL}_m(A)$ sur le A-module $\mathsf{M}_{n\times m}(A)$ par

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

Deux matrices $M_1, M_2 \in \mathsf{M}_{n\times m}(A)$ sont dites **équivalentes** si elles sont dans la même orbite pour cette action. On écrit alors $M_1 \sim M_2$ (cela définit une relation d'équivalence). Remarquons qu'on peut aussi faire agir $\mathsf{GL}_n(A) \times \mathsf{GL}_m(A)$ de la même façon.

Remarque 1.5.5. Lorsque $n = m$, on prendra garde à ne pas confondre cette notion avec celle, plus fine, de matrices **semblables** : si $M_1, M_2 \in \mathsf{M}_n(A)$, on dit que M_1 et M_2 sont semblables s'il existe $P \in \mathsf{GL}_n(A)$ tel que $M_2 = P^{-1}M_1P$.

Définition 1.5.6. Un matrice **réduite** est une matrice de la forme

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

avec $r \in \{0, \dots, \min\{m,n\}\}$ et $\alpha_1, \dots, \alpha_r \in A\backslash\{0\}$ tels que $\alpha_i | \alpha_{i+1}$ pour tout $i \in \{0, \dots r-1\}$.

Théorème 1.5.7. Tout matrice $M \in \mathsf{M}_{n\times m}(A)$ est équivalente à une matrice réduite.

Démonstration. On peut supposer $M \neq 0$. On procède par récurrence sur $d = \min\{m,n\}$.

Supposons $d = 1$. Quitte à transposer, on peut supposer $m = 1$, de sorte que M est un vecteur colonne. Si $n = 1$, il n'y a rien à faire : supposons $n \geqslant 2$. Notons α_1 le pgcd des coefficients de M : on a $M = \alpha_1 X$ où X est un vecteur colonne dont les composantes engendrent l'idéal unité. D'après la proposition 1.5.2, il existe une matrice $P \in \mathsf{SL}_n(A)$ dont la première colonne est égale à X. On a alors $P^{-1}X = {}^{\mathrm{T}}(1, 0, \dots, 0)$ et donc $P^{-1}M = {}^{\mathrm{T}}(\alpha_1, 0, \dots, 0)$.

Supposons désormais $d > 1$. Rappelons que $M \neq 0$. Soit $\delta = \min\{\ell(M'),\ M' \sim M\} \in \mathbf{N}$. Quitte à remplacer M par une matrice équivalente convenable, on peut supposer que $\ell(M) = \delta$. Il existe $i_0 \in \{1, \dots, n\}$ et $j_0 \in \{1, \dots, m\}$ tels que $\ell(m_{i_0,j_0}) = \delta$. Notons $\tau_{1,i_0} \in \mathfrak{S}_n$ (resp. $\tau_{1,j_0} \in \mathfrak{S}_m$) la transposition de $\{1, \dots, n\}$ (resp. $\{1, \dots, m\}$) échangeant 1 et i_0 (resp. j_0), et posons $M' = \widetilde{P}_{\tau_{1,i_0}}^{-1} M \widetilde{P}_{\tau_{1,j_0}} \in \mathsf{M}_{n\times m}(A)$ (où $\widetilde{P}_{\tau_{1,i_0}} \in \mathsf{SL}_n(A)$ et $\widetilde{P}_{\tau_{1,j_0}} \in \mathsf{SL}_m(A)$ sont les matrices de permutation modifiées, *cf* définition 1.5.1 (2)). On a $M' \sim M$ et $m'_{1,1} = m_{i_0,j_0}$: quitte à remplacer M par M', on peut supposer que $\ell(m_{1,1}) = \delta$. Posons $\alpha_1 := m_{1,1}$.

• Commençons par montrer que α_1 divise les coefficients de la première ligne et de la première colonne. Quitte à transposer, il suffit de traiter le cas de la première colonne. Raisonnons par l'absurde : supposons qu'il existe $i \in \{2, \dots, n\}$ tel que $\alpha_1 \nmid m_{i,1}$. Quitte à permuter la deuxième et la i-ème ligne, on peut supposer $i = 2$. Soit $\widetilde{\alpha}_1 = \mathsf{pgcd}(\alpha_1, m_{2,1})$. Comme $\widetilde{\alpha}_1$ divise strictement α_1, on a $\ell(\widetilde{\alpha}_1) < \delta$. Par ailleurs, il existe $a, b \in A$ tels que $\widetilde{\alpha}_1 = am_{1,1} + bm_{2,1}$. Posons alors

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

On a $\det(P) = 1$ et le coefficient d'indice $(1,1)$ de $M' = PM$ est $\widetilde{\alpha}_1$. On a donc $M' \sim M$ et $\ell(M') \leqslant \ell(\widetilde{\alpha}_1) < \delta$, ce qui contredit la définition de δ.

• Quitte à multiplier M à gauche par la matrice

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

et à droite par la matrice

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

on peut supposer que $m_{i,1} = 0$ pour $\in \{2, \dots, n\}$ et $m_{1,j} = 0$ pour $j \in \{2, \dots, m\}$. En effet, cela donne une matrice équivalente, et de même longueur (puisqu'on a pas changé le coefficient d'indice $(1,1)$).

• La matrice M est donc de la forme

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

avec $M_1 \in \mathsf{M}_{(n-1)\times(m-1)}(A)$. On applique l'hypothèse de récurrence à M_1 : il existe $P_1 \in \mathsf{SL}_{n-1}(A)$, $Q \in \mathsf{SL}_{m-1}(A)$, $r \in \mathbf{N}$, des éléments $\alpha_2, \dots, \alpha_r \in A\backslash\{0\}$ tels que $\alpha_i | \alpha_{i+1}$ pour tout $i \in \{2, \dots, r-1\}$ et

$$P_1^{-1} M_1 Q_1 = \begin{pmatrix} \alpha_2 & & \\ & \ddots & \\ & & \alpha_r \\ & & \end{pmatrix}$$

Quitte à multiplier M par $\begin{pmatrix} 1 & \\ & P_1^{-1} \end{pmatrix} \in \mathsf{SL}_n(A)$ à gauche et par $\begin{pmatrix} 1 & \\ & Q_1 \end{pmatrix} \in \mathsf{SL}_m(A)$ à droite, on peut supposer que

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

Reste à voir que $\alpha_1 \mid \alpha_2$, et on aura fini. Supposons le contraire. Soit $\alpha_1' = \mathsf{pgcd}(\alpha_1, \alpha_2)$. Comme $\alpha_1 \nmid \alpha_2$, on a $\ell(\alpha_1') < \ell(\alpha_1) = \delta$. Il existe $a, b \in A$ tels que $a\alpha_1 + b\alpha_2 = \alpha_1'$. L'égalité

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

montre qu'il existe $M' = (m_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}} \in \mathsf{M}_{n\times m}(A)$ équivalente à M et telle que $m_{2,1}' = \alpha_1'$. On a alors $\ell(M') \leqslant \ell(\alpha_1') < \delta$, ce qui contredit la définition de δ. On a fini. □

Remarque 1.5.8. Dans le cas où A est *euclidien*, il est possible de rendre cet énoncé constructif, à l'aide d'opérations élémentaires.

Théorème 1.5.9. (Théorème de la base adaptée). Soit M un sous-A-module d'un A-module L libre de rang n fini. Alors M est libre, et il existe une base $(e_1, \dots, e_n)$ de L, un entier $r \leqslant n$ et $\alpha_1, \dots, \alpha_r \in A\backslash\{0\}$ tels que

$$\begin{cases} \alpha_i | \alpha_{i+1} & \text{pour tout } i \in \{0, \dots r-1\} \\ (\alpha_1 e_1, \dots, \alpha_r e_r) & \text{est une base de } M. \end{cases}$$

Démonstration. Comme A est principal, il est nœthérien. Comme L est libre de rang fini, le A-module L est nœthérien (corollaire 1.1.6) : son sous-A-module M est donc lui aussi de type fini. Choisissons $x_1, \dots, x_m \in M$ une famille génératrice. On dispose donc d'une application A-linéaire

$$f \colon A^m \to L$$
$$(a_1, \dots, a_m) \mapsto \sum_{j=1}^{m} a_j x_j$$

dont l'image n'est autre que M. Après le choix d'une base $\mathfrak{B}$ de L, cette application est donnée par une matrice $n \times m$ (dont la j-ième colonne consiste en les coordonnées de x_j dans la base $\mathfrak{B}$). D'après le théorème 1.5.7, cette dernière est équivalente à une matrice réduite : quitte à effectuer un changement de base de A^m et de L, elle s'écrit

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

avec $r \in \{0, \dots, \min\{m, n\}\}$ et $\alpha_1, \dots, \alpha_r \in A\backslash\{0\}$ tels que $\alpha_i | \alpha_{i+1}$ pour tout $i \in \{0, \dots r-1\}$. Si on note $(e_1, \dots, e_n)$ la nouvelle base de L, l'image de f est donc le sous-A-module libre engendré par $(\alpha_1 e_1, \dots, \alpha_r e_r)$. □

Remarque 1.5.10. Le résultat qui précède est faux lorsque A n'est pas principal. Par exemple $\mathbf{Z}/2\,\mathbf{Z}$ est un sous-$\mathbf{Z}/4\,\mathbf{Z}$-module non libre de $\mathbf{Z}/4\,\mathbf{Z}$. De même, le sous-$\mathbf{Z} \times \mathbf{Z}$-module $\mathbf{Z} \times \{0\}$ de $\mathbf{Z} \times \mathbf{Z}$ n'est pas libre.

Théorème 1.5.11. (Théorème des diviseurs élémentaires). Soit M un A-module de type fini. Alors il existe des entiers $d, r \in \mathbf{N}$ et $a_1, \dots, a_d \in A\backslash\big(\{0\} \cup A^\times\big)$ tels que

$$\begin{cases} a_i | a_{i+1} \quad \text{pour tout } i \in \{0, \dots d-1\} \\ M \simeq (A/a_1A) \times \cdots \times (A/a_dA) \times A^r \end{cases}$$

En outre, les entiers d, r ainsi que les idéaux $a_1A, \dots, a_rA$ sont uniques. L'entier r s'appelle le **rang** de M et si $r = 0$, les éléments $(a_1, \dots, a_d)$ les **diviseurs élémentaires** de M.

Démonstration. Commençons par montrer l'existence. Comme M est de type fini, choisissons une famile génératrice $m_1, \dots, m_n$: on dispose d'une application surjective

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

Comme A^n est libre, il admet une base $(e_1, \dots, e_n)$ telle que

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

avec $s \in \{1, \dots, n\}$ et $\alpha_1, \dots, \alpha_s \in A\backslash\{0\}$ tels que $\alpha_i | \alpha_{i+1}$ pour tout $i \in \{0, \dots s-1\}$. En passant au quotient, f induit un isomorphisme A-linéaire

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

Soit $t = \max\big(i \in \{1, \dots, s\},\ \alpha_i \in A^\times\big)$ (on a $t = 0$ si $\alpha_1 \notin A^\times$). Posons $d = s - t$, $r = n - s$ et $a_i = \alpha_{t+i}$ pour $i \in \{1, \dots, d\}$. On a $a_1, \dots, a_d \in A\backslash\big(\{0\} \cup A^\times\big)$ et $a_i | a_{i+1}$ pour tout $i \in \{0, \dots d-1\}$. En outre, comme

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

on a bien

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

Montrons maintenant l'unicité. On a déjà $M_{\mathsf{tors}} = (A/a_1A) \times \cdots \times (A/a_dA)$ et donc $M/M_{\mathsf{tors}} \simeq A^r$. L'entier r ne dépend donc que de M (c'est la dimension du K-espace vectoriel $K \otimes_A M$ où $K = \mathsf{Frac}(A)$).

Il suffit donc de traiter le cas où M est de torsion. On a $M \simeq \prod_{i=1}^{d}(A/a_iA)$ avec $a_1 | a_2 | \cdots | a_d$ dans $A\backslash\{0\}$. Notons $\mathscr{P}$ l'ensemble des éléments irréductibles de A. Si $p \in \mathscr{P}$, l'idéal pA est premier non nul donc maximal (*cf* proposition 1.2.16) : le A-module M/pM est un A/pA-espace vectoriel de dimension finie $d_p(M)$ (on a $d_p(M) = \#\{i \in \{1, \dots, d\},\ p | a_i\}$). On en déduit déjà que $d = \max_{p \in \mathscr{P}} d_p(M)$ ne dépend que de M. Par ailleurs, pour tout $n \in \mathbf{N}$, on a

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

Il en résulte que pour tout $n \in \mathbf{N}_{>0}$, l'entier

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

ne dépend que de M et de p. Comme on a $v_p(a_1) \leqslant v_p(a_2) \leqslant \cdots \leqslant v_p(a_d)$, cela implique que pour tout $p \in \mathscr{P}$ et tout $i \in \{1, \dots, d\}$, l'entier $v_p(a_i)$ ne dépend que de M et de p. Cela signifie que les idéaux a_iA ne dépendent que de M. □

Corollaire 1.5.12. (1) Si M est un A-module de type fini, il est isomorphe (*non canoniquement*) à $M_{\mathsf{tors}} \oplus (M/M_{\mathsf{tors}})$.
(2) Un A-module de type fini sans torsion est libre.

Corollaire 1.5.13. Dans les théorèmes 1.5.7 et 1.5.9, les idéaux $\alpha_1A \supseteq \cdots \supseteq \alpha_rA$ sont uniques.

Démonstration. Si $M = \bigoplus_{i=1}^{r} A\alpha_i e_i \subseteq \bigoplus_{i=1}^{n} Ae_i = L$, on a $L/M \simeq \bigoplus_{i=1}^{r}(A/\alpha_i A)e_i \times A^{n-r}$. Soit s le nombre d'indices $i \in \{1,\dots,r\}$ tels que $\alpha_i \in A^\times$. On a $L/M \simeq (A/\alpha_{s+1}A) \times \cdots \times (A/\alpha_r A) \times A^{n-r}$. D'après le théorème 1.5.11, les entiers $r-s$ et $n-r$ et donc s ne dépendent que de L et M, ainsi que les idéaux $\alpha_{s+1}A \supseteq \cdots \supseteq \alpha_r A$, ce qui implique l'unicité pour le théorème 1.5.9, et donc aussi pour le théorème 1.5.7. □

1.6. **Sous-groupes discrets de $\mathbf{R}^n$.**

Définition 1.6.1. Soit $n \in \mathbf{N}$. Un **sous-groupe discret** de $\mathbf{R}^n$ est un sous-groupe $\Lambda \subset \mathbf{R}^n$ tel que pour toute partie compacte B de $\mathbf{R}^n$, l'ensemble $\Lambda \cap B$ est fini.

Exemple 1.6.2. Le sous-groupe $\mathbf{Z}^n \subset \mathbf{R}^n$ est discret.

Proposition 1.6.3. Soit $\Lambda \subset \mathbf{R}^n$ un sous-groupe discret. Alors il existe une base $(e_1,\dots,e_n)$ de $\mathbf{R}^n$ et $r \in \{0,\dots,n\}$ tel que $\Lambda = \mathbf{Z}\,e_1 \oplus \cdots \oplus \mathbf{Z}\,e_r$. En particulier, Λ est libre de rang $r \leqslant n$.

Démonstration. Comme Λ est un sous-groupe de $\mathbf{R}^n$ qui est abélien sans torsion, c'est un $\mathbf{Z}$-module sans torsion. Soit $r \leqslant n$ maximal tel qu'il existe une partie $\{\lambda_1,\dots,\lambda_r\} \subset \Lambda$ libre dans $\mathbf{R}^n$. Posons

$$B = \Big\{ \sum_{i=1}^{r} x_i\lambda_i,\ (\forall i \in \{1,\dots,r\})\, 0 \leqslant x_i \leqslant 1 \Big\}$$

c'est une partie compacte de $\mathbf{R}^n$ (homéomorphe à $[0,1]^r$). L'intersection $\Lambda \cap B$ est donc finie vu que Λ est discret. Soit $\lambda \in \Lambda$. Par maximalité de r, la partie $\{\lambda,\lambda_1,\dots,\lambda_r\}$ est liée : il existe $y_1,\dots,y_r \in \mathbf{R}$ tels que $\lambda = \sum_{i=1}^{r} y_i\lambda_i$. On a alors $\lambda - \sum_{i=1}^{r} \lfloor y_i \rfloor \lambda_i \in \Lambda \cap B$. Cela implique que le $\mathbf{Z}$-module Λ est engendré par $\{\lambda_1,\dots,\lambda_r\} \cup \big(\Lambda \cap B\big)$: il est donc de type fini. Comme il est sans torsion, il est libre de rang fini (théorème 1.5.11).

D'après ce qui précède, si $\lambda \in \Lambda$, il existe $n_1,\dots,n_r \in \mathbf{Z}$ tels que $\lambda - \sum_{i=1}^{r} n_i\lambda_i \in \Lambda \cap B$. Comme $\Lambda \cap B$ est fini, cela implique que le groupe $\Lambda/(\mathbf{Z}\,\lambda_1 \oplus \cdots \mathbf{Z}\,\lambda_r)$ est fini, et donc que Λ est de rang r. Soit $(e_1,\dots,e_r)$ une base de Λ. C'est une famille libre dans $\mathbf{R}^n$: il suffit alors de la compléter en une base $(e_1,\dots,e_n)$ de $\mathbf{R}^n$. □

Définition 1.6.4. Un **réseau** de $\mathbf{R}^n$ est un sous-groupe discret de rang maximal dans $\mathbf{R}^n$. D'après la proposition 1.6.3, c'est un sous-groupe de la forme $\mathbf{Z}\,e_1 \oplus \cdots \oplus \mathbf{Z}\,e_n$ où $(e_1,\dots,e_n)$ est une base de $\mathbf{R}^n$.

Dans tout ce qui suit, μ désigne la mesure de Lebesgue.

Définition 1.6.5. Soient Λ un réseau de $\mathbf{R}^n$, et $\mathbf{e} = (e_1,\dots,e_n)$ une base de Λ.

(1) L'ensemble

$$D_{\mathbf{e}} = \Big\{ \sum_{i=1}^{r} x_i e_i,\ (\forall i \in \{1,\dots,n\})\, 0 \leqslant x_i < 1 \Big\}$$

s'appelle le **domaine fondamental** associé à $\mathbf{e}$.

(2) Le **volume** de Λ est le réel $\mu(\Lambda) = \mu(D_{\mathbf{e}})$.

Remarque 1.6.6. (1) Pour tout $x \in \mathbf{R}^n$, il existe un unique $\lambda \in \Lambda$ tel que $x - \lambda \in D_{\mathbf{e}}$. Si $x = \sum_{i=1}^{n} x_i e_i$, on a $\lambda = \sum_{i=1}^{n} \lfloor x_i \rfloor e_i$.

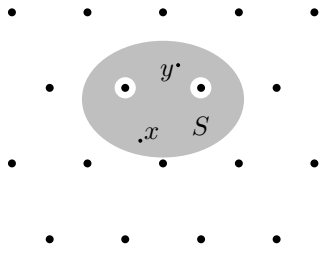
(2) Comme la notation et la terminologie le suggèrent, le nombre $\mu(\Lambda)$ ne dépend pas du choix de la base $\mathbf{e}$. En effet, si $\mathbf{e}'$ est une autre base de Λ, et $M \in \mathsf{GL}_n(\mathbf{R})$ la matrice de passage entre $\mathbf{e}$ et $\mathbf{e}'$, alors M est un automorphisme de Λ, de sorte que $M \in \mathsf{GL}_n(\mathbf{Z})$, en particulier, on a $\det(M) \in \{\pm 1\}$. On a donc $\mu(D_{\mathbf{e}'}) = |\det(M)|\,\mu(D_{\mathbf{e}}) = \mu(D_{\mathbf{e}})$.

Théorème 1.6.7. Soient $\Lambda \subset \mathbf{R}^n$ un réseau et $S \subseteq \mathbf{R}^n$ mesurable et telle que $\mu(S) > \mu(\Lambda)$. Il existe $x, y \in S$ tels que $x \neq y$ et $x - y \in \Lambda$.

Démonstration. Soit $\mathbf{e}$ une base de Λ. On a $\mathbf{R}^n = \coprod_{\lambda\in\Lambda} (\lambda + D_{\mathbf{e}})$ (l'union étant disjointe), de sorte que $S = \coprod_{\lambda\in\Lambda} S \cap \big(\lambda + D_{\mathbf{e}}\big)$. Comme l'union est disjointe, on a donc $\mu(S) = \sum_{\lambda\in\Lambda} \mu\big(S \cap \big(\lambda + D_{\mathbf{e}}\big)\big)$. Pour $\lambda \in \Lambda$, on a $\mu\big(S \cap \big(\lambda + D_{\mathbf{e}}\big)\big) = \mu\big((-\lambda + S) \cap D_{\mathbf{e}}\big)$ en translatant par $-\lambda$. Si les ensembles $\big\{(-\lambda + S) \cap D_{\mathbf{e}}\big\}_{\lambda\in\Lambda}$ étaient deux-à-deux disjoints, on aurait donc

$$\mu(S) = \sum_{\lambda\in\Lambda} \mu\big((-\lambda + S) \cap D_{\mathbf{e}}\big) \leqslant \mu(D_{\mathbf{e}})$$

ce qui contredit l'hypothèse $\mu(S) > \mu(\Lambda)$. Il existe donc $\lambda, \lambda' \in \Lambda$ tels que $\lambda \neq \lambda'$ et $\big((-\lambda + S) \cap D_{\mathbf{e}}\big) \cap \big((-\lambda' + S) \cap D_{\mathbf{e}}\big) \neq \varnothing$, et donc $(\lambda' - \lambda + S) \cap S \neq \varnothing$. Il suffit de prendre $x \in (\lambda' - \lambda + S) \cap S$ et $y = x + \lambda - \lambda'$. □



Corollaire 1.6.8. Soient $\Lambda \subset \mathbf{R}^n$ un réseau et $S \subseteq \mathbf{R}^n$ mesurable convexe et symétrique par rapport à l'origine. Supposons en outre que $\mu(S) > 2^n\mu(\Lambda)$ ou bien $\mu(S) \geqslant 2^n\mu(\Lambda)$ et S compact. Alors

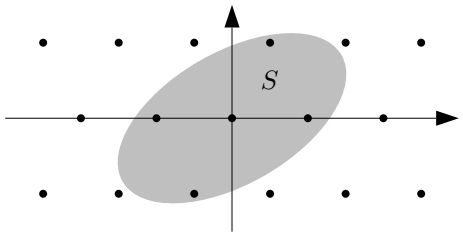
$$S \cap (\Lambda\backslash\{0\}) \neq \varnothing$$

Démonstration. Supposons $\mu(S) > 2^n\mu(\Lambda)$. D'après le théorème 1.6.7 appliqué à $\frac{1}{2}S$, il existe $x, y \in \frac{1}{2}S$ tels que $x \neq y$ et $x - y \in \Lambda$. On a $2x, 2y \in S$. Comme S est symétrique par rapport à l'origine, on a $-2y \in S$, et comme il est convexe, on a $x - y = \frac{1}{2}(2x - 2y) \in S \cap (\Lambda\backslash\{0\})$.

Supposons désormais $\mu(S) \geqslant 2^n\mu(\Lambda)$ et S compact. Pour $i \in \mathbf{N}_{>0}$, posons

$$T_i = \Big(1 + \frac{1}{i}\Big)S \cap (\Lambda\backslash\{0\})$$

L'ensemble $\big(1 + \frac{1}{i}\big)S$ est mesurable, convexe et symétrique par rapport à l'origine. D'après ce qui précède, comme $\mu\big(\big(1 + \frac{1}{i}\big)S\big) = \big(1 + \frac{1}{i}\big)^n\mu(S) > 2^n\mu(\Lambda)$, on a $T_i \neq \varnothing$. Comme S est compact, il en est de même de $\big(1 + \frac{1}{i}\big)S$: l'ensemble T_i est fini donc fermé pour tout $i \in \mathbf{N}_{>0}$. La suite $(T_i)_{i\in\mathbf{N}_{>0}}$ est décroissante dans le compact $2S$: si $\bigcap_{i=1}^{\infty} T_i = \varnothing$, il existe $i \in \mathbf{N}_{>0}$ tel que $T_i = \varnothing$, ce qui n'est pas. On a donc $S \cap (\Lambda\backslash\{0\}) = \bigcap_{i=1}^{\infty} T_i \neq \varnothing$. □



2. Anneaux d'entiers

2.1. **Extensions entières.** Dans tout ce qui suit, A est un anneau et B une A-algèbre (*cf* définition 1.1.8).

Définition 2.1.1. (1) Un élément $b \in B$ est dit **entier** sur A s'il existe $P \in A[X]$ *unitaire* tel que $P(b) = 0$. L'égalité $P(b) = 0$ s'appelle alors une **relation de dépendance intégrale**.
(2) On dit que B est **entière** sur A si tous ses éléments sont entiers sur A.

Exemples 2.1.2. (1) L'élément $\sqrt{2} \in \mathbf{C}$ (resp. $\alpha = \frac{1+\sqrt{5}}{2} \in \mathbf{C}$) est entier sur $\mathbf{Z}$, une relation de dépendance intégrale étant donnée par $(\sqrt{2})^2 - 2 = 0$ (resp. $\alpha^2 - \alpha - 1 = 0$).
(2) On verra plus tard que $\frac{\sqrt{2}}{2} \in \mathbf{C}$ n'est pas entier sur $\mathbf{Z}$.
(3) Si A et B sont des corps, alors $b \in B$ est entier sur A si et seulement si b est algébrique sur A, et B est entière (resp. finie) sur A si et seulement si elle est algébrique (resp. de degré fini).

Proposition 2.1.3. Supposons B intègre [a] et soit $b \in B$. Les conditions suivantes sont équivalentes :
(*i*) b est entier sur A ;
(*ii*) la A-algèbre $A[b]$ est finie ;
(*iii*) il existe un sous-A-module $B' \subseteq B$ de type fini, non nul et stable par la multiplication par b (*i.e.* tel que $bB' \subseteq B'$).

a. Cette hypothèse est inutile si dans (iii), on requiert $1 \in B'$. En particulier, elle est n'est pas nécessaire pour l'équivalence $(i) \Leftrightarrow (ii)$.

Démonstration. $(i) \Rightarrow (ii)$ Soient $P \in A[X]$ unitaire tel que $P(b) = 0$. Si $\deg(P) = n$, le A-module $A[b]$ est engendré par $\{1, b, \dots, b^{n-1}\}$ (division euclidienne), donc de type fini.
$(ii) \Rightarrow (iii)$ On prend $M = A[b]$.
$(iii) \Rightarrow (i)$ Soit $(\beta_1, \dots, \beta_n)$ une famille génératrice du A-module B'. Comme $b\beta_i \in B'$, il existe $M = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(A)$ telle que $b\beta_i = \sum_{j=1}^{n} a_{i,j}\beta_j$ pour tout $i \in \{1, \dots, n\}$. Posons $X = (\beta_i)_{1 \leqslant i \leqslant n} \in \mathsf{M}_{n \times 1}(B)$: on a $MX = bX$, *i.e.*

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

Posons $P(X) = \det(X\,\mathrm{I}_n - M)$. C'est un polynôme unitaire de degré n, à coefficients dans A. En multipliant l'égalité $(*)$ par la transposée de la comatrice de $b\,\mathrm{I}_n - M$, il vient $P(b)X = 0$: on a $P(b)B' = 0$, et donc $P(b) = 0$ (car B est intègre). Comme le polynôme $P(X) \in A[X]$ est unitaire, l'élément b est entier sur A. □

Lemme 2.1.4. Soient $b_1, \dots, b_n \in B$ tels que b_i soit entier sur $A[b_1, \dots, b_{i-1}]$ pour tout $i \in \{1, \dots, n\}$. Alors la A-algèbre $A[b_1, \dots, b_n]$ est finie.

Démonstration. On procède par récurrence sur n, le cas $n = 1$ résultant de la proposition 2.1.3. Soient $n > 1$ et $A' = A[b_1, \dots, b_{n-1}] \subseteq B$. Par hypothèse de récurrence, la A-algèbre A' est finie, et comme b_n est entier sur A', la A'-algèbre $A'[b_n]$ est finie. Il en résulte que la A-algèbre $A[b_1, \dots, b_n] = A'[b_n]$ est finie. □

Proposition 2.1.5. La A-algèbre B est finie si et seulement si elle est entière et de type fini.

Démonstration. Si B est finie sur A, elle est entière en vertu de la proposition 2.1.3 (l'implication $(iii) \Rightarrow (i)$ avec $B' = B$). Par ailleurs, si $\{b_1, \dots, b_n\}$ est une partie génératrice du A-module B, le morphisme de A-algèbres $A[X_1, \dots, X_n] \to B$ qui envoie X_i sur b_i est surjectif, de sorte que B est de type fini sur A.

Réciproquement, supposons B entière et de type fini sur A. On peut écrire $B = A[b_1, \dots, b_n]$, et comme $b_1, \dots, b_n$ sont entiers sur A, le A-module B est de type fini d'après le lemme 2.1.4. □

Proposition 2.1.6. Si B est une A-algèbre entière et C une B-algèbre entière, alors C est une A-algèbre entière.

Démonstration. Soient $c \in C$ et $P(c) = 0$, avec $P(X) = X^n + b_1X^{n-1} + \cdots + b_n \in B[X]$, une relation de dépendance intégrale. Comme B est entière sur A, les éléments $b_1, \ldots, b_n$ sont entiers sur A : d'après le lemme 2.1.4, $B' = A[b_1, \ldots, b_n]$ est finie sur A. Comme $B'[c]$ est finie sur B, elle est finie sur A, ce qui implique que c est entier sur A (proposition 2.1.3, en notant que $1 \in B'[c]$). □

Corollaire 2.1.7. Soient $b, b' \in B$ entiers sur A. Alors $b - b'$ et bb' sont entiers sur A.

Démonstration. D'après le lemme 2.1.4, l'extension $A \subseteq A[b, b']$ est finie donc entière : comme $b - b', bb' \in A[b, b']$, ils sont entiers sur A. □

Remarque 2.1.8. Si B est une A-algèbre et $b \in B$ est inversible et entier sur A, l'inverse $b^{-1} \in B$ n'est pas entier sur A en général.

Définition 2.1.9. (1) D'après le corollaire 2.1.7, l'ensemble des éléments de B qui sont entiers sur A est une sous-A-algèbre de B. On l'appelle la **clôture intégrale** de A dans B.

(2) Supposons A intègre et notons K son corps des fractions. La **clôture intégrale** de A est la clôture intégrale de A dans K. On dit que A est **intégralement clos** s'il est égal à sa clôture intégrale, c'est-à-dire lorsque les seuls éléments de K entiers sur A sont les éléments de A.

Proposition 2.1.10. Tout anneau factoriel est intégralement clos. En particulier, tout anneau principal est intégralement clos.

Démonstration. Soient A un anneau factoriel, K son corps des fractions et $x \in K$ entier sur A. Écrivons $x = a/b$ avec $a \in A$ et $b \in A\backslash\{0\}$ premiers entre eux. Soit $x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n = 0$ une relation de dépendance intégrale (avec $\alpha_1, \ldots, \alpha_n \in A$). En la multipliant par b^n, on a

$$a^n + \alpha_1 a^{n-1} b + \cdots + \alpha_n b^n = 0$$

de sorte que b divise a^n. Comme a et b sont premiers entre eux, cela implique $b \in A^\times$, et donc $x = ab^{-1} \in A$. □

Exemple 2.1.11. Soient K un corps, t une indéterminée et $A = K[t^2, t^3] \subseteq B = K[t]$. Alors A et B ont même corps des fractions $K(t)$. Comme B est factoriel (car principal), il est intégralement clos d'après la proposition 2.1.10. L'élément t est entier sur A, mais $t \notin A$, de sorte que A n'est pas intégralement clos (et donc non factoriel d'après la proposition 2.1.10).

Proposition 2.1.12. Soient A un anneau intègre, K son corps des fractions et L/K une extension algébrique de corps. Notons B la clôture intégrale de A dans L. Alors pour tout $x \in L$, il existe $a \in A\backslash\{0\}$ tel que $ax \in B$. En particulier, on a [a] $L = \mathsf{Frac}(B)$ et B est intégralement clos.

a. Comme le montre la preuve, on a en fait $L = (A\backslash\{0\})^{-1}B$.

Démonstration. Soient $x \in L$ et $X^d + \alpha_1 X^{d-1} + \cdots + \alpha_d \in K[X]$ son polynôme minimal. Il existe $a \in A\backslash\{0\}$ tel que $a\alpha_i \in A$ pour tout $i \in \{1, \ldots, d\}$. Le polynôme minimal de ax est alors $X^d + a\alpha_1 X^{d-1} + \cdots + a^d\alpha_n \in A[X]$, donc $ax \in B$. Cela implique que $\mathsf{Frac}(B) = L$. Si $x \in L$ est entier sur B, alors il est entier sur A (proposition 2.1.6), de sorte que $x \in B$, et B est intégralement clos. □

Proposition 2.1.13. Sous les hypothèses de la proposition 2.1.12, soit $S \subset A$ une partie multiplicative. Alors la clôture intégrale de $S^{-1}A \subset K$ dans L est $S^{-1}B$ (« la clôture intégrale commute aux localisations »).

Démonstration. Soient $b \in B$ et $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ une relation de dépendance intégrale sur A. Si $s \in S$ et $x = \frac{b}{s} \in S^{-1}B$, on a $x^n + \frac{a_1}{s}x^{n-1} + \cdots + \frac{a_n}{s^n} = 0$, ce qui montre que x est entier sur $S^{-1}A$. Réciproquement, soient $x \in L$ entier sur $S^{-1}A$ et $x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n = 0$ une relation de dépendance intégrale sur $S^{-1}A$. Il existe $s \in S$ tel que $a_i := s\alpha_i \in A$ pour tout $i \in \{1, \ldots, n\}$ (on prend pour s un dénominateur commun aux α_i). Posons $b = sx \in L$: on a $b^n + a_1 b^{n-1} + sa_2 b^{n-2} + \cdots + s^{n-2}a_{n-1}b + s^{n-1}a_n = 0$, ce qui montre que b est entier sur A. On a donc $b \in B$, et $x \in S^{-1}B$. □

Définition 2.1.14. Un **corps de nombres** est une extension finie de $\mathbf{Q}$ (généralement, on la voit comme un sous-corps de $\mathbf{C}$). Si K est un corps de nombres, l'**anneau des entiers** de K est la clôture intégrale de $\mathbf{Z}$ dans K. On la note $\mathcal{O}_K$. D'après la proposition précédente, c'est un anneau intégralement clos et $K = (\mathbf{Z}\backslash\{0\})^{-1}\mathcal{O}_K$.

Proposition 2.1.15. Soient A un anneau intègre et intégralement clos, $K = \mathsf{Frac}(A)$ et L/K une extension algébrique. Un élément de L est entier sur A si et seulement si son polynôme minimal est à coefficients dans A.

Démonstration. Soient $x \in L$ et $P \in K[X]$ son polynôme minimal. Si $P \in A[X]$, l'égalité $P(x) = 0$ est une relation de dépendance intégrale, et x est entier sur A. Réciproquement, supposons $x \in L$ entier sur A. Fixons $\overline{L}$ une clôture algébrique de L, et soient $x_1, \ldots, x_n \in \overline{L}$ les racines de P dans $\overline{L}$ (*i.e.* les conjugués de x, comptés avec multiplicités). Si $i \in \{1, \ldots, n\}$, il existe un K-isomorphisme de corps $f\colon K(x) \to K(x_i)$ qui envoie x sur x_i (théorème de prolongement des isomorphismes). Si $Q(x) = 0$ est une relation de dépendance intégrale (avec $Q \in A[X]$), on a $Q(x_i) = Q(f(x)) = f(Q(x)) = 0$, si bien que x_i est entier sur A pour tout $i \in \{1, \ldots, n\}$. D'après le corollaire 2.1.7, il en est donc de même des coefficients de P (qui sont, au signe près, des polynômes symétriques en $x_1, \ldots, x_n$). Comme ces coefficients appartiennent à K et A est intégralement clos dans K par hypothèse, on a $P \in A[X]$. □

Exemple 2.1.16. $\frac{\sqrt{2}}{2}$ n'est pas entier sur $\mathbf{Z}$ (son polynôme minimal sur $\mathbf{Q}$ est $X^2 - \frac{1}{2} \notin \mathbf{Z}[X]$).

Proposition 2.1.17. Soient $d \in \mathbf{Z}\backslash\{0, 1\}$ sans facteur carré et $K = \mathbf{Q}(\sqrt{d})$. Alors

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

Démonstration. Soit $x = \lambda + \mu\sqrt{d} \in K$ avec $\lambda, \mu \in \mathbf{Q}$. Les conjugués de x sont x et $y = \lambda - \mu\sqrt{d}$: son polynôme minimal est $P(X) = X^2 - 2\lambda X + \lambda^2 - d\mu^2$. Comme $\mathbf{Z}$ est factoriel, il est intégralement clos : d'après la proposition 2.1.15, x est entier sur $\mathbf{Z}$ si et seulement si $2\lambda \in \mathbf{Z}$ et $\lambda^2 - d\mu^2 \in \mathbf{Z}$. On a en particulier $(2\lambda)^2 - d(2\mu)^2 \in 4\,\mathbf{Z}$. Cela implique déjà $d(2\mu)^2 \in \mathbf{Z}$, et donc $2\mu \in \mathbf{Z}$ (parce que d est dans facteur carré). Si $2\mu \notin 2\,\mathbf{Z}$, alors 2μ a une image inversible dans $\mathbf{Z}/4\,\mathbf{Z}$, et d est un carré modulo 4. Ce n'est possible que si $d \equiv 0, 1 \mod 4\,\mathbf{Z}$. On n'a pas $d \in 4\,\mathbf{Z}$ (parce que d est sans facteur carré). Il en résulte que si $d \not\equiv 1 \mod 4\,\mathbf{Z}$, on a $2\mu \in 2\,\mathbf{Z}$, *i.e.* $\mu \in \mathbf{Z}$, et donc $\lambda^2 \in \mathbf{Z}$ *i.e.* $\lambda \in \mathbf{Z}$, ce qui implique que $\mathcal{O}_K \subseteq \mathbf{Z}[\sqrt{d}]$ dans ce cas. L'inclusion réciproque est évidente.

Supposons désormais que $d \equiv 1 \mod 4\,\mathbf{Z}$, et posons $\alpha = \frac{1+\sqrt{d}}{2}$. On a $\alpha^2 = \frac{1+d+2\sqrt{d}}{4} = \frac{d-1}{4} + \alpha$, de sorte que $\alpha \in \mathcal{O}_K$, donc $\mathbf{Z}[\alpha] \subseteq \mathcal{O}_K$. On a $x = \lambda - \mu + 2\mu\alpha$. Si $x \in \mathcal{O}_K$, on a vu que $2\mu \in \mathbf{Z}$, donc $\lambda - \mu = x - 2\mu\alpha \in \mathcal{O}_K$. Comme $\lambda - \mu \in \mathbf{Q}$ et $\mathbf{Z}$ est intégralement clos, cela implique $\lambda - \mu \in \mathbf{Z}$, et $x = \lambda - \mu + 2\mu\alpha \in \mathbf{Z} + \mathbf{Z}\,\alpha \subseteq \mathcal{O}_K$: on a $\mathcal{O}_K = \mathbf{Z}[\alpha]$. □

Exercice 2.1.18. Trouver un contre-exemple à l'énoncé du théorème 2.1.15 lorsque A n'est pas supposé intégralement clos [2].

Exemple 2.1.19. Soient A un anneau factoriel dans lequel 2 est inversible, $\alpha \in A$ sans facteur carré (*i.e.* non divisible par le carré d'un élément premier) et $B = A[\sqrt{\alpha}]$. Montrons que B est intégralement clos.

2. On prend $A = \mathbf{Z}[\sqrt{5}]$. On a $K = \mathbf{Q}(\sqrt{5}) \ni \alpha = \frac{1+\sqrt{5}}{2}$: le polynôme minimal de α sur K est $X - \alpha \notin A[X]$, mais α est entier sur A (on a $\alpha^2 - \alpha - 1 = 0$).

Notons K le corps des fractions de A : on a $\mathsf{Frac}(B) = K(\sqrt{\alpha})$. Si $\sqrt{\alpha} \in K$, alors $\sqrt{\alpha} \in A$ vu que A est intégralement clos en vertu de la proposition 2.1.10, si bien que $A[\sqrt{\alpha}] = A$ est intégralement clos. Supposons désormais que $\sqrt{\alpha} \notin K$: l'extension $K(\sqrt{\alpha})/K$ est de degré 2, et on a $K(\sqrt{\alpha}) = K \oplus K\sqrt{\alpha}$. Soit $x = \lambda + \mu\sqrt{\alpha} \in K(\sqrt{\alpha})$, avec $\lambda, \mu \in K$. Supposons x entier sur $A[\sqrt{\alpha}]$. Comme $A \subseteq A[\sqrt{\alpha}]$ est entière, l'élément x est entier sur A (proposition 2.1.6), de sorte que son polynôme minimal P sur K est à coefficients dans A (proposition 2.1.15). L'extension $K(\sqrt{\alpha})/K$ est galoisienne, son groupe de Galois étant engendré par le K-automorphisme σ défini par $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$: les conjugués de x sont donc x et $y = \sigma(x) = \lambda - \mu\sqrt{\alpha}$, d'où

$$P(X) = (X - x)(X - y) = X^2 - (x + y)X + xy = X^2 - 2\lambda X + \lambda^2 - \alpha\mu^2$$

si bien que x est entier sur A si et seulement si $2\lambda \in A$ et $\lambda^2 - \alpha\mu^2 \in A$. Comme $2 \in A^\times$, cela équivaut à $\lambda \in A$ et $\lambda^2 - \alpha\mu^2 \in A$, soit $\alpha\mu^2 \in A$. Si $p \in A$ est irréductible, on a donc $v_p(\alpha) + 2v_p(\mu) \geqslant 0$. Comme α est sans facteur carré, on a $v_p(\alpha) \in \{0, 1\}$, donc $v_p(\mu) \geqslant -1/2$. Comme $v_p(\mu) \in \mathbf{N}$, on a $v_p(\mu) \geqslant 0$ pour tout p irréductible, et donc $\mu \in A$, soit $x = \lambda + \mu\sqrt{\alpha} \in B$.

Proposition 2.1.20. Soient $A \to B$ un morphisme *injectif* avec B intègre [a] et entier sur A. Alors A est un corps si et seulement si B est un corps.

a. Ce qui implique que A est intègre.

Démonstration. Supposons que A soit un corps, et soit $b \in B\backslash\{0\}$. Comme B est entière sur A, on a une relation de dépendance intégrale $b^n + a_1 b^{n-1} + \cdots + a_n = 0$, avec $a_1, \ldots, a_n \in A$. Comme B est supposé intègre, on peut supposer $a_n \neq 0$ (sinon on divise l'égalité par b). On a alors $bc = 1$ avec

$$c = -a_n^{-1}(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) \in B$$

si bien que b est inversible dans B, et B est un corps.

Réciproquement, supposons que B soit un corps. Si $a \in A\backslash\{0\}$, alors a a une image non nulle donc inversible dans B : on note $a^{-1} \in B$ son inverse. Comme B est entière sur A, on dispose d'une relation de dépendance intégrale $(a^{-1})^n + \alpha_1(a^{-1})^{n-1} + \cdots + \alpha_n = 0$ avec $\alpha_1, \ldots, \alpha_n \in A$ et

$$a^{-1} = -\alpha_1 - \alpha_2 a - \cdots - \alpha_n a^{n-1} \in A$$

de sorte que A est un corps. □

Proposition 2.1.21. Soit B une A-algèbre entière. Si $\mathfrak{M} \subset B$ est un idéal maximal, alors $\mathfrak{M} \cap A$ est un idéal maximal de A. Réciproquement, si $\mathfrak{m} \subset A$ est un idéal maximal, il existe un idéal premier $\mathfrak{M} \subset B$ tel que $\mathfrak{m} = \mathfrak{M} \cap A$, et les tels $\mathfrak{M}$ sont maximaux dans B.

Démonstration. Supposons $\mathfrak{M} \subset B$ maximal, et posons $\mathfrak{m} = \mathfrak{M} \cap A$. On dispose du morphisme injectif $A/\mathfrak{m} \to B/\mathfrak{M}$. La $A/\mathfrak{m}$-algèbre $B/\mathfrak{M}$ est entière parce que B l'est sur A (si $b \in B$ et $P(b) = 0$ est une relation de dépendance intégrale, avec $P \in A[X]$, on a $\overline{P}(\overline{b}) = 0$ où $\overline{P} \in (A/\mathfrak{m})[X]$ et $\overline{b} \in B/\mathfrak{M}$ désignent la réduction de P modulo $\mathfrak{m}A[X]$ et la réduction de b modulo $\mathfrak{M}$ respectivement). Comme $B/\mathfrak{M}$ est un corps, il en est de même de $A/\mathfrak{m}$ en vertu de la proposition 2.1.20, et $\mathfrak{m}$ est maximal dans A.

Soit $\mathfrak{m} \subset A$ maximal. Commençons par montrer que $\mathfrak{m}B \neq B$. Supposons au contraire que $\mathfrak{m}B = B$, *i.e.* $1 \in \mathfrak{m}B$: on peut écrire

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

avec $\alpha_1, \ldots, \alpha_n \in \mathfrak{m}$ et $b_1, \ldots, b_n \in B$. Comme B est entière sur A, il en est de même de $B' = A[b_1, \ldots, b_n]$. Comme B' est de type fini sur A, la A-algèbre B' est en fait finie (*cf* proposition 2.1.5) : on peut écrire $B' = A\beta_1 + \cdots + A\beta_n$. Par ailleurs, l'égalité $(*)$ implique que $\mathfrak{m}B' = B'$: pour tout $i \in \{1, \ldots, n\}$, il existe $\lambda_{i,1}, \ldots, \lambda_{i,n} \in \mathfrak{m}$ tels que

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

Si $M = (\lambda_{i,j})_{1\leqslant i,j\leqslant n} \in \mathsf{M}_n(A)$ et $X = (\beta_i)_{1\leqslant i\leqslant n} \in \mathsf{M}_{n\times 1}(B')$, on a $MX = X$, et donc $(\mathrm{I}_n - M)X = 0$: en multipliant par la transposée de la comatrice de $\mathrm{I}_n - M$, il vient $\det(\mathrm{I}_n - M)X = 0$, *i.e.* $\det(\mathrm{I}_n - M)B' = 0$, et donc $\det(\mathrm{I}_n - M) = 0$ vu que $1 \in B'$. Mais comme $\det(\mathrm{I}_n - M) \equiv 1 \mod \mathfrak{m}$, on a $1 \in \mathfrak{m}$ ce qui est absurde : on a nécessairement $\mathfrak{m}B \neq B$.

Comme l'idéal $\mathfrak{m}B \subset B$ est propre, il existe $\mathfrak{M} \subset B$ maximal tel que $\mathfrak{m}B \subseteq \mathfrak{M}$ (théorème 1.0.1). On a bien sûr $\mathfrak{m} \subseteq \mathfrak{M} \cap A$, et donc $\mathfrak{m} = \mathfrak{M} \cap A$ vu que $\mathfrak{m}$ est maximal dans A.

Si $\mathfrak{P} \subset B$ est premier et tel que $\mathfrak{m} = \mathfrak{P} \cap A$, on dispose du morphisme injectif $A/\mathfrak{m} \to B/\mathfrak{P}$. Il fait de $B/\mathfrak{P}$ une $A/\mathfrak{m}$-algèbre entière vu que B l'est sur A, et $B/\mathfrak{P}$ est intègre : comme $A/\mathfrak{m}$ est un corps, il en est de même de $B/\mathfrak{P}$ d'après la proposition 2.1.20, si bien que $\mathfrak{P}$ est en fait maximal dans B. □

2.2. **Trace, norme et discriminant.** Soit A un anneau.

2.2.1. *Trace et norme.*

Définition 2.2.2. (1) Soient M un A-module libre [a] de rang fini et $f \in \mathsf{End}_A(M)$. Si $\mathfrak{B}$ est une base de M sur A, on peut décrire f par une matrice $(a_{i,j})_{1\leqslant i,j\leqslant n}$ (où $n = \mathrm{rg}_A(M)$). La **trace**, le **déterminant** et le **polynôme caractéristique** de f sont

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

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

Ils ne dépendent que de f et pas du choix de la base $\mathfrak{B}$. Rappelons que $\mathsf{Tr}(f + \alpha g) = \mathsf{Tr}(f) + \alpha\,\mathsf{Tr}(g)$, $\det(fg) = \det(f)\det(g)$ et $\det(\alpha f) = \alpha^n \det(f)$ pour $\alpha \in A$ et $f, g \in \mathsf{End}_A(M)$.

(2) Soit B une A-algèbre libre [b] de rang fini sur A. Si $x \in B$, on dispose de $m_x \in \mathsf{End}_A(B)$ défini par $m_x(b) = xb$. On pose alors

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

qu'on appelle respectivement la **trace**, la **norme** et le **polynôme caractéristique** de x (notons que ce dernier est unitaire).

a. Il est possible d'étendre les définitions qui suivent à un cadre un peu plus général (où M est **projectif** sur A), ce qui serait à vrai dire nécessaire pour travailler avec des extensions de corps de nombres dont le corps de base n'est pas $\mathbf{Q}$.

b. *I.e.* telle que B soit libre vu comme A-module.

Proposition 2.2.3. Soient B une A-algèbre faisant de B un A-module libre de rang n, $x, y \in B$ et $a \in A$. On a

(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 2.2.4. Soient L/K une extension de corps de degré fini, $x \in L$, et $x_1, \ldots, x_n$ les racines (dans une clôture algébrique $\overline{K}$ de K, comptées avec multiplicités) du polynôme minimal P de x sur K. Alors

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

Démonstration. Commençons par traiter le cas où $L = K(x)$. Soit $\mathfrak{B} = (1, x, \ldots, x^{n-1})$, c'est une base de L sur K. Si $P_{x,K}(X) = X^n - \lambda_1 X^{n-1} - \cdots - \lambda_n$, la matrice de la multiplication par x

dans la base $\mathfrak{B}$ est la matrice compagnon :

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

On a $\chi_C = \det(X\mathrm{I}_n - C) = X^n - \lambda_1 X^{n-1} - \cdots - \lambda_n$, de sorte que $\chi_{x,L/K} = P$. En particulier, on a $\mathsf{Tr}_{L/K}(x) = \lambda_1 = \sum_{i=1}^{d} x_i$ et $\mathsf{N}_{L/K}(x) = (-1)^{n-1}\lambda_n = \prod_{i=1}^{d} x_i$.

Passons au cas général. Soient $d = [L : K(x)]$ et $(y_1, \dots, y_d)$ une base de L sur $K(x)$, de sorte que $L = K(x)y_1 \oplus \cdots \oplus K(x)y_d$. Comme la multiplication par x préserve chacun des $K(x)y_i$, on a $\mathsf{Tr}_{L/K}(x) = d\,\mathsf{Tr}_{K(x)/K}(x) = d\sum_{i=1}^{d} x_i$, $\mathsf{N}_{L/K}(x) = \mathsf{N}_{K(x)/K}(x)^d = \Big(\prod_{i=1}^{d} x_i\Big)^d$ et $\chi_{x,L/K} = \chi^d_{x,K(x)/K} = P^d$. □

Exemples 2.2.5. (1) Soient K un corps, x algébrique sur K et $P(X) = X^n + a_1X + \cdots + a_n \in K[X]$ son polynôme minimal. On a $\mathsf{Tr}_{K(x)/K}(x) = -a_1$, $\mathsf{N}_{K(x)/K}(x) = (-1)^n a_n$ et $\chi_{x,L/K} = P$.
(2) Si L/K est une extension finie *séparable*, $\overline{K}$ une clôture algébrique de K et $\mathsf{Hom}_{K\text{-alg}}(L, \overline{K}) = \{\sigma_1, \dots, \sigma_d\}$, on a $d = [L : K]$, et

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

(3) Soient $d \in \mathbf{Z}\backslash\{0,1\}$ sans facteur carré et $K = \mathbf{Q}(\sqrt{d})$. On a $K = \mathbf{Q} \oplus \mathbf{Q}\sqrt{d}$ et $\mathsf{Gal}(K/\mathbf{Q}) = \{\mathrm{Id}_K, \sigma\}$ où $\sigma(\sqrt{d}) = -\sqrt{d}$. Si $z = x + y\sqrt{d} \in K$ (avec $x, y \in \mathbf{Q}$), on a donc $\mathsf{Tr}_{K/\mathbf{Q}}(z) = 2x$ et $\mathsf{N}_{K/\mathbf{Q}}(z) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$.

Corollaire 2.2.6. Soient A un anneau intègre et intégralement clos, $K = \mathsf{Frac}(A)$, L/K une extension finie et B la clôture intégrale de A dans L. Si $b \in B$, alors $\mathsf{Tr}_{L/K}(b), \mathsf{N}_{L/K}(b) \in A$ et $\chi_{b,L/K} \in A[X]$. En outre, on a $b \in B^\times \Leftrightarrow \mathsf{N}_{L/K}(b) \in A^\times$.

Démonstration. Comme les conjugués de b sont eux aussi entiers sur A, il en est de même de leur somme, de leur produit, et plus généralement de tout polynôme symétrique évalué en ces conjugués. Il en résulte que $\mathsf{Tr}_{L/K}(b), \mathsf{N}_{L/K}(b) \in A$ et $\chi_{b,L/K} \in A[X]$.
Soient $b \in B\backslash\{0\}$ et P son polynôme minimal sur K. D'après la proposition 2.1.15, on a $P \in A[X]$. Écrivons $P(X) = X^d + a_1X^{d-1} + \cdots + a_d$: le polynôme minimal de b^{-1} sur K est alors $X^d + \frac{a_{d-1}}{a_d}X^{d-1} + \cdots + \frac{a_1}{a_d}X + \frac{1}{a_d}$. D'après la proposition 2.1.15, on a donc $b \in B^\times \Leftrightarrow a_d \in A^\times$. On conclut en observant que $\mathsf{N}_{L/K}(b) = \big((-1)^d a_d\big)^{[L:K(b)]}$. □

Exemples 2.2.7. (1) Soient $d \in \mathbf{Z}\backslash\{0,1\}$ sans facteur carré et $K = \mathbf{Q}(\sqrt{d})$. On a vu (proposition 2.1.17) que si $d \not\equiv 1 \mod 4\,\mathbf{Z}$, alors $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$. Si $z = x + y\sqrt{d} \in \mathbf{Z}[\sqrt{d}]$, on a vu que $\mathsf{N}_{K/\mathbf{Q}}(z) = x^2 - dy^2$ (exemple 2.2.5 (3)). Comme $\mathbf{Z}^\times = \{\pm 1\}$, on a donc $z \in \mathbf{Z}[\sqrt{d}]^\times \Leftrightarrow x^2 - dy^2 \in \{\pm 1\}$. Lorsque $d < 0$ (l'extension $K/\mathbf{Q}$ est alors « quadratique imaginaire »), cela équivaut à $x^2 - dy^2 = 1$. Il en résulte que si $d \leqslant -2$, on a $\mathbf{Z}[\sqrt{d}]^\times = \{\pm 1\}$ et si $d = -1$, on a $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$.
(2) Soient p un nombre premier impair, $\zeta \in \mathbf{C}$ une racine primitive p-ième de l'unité et $K = \mathbf{Q}(\zeta)$. Le polynôme minimal de ζ sur $\mathbf{Q}$ est $P(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. On a donc $\mathsf{Tr}_{K/\mathbf{Q}}(\zeta) = -1$ et $\mathsf{N}_{K/\mathbf{Q}}(\zeta) = 1$. On a donc $\mathsf{Tr}_{K/\mathbf{Q}}(\zeta - 1) = \mathsf{Tr}_{K/\mathbf{Q}}(\zeta) - \mathsf{Tr}_{K/\mathbf{Q}}(1) = -p$. Le polynôme minimal de $\zeta - 1$ est $P(X + 1)$, donc $\mathsf{N}_{K/\mathbf{Q}}(\zeta - 1) = P(1) = p$. De même, le polynôme minimal de $\zeta + 1$ est $P(X - 1)$, donc $\mathsf{N}_{K/\mathbf{Q}}(\zeta + 1) = P(-1) = 1$ (ce qui montre que $\frac{1}{\zeta+1}$ est entier sur $\mathbf{Z}$ en vertu du corollaire précédent).

Proposition 2.2.8. (Transitivité). Si L/K et K/F sont des extensions finies de corps, on a

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

Lemme 2.2.9. Soient L/K et K/F des extensions algébriques, et $\overline{F}$ un clôture algébrique de F. Alors il existe une bijection

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

Démonstration. Si $\rho \in \mathsf{Hom}_{F\text{-alg}}(K,\overline{L})$, on fixe un prolongement $\widehat{\rho} \in \mathsf{Hom}_{F\text{-alg}}(\overline{F},\overline{F})$ (on applique le théorème de Steinitz). Si $\sigma \in \mathsf{Hom}_{F\text{-alg}}(L,\overline{F})$ on note σ_K la restriction de σ à K et on pose $\sigma^K = \widehat{\sigma_{|K}}^{-1} \circ \sigma$. Par construction, σ^K laisse K invariant : on a $\sigma^K \in \mathsf{Hom}_{K\text{-alg}}(L,\overline{F})$. On dispose donc de l'application

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

Elle est injective parce que $\sigma = \widehat{\sigma_K} \circ \sigma^K$. Elle est surjective parce que si $(\rho,\tau) \in \mathsf{Hom}_{K\text{-alg}}(L,\overline{F}) \times \mathsf{Hom}_{F\text{-alg}}(K,\overline{F})$, et si $\sigma = \widehat{\rho} \circ \tau$, on a $\sigma_K = \rho$ et $\sigma^K = \tau$. □

Démonstration de la proposition 2.2.8. On se restreint au cas où L/F est séparable. On conserve les notations du lemme 2.2.9. Soit $x \in L$: d'après l'exemple 2.2.5, on a

$$\begin{aligned} \mathsf{Tr}_{L/F}(x) &= \sum_{\sigma \in \mathsf{Hom}_{F\text{-alg}}(L,\overline{F})} \sigma(x) \\ &= \sum_{\substack{\tau \in \mathsf{Hom}_{K\text{-alg}}(L,\overline{F}) \\ \rho \in \mathsf{Hom}_{F\text{-alg}}(K,\overline{F})}} \widehat{\rho}\big(\tau(x)\big) \qquad \text{(d'après le lemme 2.2.9)} \\ &= \sum_{\rho \in \mathsf{Hom}_{F\text{-alg}}(K,\overline{F})} \widehat{\rho}\Big(\sum_{\tau \in \mathsf{Hom}_{K\text{-alg}}(L,\overline{F})} \tau(x)\Big) \\ &= \sum_{\rho \in \mathsf{Hom}_{F\text{-alg}}(K,\overline{F})} \widehat{\rho}(\mathsf{Tr}_{L/K}(x)) \qquad \text{(parce que } L/K \text{ est séparable, } cf \text{ exemple 2.2.5 (2))} \end{aligned}$$

Comme $\mathsf{Tr}_{L/K}(x) \in K$, on a $\widehat{\rho}(\mathsf{Tr}_{L/K}(x)) = \rho(\mathsf{Tr}_{L/K}(x))$ pour tout $\rho \in \mathsf{Hom}_{F\text{-alg}}(K,\overline{F})$, et donc $\mathsf{Tr}_{L/F}(x) = \mathsf{Tr}_{K/F}(\mathsf{Tr}_{L/K}(x))$ (*cf* exemple 2.2.5 (2)). Le calcul pour la norme est identique à ceci près qu'on remplace les sommes par des produits. □

2.2.10. *Discriminant.*

Définition 2.2.11. Soient B une A-algèbre libre de rang fini n et $x_1,\dots,x_n \in B$. Le **discriminant** de $(x_1,\dots,x_n)$ est l'élément

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

Proposition 2.2.12. Dans les conditions de la définition 2.2.11, soit $M = (a_{i,j})_{1\leqslant i,j\leqslant n} \in \mathsf{M}_n(A)$ et $y_i = \sum_{j=1}^{n} a_{i,j}x_j \in B$ pour $i \in \{1,\dots,n\}$. Alors

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

Démonstration. Posons $X = \big(\mathsf{Tr}_{B/A}(x_i x_j)\big)_{1\leqslant i,j\leqslant n}$ et $Y = \big(\mathsf{Tr}_{B/A}(y_i y_j)\big)_{1\leqslant i,j\leqslant n}$. Pour tout $i,j \in \{1,\dots,n\}$, on a

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

d'où

$$\mathsf{Tr}_{B/A}(y_i y_j) = \sum_{k=1}^{n}\sum_{l=1}^{n} a_{i,k}\,\mathsf{Tr}_{B/A}(x_k x_l)a_{j,l}$$

soit $Y = MX^{\mathrm{T}}M$, donc $\det(Y) = \det(M)^2\det(X)$ *i.e.* $\mathrm{D}(y_1,\dots,y_n) = \det(M)^2\,\mathrm{D}(x_1,\dots,x_n)$. □

Corollaire 2.2.13. Dans les conditions de la définition 2.2.11, soient $(x_1, \dots, x_n)$ et $(y_1, \dots, y_n)$ deux bases de B sur A. Alors

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

Démonstration. Il existe $M = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{GL}_n(A)$ telle que $y_i = \sum_{j=1}^{n} a_{i,j} x_j \in B$ pour $i \in \{1, \dots, n\}$. On a alors $\mathrm{D}(y_1, \dots, y_n) = \det(M)^2 \, \mathrm{D}(x_1, \dots, x_n)$ d'après la proposition 2.2.12 : comme $\det(M) \in A^\times$, on a bien $\mathrm{D}(y_1, \dots, y_n)A = \mathrm{D}(x_1, \dots, x_n)A$. □

Remarque 2.2.14. Lorsque $\mathfrak{B} = (x_1, \dots, x_n)$ est une base de B sur A, l'élément $\mathrm{D}(x_1, \dots, x_n)$ est le discriminant de la forme bilinéaire $B \times B \to A$; $(x, y) \mapsto \mathsf{Tr}_{B/A}(xy)$ dans la base $\mathfrak{B}$.

Définition 2.2.15. D'après le corollaire 2.2.13, dans les conditions de la définition 2.2.11, l'idéal $\mathrm{D}(x_1, \dots, x_n)A$ ne dépend pas de la base $(x_1, \dots, x_n)$ de B sur A. Cet idéal principal s'appelle le **discriminant** de B sur A et est noté $\mathfrak{d}_{B/A}$.

Proposition 2.2.16. Sous les hypothèses de la définition 2.2.11, si $\mathfrak{d}_{B/A}$ contient un élément qui n'est pas diviseur de zéro, et si $x_1, \dots, x_n \in B$, les conditions suivantes sont équivalentes :
(i) $(x_1, \dots, x_n)$ est une base de B sur A ;
(ii) $\mathrm{D}(x_1, \dots, x_n)$ engendre $\mathfrak{d}_{B/A}$.

Démonstration. L'implication (i) ⇒ (ii) résulte de la définition de l'idéal $\mathfrak{d}_{B/A}$. Réciproquement, supposons que $\mathrm{D}(x_1, \dots, x_n)$ engendre $\mathfrak{d}_{B/A}$. Soient $(b_1, \dots, b_n)$ une base de B sur A et $d = \mathrm{D}(b_1, \dots, b_n)$ de sorte que $\mathfrak{d}_{B/A} = dA$. Il existe $M = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(A)$ telle que $x_i = \sum_{j=1}^{n} a_{i,j} b_j$ pour tout $i \in \{1, \dots, n\}$. D'après la proposition 2.2.12, on a $\mathrm{D}(x_1, \dots, x_n) = \det(M)^2 d$. Comme $\mathrm{D}(x_1, \dots, x_n)$ engendre $\mathfrak{d}_{B/A} = dA$, il existe $u \in A^\times$ tel que $\mathrm{D}(x_1, \dots, x_n) = ud$, si bien que $d(u - \det(M)^2) = 0$. Comme d n'est pas diviseur de zéro (sinon $\mathfrak{d}_{B/A}$ ne serait constitué que de diviseurs de zéro, contrairement à l'hypothèse), on a $\det(M)^2 = u$ et donc $\det(M) \in A^\times$, de sorte que $M \in \mathsf{GL}_n(A)$, ce qui implique que $(x_1, \dots, x_n)$ est une base de B sur A. □

Corollaire 2.2.17. Sous les hypothèses de la définition 2.2.11, supposons en outre A factoriel. Soit $x_1, \dots, x_n \in B$ tel que $d = \mathrm{D}(x_1, \dots, x_n) \in A \backslash \{0\}$ soit sans facteur carré. Alors $(x_1, \dots, x_n)$ est une base de B sur A, et $\mathfrak{d}_{B/A} = dA$.

Démonstration. Soit $(e_1, \dots, e_n)$ une base de B sur A : il existe $M = [a_{i,j}]_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(A)$ telle que $x_i = \sum_{j=1}^{n} a_{i,j} e_j$. On a alors $\mathrm{D}(x_1, \dots, x_n) = \det(M)^2 \, \mathrm{D}(e_1, \dots, e_n)$ d'après la proposition 2.2.12, *i.e.* $dA = \det(M)^2 \mathfrak{d}_{B/A}$. Comme d est sans facteur carré par hypothèse, on a nécessairement $\det(M) \in A^\times$, de sorte que $\mathfrak{d}_{B/A} = dA$. D'après la proposition 2.2.16, la famille $(x_1, \dots, x_n)$ est donc une base de B sur A. □

Théorème 2.2.18. (Dedekind). Soient K/F et L/F des extensions. Alors les éléments de $\mathsf{Hom}_{F\text{-alg}}(K, L)$ sont linéairement indépendants dans le L-espace vectoriel $\mathsf{Hom}_{F\text{-lin}}(K, L)$.

Démonstration. Supposons le contraire. Soit $\sum_{i=1}^{r} \lambda_i \sigma_i = 0$ avec $\lambda_i \in L$ et $\sigma_i \in \mathsf{Hom}_{F\text{-alg}}(K, L)$ pour $i \in \{1, \dots, r\}$ une relation de dépendance linéaire non triviale avec r *minimal*. Par minimalité, on a $\lambda_i \neq 0$ pour tout $i \in \{1, \dots, r\}$, et les σ_i sont deux à deux distincts. Quitte à diviser la relation par λ_r, on peut supposer que $\lambda_r = 1$. Pour tout $x \in K$, on a donc

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

En appliquant l'égalité $(*)$ au produit de $x, y \in K$, il vient

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

En soustrayant $\sigma_r(y)$ fois l'égalité $(*)$ à l'égalité précédente, il vient

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

pour tout $x, y \in K$. En particulier, à y fixé, on a

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

Par minimalité de r, les coefficients de la combinaison linéaire sont tous nuls : on a $\sigma_i(y) = \sigma_r(y)$ pour tout $y \in K$. Les σ_i étant deux à deux distincts, cela implique $r = 1$, ce qui est impossible. □

Proposition 2.2.19. Soit L/K une extension finie séparable de corps, $\overline{K}$ une clôture algébrique de K, et $x_1, \dots, x_n$ une base de L sur K. Écrivons $\mathsf{Hom}_{K\text{-alg}}(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$. Alors

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

Démonstration. Rappelons que $\mathsf{Tr}_{L/K}(x) = \sum_{k=1}^{n} \sigma_k(x)$ pour tout $x \in L$ (exemple 2.2.5 (2)). On a alors

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

de sorte que $\left(\mathsf{Tr}_{L/K}(x_i x_j)\right)_{1\leqslant i,j\leqslant n} = {}^{\mathrm{T}}MM$ où $M = (\sigma_i(x_j))_{1\leqslant i,j\leqslant n} \in \mathsf{M}_n(\overline{K})$. On a donc

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

Reste à voir que $\det(M) \neq 0$. Soit $X = (\lambda_i)_{1\leqslant i\leqslant n} \in \mathsf{M}_{1\times n}(\overline{K})$ tel que $XM = 0$. On a alors $\sum_{i=1}^{n} \lambda_i \sigma_i(x_j) = 0$ pour tout $j \in \{1, \dots, n\}$. Par K-linéarité, cela implique que $\sum_{i=1}^{n} \lambda_i \sigma_i = 0$ dans $\mathsf{Hom}_{K\text{-lin}}(L, \overline{K})$. Mais comme l'extension L/K est séparable, le théorème de Dedekind (théorème 2.2.18) implique que $X = 0$: la matrice M est inversible, et $\det(M) \neq 0$. □

Corollaire 2.2.20. Soit L/K une extension séparable de degré n. Une famille $(x_1, \dots, x_n) \in L^n$ est une K-base de L si et seulement si $\mathrm{D}(x_1, \dots, x_n) \neq 0$.

Proposition 2.2.21. (Transitivité du discriminant) Soient K/F et L/K deux extensions finies séparables, $x_1, \dots, x_n$ une base de K sur F et $(y_1, \dots, y_m)$ une base de L sur K. Alors $\mathrm{D}(x_i y_j)_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}} = \mathrm{D}(x_1, \dots, x_n)^{[L:K]}\, \mathsf{N}_{K/F}(\mathrm{D}(y_1, \dots, y_m))$.

Démonstration. Écrivons $\mathsf{Hom}_{F\text{-alg}}(K, \overline{F}) = \{\rho_1, \dots, \rho_n\}$ et $\mathsf{Hom}_{K\text{-alg}}(L, \overline{F}) = \{\tau_1, \dots, \tau_n\}$. Fixons des relèvements $\widehat{\rho}_1, \dots, \widehat{\rho}_n \in \mathsf{Hom}_{F\text{-alg}}(\overline{F}, \overline{F})$ de $\rho_1, \dots, \rho_n$: on a $\mathsf{Hom}_{F\text{-alg}}(L, \overline{F}) = \left\{\widehat{\rho}_i \tau_j\right\}_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}}$ (*cf* lemme 2.2.9). Par ailleurs, on a $\mathrm{D}(x_i y_j)_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}} = \det(M)^2$ où $M \in \mathsf{M}_{mn}(\overline{F})$ est la matrice de terme général $\widehat{\rho}_i\tau_j(x_k y_\ell) = \rho_i(x_k)\widehat{\rho}_i\tau_j(y_\ell)$ pour $(i,j), (k,\ell) \in \left(\{1, \dots, n\} \times \{1, \dots, m\}\right)^2$ (*cf* proposition 2.2.19). Posons $Y = (\tau_j(y_\ell))_{1\leqslant j,\ell\leqslant m} \in \mathsf{M}_m(\overline{F})$: la matrice M s'écrit par blocs $\begin{pmatrix} \rho_1(x_1)\widehat{\rho}_1(Y) & \cdots & \rho_1(x_n)\widehat{\rho}_1(Y) \\ \vdots & & \vdots \\ \rho_n(x_1)\widehat{\rho}_n(Y) & \cdots & \rho_n(x_n)\widehat{\rho}_n(Y) \end{pmatrix} = M_1 M_2$ en posant $M_1 = \mathsf{diag}\left(\widehat{\rho}_1(Y), \dots, \widehat{\rho}_n(Y)\right) \in \mathsf{M}_{mn}(\overline{F})$ et $M_2 = \begin{pmatrix} \rho_1(x_1)\,\mathrm{I}_m & \cdots & \rho_1(x_n)\,\mathrm{I}_m \\ \vdots & & \vdots \\ \rho_n(x_1)\,\mathrm{I}_m & \cdots & \rho_n(x_n)\,\mathrm{I}_m \end{pmatrix} \in \mathsf{M}_{mn}(\overline{F})$. On a $\det(M_1)^2 = \prod_{\rho\in\mathsf{Hom}_{\text{-alg}}\, F(K,\overline{F})} \widehat{\rho}(\det(Y)^2) = \mathsf{N}_{K/F}(\mathrm{D}(y_1, \dots, y_m))$. Par ailleurs, il existe une matrice de permutation $P \in \mathsf{GL}_{mn}(\mathbf{Z})$ telle que $P^{-1}M_2P = \mathsf{diag}(X, \dots, X)$ avce $X = (\rho_i(x_k))_{1\leqslant i,k\leqslant n} \in \mathsf{M}_n(\overline{F})$. On a donc $\det(M_2) = \det(X)^m$,

d'où $\det(M_2)^2 = \mathrm{D}(x_1,\dots,x_n)^{[L:K]}$ (parce que $[L:K]=m$). Finalement, on a $\mathrm{D}(x_iy_j)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}} = \det(M)^2 = \det(M_1)^2\det(M_2)^2 = \mathrm{D}(x_1,\dots,x_n)^{[L:K]}\,\mathsf{N}_{K/F}(\mathrm{D}(y_1,\dots,y_m))$. □

Corollaire 2.2.22. (Transitivité du discriminant) Soient A un anneau intègre, $F=\mathsf{Frac}(A)$ et K/F et L/K deux extensions finies séparables. On note B (resp. C) la clôture intégrale de A dans K (resp. L). On suppose B libre sur A et C libre sur B. Alors $\mathfrak{d}_{C/A} = \mathfrak{d}_{B/A}^{\mathrm{rg}_B(C)}\,\mathsf{N}_{B/A}(\mathfrak{d}_{C/B})$ (où [a] $\mathsf{N}_{B/A}(dB) = \mathsf{N}_{B/A}(d)A$).

a. Cela ne dépend pas du choix du générateur d.

2.3. **Discriminant d'un polynôme.**

Définition 2.3.1. Soient K un corps, $P\in K[X]$ unitaire et $\alpha_1,\dots,\alpha_n\in\overline{K}$ les racines de P dans une clôture algébrique $\overline{K}$ de K (comptées avec multiplicité). Le **discriminant** de P est

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

C'est un polynôme symétrique en les racines de P, donc un polynôme en les coefficients de P, et $\mathsf{disc}(P)\in K$. Par définition, P est séparable si et seulement si $\mathsf{disc}(P)\neq 0$.

Lemme 2.3.2. Avec les notations de la définition 2.3.1, on a

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

Démonstration. On a $P'(X) = \sum_{i=1}^{n}\prod_{1\leqslant j\neq i\leqslant n}(X-\alpha_j)$ donc $P'(\alpha_i) = \prod_{1\leqslant j\neq i\leqslant n}(\alpha_i-\alpha_j)$ ce qui implique $\prod_{i=1}^{n}P'(\alpha_i) = \prod_{1\leqslant i\neq j\leqslant n}(\alpha_i-\alpha_j) = (-1)^{\frac{n(n-1)}{2}}\mathsf{disc}(P)$. □

Exemples 2.3.3. (1) Le discriminant de X^2+aX+b est a^2-4b. Celui de X^3+pX+q est $-4p^3-27q^2$ (exercice).
(2) Soient $n\in\mathbf{N}_{>0}$ et $P(X)=X^n-1\in\mathbf{Q}[X]$. On pose $\mu_n=\{z\in\mathbf{C},\,z^n=1\}$: on a $P(X)=\prod_{\zeta\in\mu_n}(X-\zeta)$. Pour $\zeta\in\mu_n$, on a $P'(\zeta)=n\zeta^{n-1}$: comme $\prod_{\zeta\in\mu_n}\zeta=(-1)^{n+1}$, on a $\prod_{\zeta\in\mu_n}P'(\zeta) = n^n(-1)^{n^2-1}$, et donc

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

Remarque 2.3.4. À un coefficient de normalisation près, le discriminant n'est autre que le résultant de P et de P'.

Proposition 2.3.5. Soient L/K une extension séparable de degré d, $\alpha\in L$ tel que $L=K[\alpha]$ et $P\in K[X]$ le polynôme minimal de α sur K. Alors $(1,\alpha,\alpha^2,\dots,\alpha^{n-1})$ est une base de L sur K et

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

Démonstration. Soient $\overline{K}$ une clôture algébrique de K et $\mathsf{Hom}_{K\text{-alg}}(L,\overline{K})=\{\sigma_1,\dots,\sigma_n\}$. Les conjugués de α sont les $\alpha_i:=\sigma_i(\alpha)$ pour $i\in\{1,\dots,n\}$. L'extension L/K est séparable : d'après la proposition 2.2.19, on a

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

Comme $\det\left((\alpha_i^{j-1})_{1\leqslant i,j\leqslant n}\right) = \prod_{1\leqslant i<j\leqslant n}(\alpha_i-\alpha_j)$ (déterminant de Vandermonde), cela prouve la première égalité.

D'après le lemme 2.3.2, on a $\mathsf{disc}(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} P'(\alpha_i)$. Pour $i \in \{1, \dots, n\}$, on a $\alpha_i = \sigma_i(\alpha)$, donc $\prod_{i=1}^{n} P'(\alpha_i) = \prod_{i=1}^{n} \sigma(P'(\alpha)) = \mathsf{N}_{L/K}(P'(\alpha))$, ce qui prouve la seconde égalité. □

Exemple 2.3.6. Soient K un corps et $P(X) = X^n + aX + b \in K[X]$ supposé irréductible et séparable. Si α est une racine de P dans une clôture algébrique de K, on a [3]

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

Pour $n \in \{2, 3\}$, on retrouve les formules de l'exemple 2.3.3 (1).

2.4. **Clôture intégrale dans une extension séparable.**

Proposition 2.4.1. Soit L/K une extension finie séparable de corps.

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

est une forme bilinéaire non dégénérée.

Démonstration. La bilinéarité de l'application résulte de la proposition 2.2.3. Soit $x \in L$ tel que $\mathsf{Tr}_{L/K}(xy) = 0$ pour tout $y \in L$. Soient $\overline{K}$ une clôture algébrique de K et $\mathsf{Hom}_{K\text{-alg}}(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$, on a $\mathsf{Tr}_{L/K}(xy) = \sum_{i=1}^{n} \sigma_i(x)\sigma_i(y)$, de sorte que $\sum_{i=1}^{n} \sigma_i(x)\sigma_i$. Mais comme $\{\sigma_1, \dots, \sigma_n\}$ est libre dans $\mathsf{Hom}_{K\text{-lin}}(L, \overline{K})$ (théorème de Dedekind), cela implique $\sigma_i(x) = 0$ pour tout $i \in \{1, \dots, n\}$, et donc $x = 0$. Le noyau de la forme bilinéaire est nul : elle est non dégénérée. □

Remarque 2.4.2. En fait, la proposition qui précède est une équivalence. En effet, si L/K est inséparable, $\mathsf{car}(K) = p$ est un nombre premier, et il existe une sous-extension L'/K telle que L'/K soit séparable et L/L' totalement inséparable. On a $[L : L'] = p^d$ avec $d \in \mathbf{N}_{>0}$. Soient $x \in L$, $x_1, \dots, x_n \in \overline{L}$ les conjugués de x sur K (comptés sans multiplicité) et $r \in \mathbf{N}$ minimal tel que $x^{p^r} \in L'$ (on a bien entendu $r \leqslant d$). La multiplicité de chaque x_i est alors p^r. On a donc $\mathsf{Tr}_{K(x)/K}(x) = p^r(x_1 + \cdots + x_n)$. Comme $[L : K(x)] = \frac{p^d[L':K]}{p^r n}$, on a donc

$$\mathsf{Tr}_{L/K}(x) = [L : K(x)]\, \mathsf{Tr}_{K(x)/K}(x) = p^d \frac{[L' : K]}{n}(x_1 + \cdots + x_n) = 0$$

Cela implique que $\mathsf{Tr}_{L/K} = 0$, et donc que la forme bilinéaire $\mathsf{Tr}_{L/K}$ est dégénérée.

Corollaire 2.4.3. Soit L/K une extension finie séparable de corps. L'application

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

est un isomorphisme de K-espaces vectoriels. Si $(x_1, \dots, x_n)$ est une base de L sur K, il existe une unique base $(y_1, \dots, y_n)$ de L sur K telle que $\mathsf{Tr}_{L/K}(x_i y_j) = \delta_{i,j}$ pour tout $i, j \in \{1, \dots, n\}$. On l'appelle la base **duale** de $(x_1, \dots, x_n)$.

Démonstration. L'application $f\colon L \to \mathsf{Hom}_{K\text{-lin}}(L, K)$ est la première application linéaire associée à la forme bilinéaire $(x, y) \mapsto \mathsf{Tr}_{L/K}(xy)$. Comme cette dernière est non dégénérée, l'application f est injective. C'est donc un isomorphisme vu que $\dim_K \left(\mathsf{Hom}_{K\text{-lin}}(L, K)\right) = \dim_K(L)$. Si $(x_1, \dots, x_n)$ est une base de L sur K, la famille $(f(x_1), \dots, f(x_n))$ est une base de $\mathsf{Hom}_{K\text{-lin}}(L, K)$ sur K. La famille $(y_1, \dots, y_n)$ vérifie $\mathsf{Tr}_{L/K}(x_i y_j) = f(x_i)(y_j) = \delta_{i,j}$ pour tout $i, j \in \{1, \dots, n\}$ si et seulement si c'est la base duale de $(f(x_1), \dots, f(x_n))$ dans L : elle existe et est unique. □

3. On a $P'(\alpha) = n\alpha^{n-1} + a = n\frac{-a\alpha - b}{\alpha} + a = -\frac{nb}{\alpha} - (n-1)a$. Le polynôme minimal de α^{-1} étant $X^n + \frac{a}{b}X^{n-1} + \frac{1}{b}$, celui de $-\frac{nb}{\alpha}$ est $Q(X) = X^n - naX^{n-1} + (-n)^n b^{n-1}$ et celui de $P'(\alpha)$ est donc $Q(X + (n-1)a)$. On a donc $\mathsf{N}_{K(\alpha)/K}(P'(\alpha)) = (-1)^n Q((n-1)a) = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n$.

Proposition 2.4.4. Soient A un anneau intègre et intégralement clos, K son corps des fractions et L/K une extension finie séparable. Notons B la clôture intégrale de A dans L. Alors B contient une base de L sur K, et c'est un sous-A-module d'un A-module libre de rang $[L : K]$ contenu dans L.

Démonstration. Si $(e_1, \dots, e_n)$ est une base de L sur K, il existe $a \in A\backslash\{0\}$ tels que $x_i := ae_i \in B$ pour tout $i \in \{1, \dots, n\}$ (*cf* proposition 2.1.12). La famille $(x_1, \dots, x_n)$ est encore une base de L sur K, et elle est constituée d'éléments de B.

Soient $(y_1, \dots, y_n)$ la base duale de $(x_1, \dots, x_n)$ et B' le sous-A-module de L engendré par $\{y_1, \dots, y_n\}$. Comme $(y_1, \dots, y_n)$ est une base de L sur K, le A-module B' est libre de rang $n = [L : K]$. Si $x \in B$, on peut écrire de façon unique $x = \sum_{j=1}^{n} \lambda_j y_j$ avec $\lambda_1, \dots, \lambda_n \in K$. On a alors $x_i x \in B$ donc $\mathsf{Tr}_{L/K}(x_i x) = \sum_{j=1}^{n} \lambda_j \mathsf{Tr}_{L/K}(x_i y_j) = \lambda_i \in A$ pour tout $i \in \{1, \dots, n\}$ (corollaire 2.2.6), et donc $x \in B'$. □

Proposition 2.4.5. Sous les hypothèses de la proposition 2.4.4, on a en fait l'énoncé plus explicite suivant. Si $(x_1, \dots, x_n)$ est une base de L sur K constituée d'éléments de B, on a

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

où $d = \mathrm{D}(x_1, \dots, x_d)$.

Démonstration. D'après la preuve de la proposition 2.4.4, si $(y_1, \dots, y_n)$ désigne la base duale de $(x_1, \dots, x_n)$, on a

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

Écrivons $y_i = \sum_{j=1}^{n} \alpha_{i,j} x_j$ avec $\alpha_{i,j} \in K$ pour tout $i, j \in \{1, \dots, n\}$. On a

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

de sorte que si $M = \big(\mathsf{Tr}_{L/K}(x_i x_j)\big)_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(A)$ et $N = (\alpha_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathsf{M}_n(K)$, on a $M\,{}^{\mathrm{T}}N = \mathrm{I}_n$, *i.e.* ${}^{\mathrm{T}}N = M^{-1} \in \frac{1}{d}\mathsf{M}_n(A)$ d'après les formules de Cramer : on a $\alpha_{i,j} \in \frac{1}{d}A$ pour tout $i, j \in \{1, \dots, n\}$. □

Corollaire 2.4.6. Sous les hypothèses de la proposition 2.4.4, on a :
(1) si A est nœthérien, alors B est une A-algèbre finie (en particulier, B est nœthérien) ;
(2) si A est principal, alors B est un A-module libre de rang $[L : K]$.

Démonstration. D'après la proposition 2.4.4, il existe B' un sous-A-module de L qui est libre de rang $[L : K]$ et tel que $B \subseteq B'$.
(1) Si A est nœthérien, il en est de même de B' (corollaire 1.1.6) : le A-module B est de type fini (et donc nœthérien d'après le corollaire 1.1.6). En particulier, B est finie sur A (proposition 2.1.5).
(2) Si A est principal, B est libre de rang fini comme sous-A-module du A-module libre de rang fini B' (théorème 1.5.9). Comme il contient une base de L sur K (proposition 2.4.4), il est nécessairement de rang $[L : K]$. □

Remarque 2.4.7. Sous les hypothèses de la proposition 2.4.4, supposons en outre A principal. D'après le corollaire 2.2.17, si $x_1, \dots, x_n \in B$ sont tels que $\mathrm{D}(x_1, \dots, x_n)$ soit sans facteur carré dans l'anneau A (qui est principal donc factoriel), alors $(x_1, \dots, x_n)$ est une base de B sur A.

2.5. **Bases des anneaux d'entiers des corps de nombres.** Dans tout ce qui suit, $\overline{\mathbf{Q}}$ désigne la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$. Rappelons qu'un corps de nombres est une extension finie de $\mathbf{Q}$, et que si K est un corps de nombres, on note $\mathcal{O}_K$ l'anneau des entiers de K, *i.e.* est la clôture intégrale de $\mathbf{Z}$ dans K.

Proposition 2.5.1. Soient K un corps de nombres et $n = [K : \mathbf{Q}]$. L'anneau des entiers $\mathcal{O}_K$ est un $\mathbf{Z}$-module libre de rang n.

Démonstration. Résulte du fait que $\mathbf{Z}$ est un anneau principal et du corollaire 2.4.6 (2). □

Définition 2.5.2. Soient $(x_1, \dots, x_n)$ et $(y_1, \dots, y_n)$ deux bases de $\mathcal{O}_K$ sur $\mathbf{Z}$. Il existe $M = [m_{i,j}]_{1 \leqslant i,j \leqslant n} \in \mathsf{GL}_n(\mathbf{Z})$ telle que $y_i = \sum_{j=1}^{n} m_{i,j} x_j$ pour tout $i \in \{1, \dots, n\}$, de sorte que

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

(car $\det(M) \in \{\pm 1\} = \mathbf{Z}^\times$). L'entier

$$d_K = \mathrm{D}(x_1, \dots, x_n)$$

ne dépend pas du choix de la base $(x_1, \dots, x_n)$. On l'appelle le **discriminant absolu** de K.

Exemple 2.5.3. Soient $d \in \mathbf{Z} \backslash \{0, 1\}$ sans facteur carré et $K = \mathbf{Q}(\sqrt{d})$. Si $d \equiv 1 \mod 4\,\mathbf{Z}$, alors $\mathcal{O}_K = \mathbf{Z}[\alpha]$ avec $\alpha = \frac{1+\sqrt{d}}{2}$ (proposition 2.1.17) : la famille $(1, \alpha)$ est une base de $\mathcal{O}_K$ sur $\mathbf{Z}$. Le polynôme minimal de α sur $\mathbf{Q}$ est $P(X) = X^2 - X - \frac{d-1}{4}$: on a donc $d_K = \mathrm{D}(1, \alpha) = \mathsf{disc}(P) = d$ (on peut aussi faire le calcul directement). Si $d \not\equiv 1 \mod 4\,\mathbf{Z}$, on a $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$ (proposition 2.1.17) : la famille $(1, \sqrt{d})$ est une base de $\mathcal{O}_K$ sur $\mathbf{Z}$. Le polynôme minimal de $\sqrt{d}$ sur $\mathbf{Q}$ est $P(X) = X^2 - d$: on a donc $d_K = \mathrm{D}(1, \sqrt{d}) = \mathsf{disc}(P) = 4d$. En résumé, on a

$$d_K = \begin{cases} d & \text{si } d \equiv 1 \mod 4\,\mathbf{Z} \\ 4d & \text{si } d \not\equiv 1 \mod 4\,\mathbf{Z} \end{cases}$$

Proposition 2.5.4. Soient K un corps de nombres et $n = [K : \mathbf{Q}]$.

(1) Une famille $x_1, \dots, x_n \in \mathcal{O}_K$ est une base de $\mathcal{O}_K$ sur $\mathbf{Z}$ si et seulement si $\mathrm{D}(x_1, \dots, x_n) = d_K$.

(2) Si $x_1, \dots, x_n \in \mathcal{O}_K$ est telle que $\mathrm{D}(x_1, \dots, x_n) \backslash \{0\}$ est sans facteur carré, alors $(x_1, \dots, x_n)$ est une base de $\mathcal{O}_K$ sur $\mathbf{Z}$.

Démonstration. Cela résulte de la proposition 2.2.16 et du corollaire 2.2.17. □

Il est en général difficile de calculer l'anneau des entiers d'un corps de nombres K. Une approche est de partir d'un élément primitif, *i.e.* un élément α tel que $K = \mathbf{Q}(\alpha)$. Quitte à multiplier α par un entier convenable (le plus petit possible), on peut supposer que $\alpha \in \mathcal{O}_K$, de sorte que $\mathbf{Z}[\alpha] \subseteq \mathcal{O}_K$. En général, l'inclusion est stricte, mais $\mathbf{Z}[\alpha]$ est d'indice fini dans $\mathcal{O}_K$. Plus précisément, d'après la proposition 2.4.5, on a $\mathbf{Z}[\alpha] \subseteq \mathcal{O}_K \subseteq \frac{1}{d}\mathbf{Z}[\alpha]$ avec $d = \mathrm{D}(1, \alpha, \dots, \alpha^{n-1})$ (où $n = [K : \mathbf{Q}]$), qu'on calcule aisément en utilisant le polynôme minimal de α sur $\mathbf{Q}$ et la proposition 2.3.5. Cela réduit déjà considérablement les possibilités pour $\mathcal{O}_K$. À partir de là, on peut chercher les conditions sur ses coordonnées dans la base $(1, \alpha, \dots, \alpha^{n-1})$ un élément $x \in K$ appartient à $\mathcal{O}_K$. Pour trouver de telles conditions, on utilise la trace et la norme. Par exemple, si $x \in K$ est entier sur $\mathbf{Z}$, il en est de même de $\alpha^i x$ de sorte que $\mathsf{Tr}_{K/\mathbf{Q}}(\alpha^i x) \in \mathbf{Z}$ pour tout $i \in \{0, \dots, n-1\}$.

Remarque 2.5.5. Contrairement aux corps de nombres, les anneaux d'entiers de corps de nombres ne sont pas monogènes : si K est un corps de nombres, en général, il n'existe pas $\alpha \in K$ tel que $\mathcal{O}_K = \mathbf{Z}[\alpha]$.

Exemple 2.5.6. Soient p premier impair, $\zeta \in \mathbf{C}$ une racine primitive p-ième de l'unité et $K = \mathbf{Q}(\zeta)$. On a bien sûr $\mathbf{Z}[\zeta] \subseteq \mathcal{O}_K$. Le polynôme minimal de ζ sur $\mathbf{Q}$ est

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 = \frac{X^p - 1}{X - 1}$$

On a $(X-1)\Phi_p'(X) + \Phi_p(X) = pX^{p-1}$, donc $\Phi_p'(\zeta) = \frac{p\zeta^{p-1}}{\zeta - 1}$. On a donc $\mathsf{N}_{K/\mathbf{Q}}(\Phi_p'(\zeta)) = \frac{\mathsf{N}_{K/\mathbf{Q}}(p)\,\mathsf{N}_{K/\mathbf{Q}}(\zeta)^{p-1}}{\mathsf{N}_{K/\mathbf{Q}}(\zeta - 1)} = \frac{p^{p-1}}{p} = p^{p-2}$ (d'après l'exemple 2.2.7 (2), on a $\mathsf{N}_{K/\mathbf{Q}}(\zeta) = 1$ et $\mathsf{N}_{K/\mathbf{Q}}(\zeta - 1) = p$), ce qui implique que

$$\mathrm{D}(1, \zeta, \zeta^2, \cdots, \zeta^{p-2}) = \mathsf{disc}(\Phi_p) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2} = (-1)^{\frac{p-1}{2}} p^{p-2}$$

(proposition 2.3.5). On sait donc que

$$\mathbf{Z}[\zeta] \subset \mathcal{O}_K \subset \tfrac{1}{p^{p-2}}\,\mathbf{Z}[\zeta]$$

Montrons que $\mathcal{O}_K = \mathbf{Z}[\zeta]$.
Commençons par observer que $(1-\zeta)\mathcal{O}_K \cap \mathbf{Z} = p\,\mathbf{Z}$. En effet, on a déjà $p \in (1-\zeta)\mathcal{O}_K$ parce que $1-\zeta \mid \mathsf{N}_{K/\mathbf{Q}}(\zeta-1) = p$. Si l'inclusion $p\,\mathbf{Z} \subset (1-\zeta)\mathcal{O}_K \cap \mathbf{Z}$ était stricte, on aurait nécessairement $(1-\zeta)\mathcal{O}_K \cap \mathbf{Z} = \mathbf{Z}$, et donc $1 \in (1-\zeta)\mathcal{O}_K$: il existerait $z \in \mathcal{O}_K$ tel que $1 = (1-\zeta)z$, donc $1 = p\,\mathsf{N}_{K/\mathbf{Q}}(z)$ dans $\mathbf{Z}$, ce qui est absurde.
Si maintenant $x = x_0 + x_1\zeta + \cdots + x_{p-2}\zeta^{p-2} \in \mathcal{O}_K$ (avec $x_0, \ldots, x_{p-2} \in \mathbf{Q}$), on a

$$(1-\zeta)x = x_0(1-\zeta) + x_1(\zeta-\zeta^2) + \cdots + x_{p-2}(\zeta^{p-2}-\zeta^{p-1})$$

Comme $\mathsf{Tr}_{K/\mathbf{Q}}(1-\zeta) = p$ et $\mathsf{Tr}_{K/\mathbf{Q}}(\zeta^k - \zeta^{k+1}) = 0$ pour $1 \leqslant k < p-1$, on a

$$\mathsf{Tr}_{K/\mathbf{Q}}((1-\zeta)x) = px_0$$

Mais comme les conjugués de $(1-\zeta)x$ sont de la forme $(1-\zeta^k)y$ donc divisibles par $1-\zeta$, on a $\mathsf{Tr}_{K/\mathbf{Q}}((1-\zeta)x) \in (1-\zeta)\mathcal{O}_K \cap \mathbf{Z} = p\,\mathbf{Z}$. Cela implique donc que $x_0 \in \mathbf{Z}$.
Si on sait que $x_0, \ldots, x_{k-1} \in \mathbf{Z}$ avec $k < p-2$, alors

$$\zeta^{-k}\big(x - (x_0 + x_1\zeta + \cdots + x_{k-1}\zeta^{k-1})\big) = x_k + x_{k+1}\zeta + \cdots + x_{p-2}\zeta^{p-2-k} \in \mathcal{O}_K$$

ce qui implique que $x_k \in \mathbf{Z}$ d'après ce qui précède. Finalement, on a $x_0, \ldots, x_{p-2} \in \mathbf{Z}$ et $x \in \mathbf{Z}[\zeta]$.

Proposition 2.5.7. (Stickelberger). Soit K un corps de nombres. On a $d_K \equiv 0 \mod 4\,\mathbf{Z}$ ou $d_K \equiv 1 \mod 4\,\mathbf{Z}$.

Démonstration. Écrivons $\mathsf{Hom}_{\mathbf{Q}\text{-alg}}(K, \overline{\mathbf{Q}}) = \{\sigma_1, \ldots, \sigma_n\}$: si $\{\alpha_1, \ldots, \alpha_n\}$ est une base de $\mathcal{O}_K$ sur $\mathbf{Z}$, on a $d_K = \det(M)^2$ avec $M = (\sigma_i(\alpha_j))_{1 \leqslant i,j \leqslant n}$ (proposition 2.2.19). On a $\det(M) = S - A$ où $S = \sum_{\substack{\tau \in \mathfrak{S}_n \\ \varepsilon(\tau)=1}} \prod_{i=1}^{n} \sigma_i(\alpha_{\tau(i)})$ et $A = \sum_{\substack{\tau \in \mathfrak{S}_n \\ \varepsilon(\tau)=-1}} \prod_{i=1}^{n} \sigma_i(\alpha_{\tau(i)})$. Il en résulte que $d_K = (S+A)^2 - 4SA$: il s'agit de voir que $S + A, SA \in \mathbf{Z}$. Comme S et A sont des polynômes en les $\sigma_i(\alpha_j) \in \mathcal{O}_K$, on a déjà $S, A \in \mathcal{O}_K$: il suffit en fait de montrer que $S + A, SA \in \mathbf{Q}$. Soit $L \subset \overline{\mathbf{Q}}$ la clôture galoisienne de K. Si $g \in \mathsf{Gal}(L/\mathbf{Q})$, l'application

$$\begin{aligned} \mathsf{Hom}_{\mathbf{Q}\text{-alg}}(K, \overline{\mathbf{Q}}) &\to \mathsf{Hom}_{\mathbf{Q}\text{-alg}}(K, \overline{\mathbf{Q}}) \\ \sigma &\mapsto g \circ \sigma \end{aligned}$$

est une permutation. Si cette dernière est paire, on a $g(S) = S$ et $g(A) = A$, si elle est impaire, on a $g(S) = A$ et $g(A) = S$: dans tous les cas on a $g(S+A) = S + A$ et $g(SA) = SA$, ce qui montre que $S + A, SA \in L^{\mathsf{Gal}(L/\mathbf{Q})} = \mathbf{Q}$. □

Corollaire 2.5.8. (Raffinement de la proposition 2.5.4 (2)). Si K est un corps de nombres de degré n et $\{x_1, \ldots, x_n\}$ une famille dont le discriminant vaut $4a$ avec $a \equiv 2, 3 \mod 4\,\mathbf{Z}$ et sans facteur carré, alors $(x_1, \ldots, x_n)$ est une base de $\mathcal{O}_K$ sur $\mathbf{Z}$.

Démonstration. Soient $\mathfrak{B}$ une base de $\mathcal{O}_K$ sur $\mathbf{Z}$ et $M \in \mathsf{M}_n(\mathbf{Z})$ la matrice dont les colonnes sont les coordonnées de $(x_1, \ldots, x_n)$ dans la base $\mathfrak{B}$. D'après la proposition 2.2.12, on a $4a = \mathrm{D}(x_1, \ldots, x_n) = \det(M)^2 d_K$. Si $(x_1, \ldots, x_n)$ n'était pas une base, on aurait $\det(M) > 1$ et donc $\det(M) = 2$ puisque a est sans facteur carré. Cela impliquerait $d_K = a \equiv 2, 3 \mod 4\,\mathbf{Z}$, contredisant la proposition 2.5.7. □

3. Anneaux de Dedekind

Si A est un anneau principal, K son corps des fractions et L/K une extension finie et séparable, la clôture intégrale B de A dans L n'est plus un anneau principal en général. Comme on va le voir, l'anneau B est de Dedekind (théorème 3.1.4). Cela implique qu'on dispose dans B d'une décomposition en facteurs premiers, mais au niveau des idéaux seulement (théorème 3.3.3).

3.1. Définition, premières propriétés.

Définition 3.1.1. Soit A un anneau intègre. On dit que A est un **anneau de Dedekind** s'il vérifie les conditions suivantes :
(1) A est nœthérien ;
(2) A est intégralement clos ;
(3) tout idéal premier non nul de A est maximal.

Remarque 3.1.2. (1) En termes savants, la dernière condition se reformule en disant que la dimension de Krull de A est inférieure à 1.
(2) Avec la définition qui précède, un corps est un anneau de Dedekind (il n'y a pas d'idéal premier non nul). Certains auteurs excluent ce cas trivial, et requièrent que A ne soit pas un corps dans la définition.

Proposition 3.1.3. Tout anneau principal est de Dedekind.

Démonstration. Si A est principal, il est intègre et nœthérien par définition. Il est intégralement clos en vertu de la proposition 2.1.10. Enfin, si ce n'est pas un corps, ses idéaux premiers non nuls sont maximaux d'après la proposition 1.2.16. □

Théorème 3.1.4. Soient A un anneau de Dedekind, K son corps des fractions, L/K une extension finie séparable, et B la clôture intégrale de A dans L. Alors B est un anneau de Dedekind.

Démonstration. L'anneau A est nœthérien : d'après le corollaire 2.4.6 (1), l'anneau B est nœthérien. L'anneau B est intégralement clos en vertu de la proposition 2.1.12. Enfin, si $\mathfrak{P} \subseteq B$ est un idéal premier non nul, l'idéal $\mathfrak{p} = \mathfrak{P} \cap A$ est premier et non nul (il contient $\mathsf{N}_{L/K}(b) \neq 0$ pour tout $b \in \mathfrak{P} \backslash \{0\}$), donc maximal. Cela implique que $\mathfrak{P}$ est maximal (proposition 2.1.21). □

Corollaire 3.1.5. L'anneau des entiers d'un corps de nombres est un anneau de Dedekind.

3.2. Caractérisation locale des anneaux de Dedekind.

Proposition 3.2.1. Soient A un anneau de Dedekind et $S \subset A$ une partie muliplicative. Alors $S^{-1}A$ est de Dedekind.

Démonstration. L'anneau $S^{-1}A$ est nœthérien en vertu de la proposition 1.3.9. Comme A est intégralement clos, il en est de même de $S^{-1}A$ d'après la proposition 2.1.13. Enfin, la proposition 1.3.10 fournit une bijection croissante (pour l'inclusion)

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

Comme les éléments non nuls de $\mathsf{Spec}(A)$ sont maximaux, il en est de même des éléments non nuls de $\mathsf{Spec}(S^{-1}A)$, ce qui achève la preuve. □

Lemme 3.2.2. Un anneau de Dedekind local est soit un corps, soit de valuation discrète.

Démonstration. Soit A de Dedekind et local. Il s'agit de voir que A est principal (*cf* définition 1.3.18). Supposons que A ne soit pas un corps : son idéal maximal $\mathfrak{m}$ est non nul, et on a $\mathsf{Spec}(A) = \{(0), \mathfrak{m}\}$.

• Soit $\alpha \in \mathfrak{m}\backslash\{0\}$. Montrons qu'il existe $r \in \mathbf{N}_{>0}$ tel que $\mathfrak{m}^r \subset \alpha A$. Comme A est nœthérien, l'idéal $\mathfrak{m}$ est de type fini : il existe $f_1, \dots, f_n \in A\backslash\{0\}$ tels que $\mathfrak{m} = \sum_{i=1}^{n} f_i A$. Soit $i \in \{1, \dots, n\}$. D'après la proposition 1.3.10, on a $\mathsf{Spec}(A_{(f_i)}) = \{\mathfrak{p} \in \mathsf{Spec}(A),\ f_i \notin \mathfrak{p}\} = \{(0)\}$, ce qui montre que $A_{(f_i)}$ est un corps (et donc $A_{(f_i)} = \mathsf{Frac}(A)$). Il en résulte que α est inversible dans $A_{(f_i)}$: il existe $r_i \in \mathbf{N}$ et $a_i \in A$ tels que $\frac{1}{\alpha} = \frac{a_i}{f_i^{r_i}}$. On a bien sûr $r_i > 0$ (parce que $\alpha \notin A^\times$ vu que $\alpha \in \mathfrak{m}$). On a donc $f_i^{r_i} \in \alpha A$. Si $r = r_1 + \cdots + r_n \in \mathbf{N}_{>0}$, on a

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

ce qu'on voulait.

• Montrons que $\mathfrak{m}$ est principal. Soient $\alpha \in \mathfrak{m}\backslash\{0\}$ et $r \in \mathbf{N}_{>0}$ *minimal* tel que $\mathfrak{m}^r \subset \alpha A$: on a $\mathfrak{m}^{r-1} \not\subset \alpha A$. Soient donc $\beta \in \mathfrak{m}^{r-1}\backslash\alpha A$ et $\pi = \frac{\alpha}{\beta} \in \mathsf{Frac}(A)$. On a

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

et $\pi^{-1}\mathfrak{m}$ est un idéal de A. Si cet idéal était propre, on aurait $\pi^{-1}\mathfrak{m} \subset \mathfrak{m}$, ce qui impliquerait que π^{-1} est entier sur A (*cf* proposition 2.1.3 (iii) $\Rightarrow$ (i)). Comme A est intégralement clos, on aurait $\pi^{-1} \in A$ *i.e.* $\beta \in \alpha A$ ce qui n'est pas. On a donc nécessairement $\pi^{-1}\mathfrak{m} = A$ et donc $\mathfrak{m} = \pi A$ est principal.

• Montrons enfin que tout idéal de A est principal. Soit $I \subset A$ un idéal propre et non nul : on a $I \subseteq \mathfrak{m}$. Soit $\alpha \in I\backslash\{0\}$: on a $\alpha \in \mathfrak{m}\backslash\{0\}$, et d'après ce qu'on a vu plus haut, il existe $r \in \mathbf{N}_{>0}$ tel que $\mathfrak{m}^r \subset \alpha A \subset I$. Si on avait $I \subset \mathfrak{m}^{r+1}$, on aurait $\pi^r \in \pi^{r+1}A$, et donc $1 \in \pi A = \mathfrak{m}$ ce qui est absurde. L'ensemble $\{n \in \mathbf{N},\ I \subset \mathfrak{m}^n\}$ est donc majoré. Comme il est non vide (il contient 1), il a un plus grand élément n_I. On a $I \subset \pi^{n_I} A$ *i.e.* $\pi^{-n_I} I \subset A$ est un idéal de A, mais $\pi^{-n_I} I \not\subset \mathfrak{m}$ (sinon $I \subset \mathfrak{m}^{n_I+1}$), et donc $\pi^{-n_I} I = A$, soit $I = \pi^{n_I} A$. □

Théorème 3.2.3. Soit A un anneau intègre nœthérien qui n'est pas un corps. Alors A est de Dedekind si et seulement si pour tout idéal maximal $\mathfrak{m}$ de A, le localisé $A_\mathfrak{m}$ est de valuation discrète.

Démonstration. Si A est de Dedekind et $\mathfrak{m}$ est un idéal maximal de A, le localisé $A_\mathfrak{m}$ est local et de Dedekind (en vertu de la proposition 3.2.1). Comme A n'est pas un corps, $\mathfrak{m}$ est non nul, et $A_\mathfrak{m}$ n'est pas un corps : cela implique que $A_\mathfrak{m}$ est de valuation discrète (lemme 3.2.2).

Réciproquement, supposons que pour tout idéal maximal $\mathfrak{m}$ de A, le localisé $A_\mathfrak{m}$ soit de valuation discrète.

Soit $x \in K = \mathsf{Frac}(A)$ entier sur A. Écrivons $x = \frac{a}{b}$ avec $a, b \in A$ et $b \neq 0$. Pour tout $\mathfrak{m}$, l'élément x est *a fortiori* entier sur $A_\mathfrak{m}$. Ce dernier étant de Dedekind, on a $x \in A_\mathfrak{m}$, soit encore $aA_\mathfrak{m} \subset bA_\mathfrak{m}$. d'après le principe local-global (proposition 1.3.16), cela implique $aA \subseteq bA$, *i.e.* $x \in A$, ce qui prouve que A est intégralement clos.

Soit $\mathfrak{p} \subset A$ premier non nul. D'après le théorème de Krull (théorème 1.0.1), il existe un idéal maximal $\mathfrak{m} \subset A$ tel que $\mathfrak{p} \subset \mathfrak{m}$. D'après la proposition 1.3.10, l'idéal $\mathfrak{p}A_\mathfrak{m}$ est premier dans $A_\mathfrak{m}$. Étant non nul par hypothèse, il est maximal, *i.e.* $\mathfrak{p}A_\mathfrak{m} = \mathfrak{m}A_\mathfrak{m}$, ce qui implique que $\mathfrak{p} = \mathfrak{m}$ (en vertu de la proposition 1.3.16), et donc que $\mathfrak{p}$ est maximal. □

3.3. **Factorisation des idéaux, groupe des classes.** Le théorème 3.2.3 implique que les anneaux de Dedekind sont localement principaux, donc localement factoriels. Il existe cependant des anneaux de Dedekind non factoriels.

Exemple 3.3.1. Soit $K = \mathbf{Q}(i\sqrt{5})$: d'après la proposition 2.1.17, on a $\mathcal{O}_K = \mathbf{Z}[i\sqrt{5}]$. Supposons $2 = xy$ avec $x, y \in \mathcal{O}_K$: écrivons $x = a + ib\sqrt{5}$ et $y = c + id\sqrt{5}$. On a $\mathsf{N}_{K/\mathbf{Q}}(2) = \mathsf{N}_{K/\mathbf{Q}}(x)\,\mathsf{N}_{K/\mathbf{Q}}(y)$ *i.e.* $4 = (a^2 + 5b^2)(c^2 + 5d^2)$, ce qui implique $b = d = 0$ soit $x, y \in \mathbf{Z}$, et donc $x \in \{\pm 1\}$ ou $y \in \{\pm 1\}$. Il en résulte que 2 est irréductible dans $\mathcal{O}_K$. Cependant, on a $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6 \in 2\mathcal{O}_K$ mais $1 + i\sqrt{5}, 1 - i\sqrt{5} \notin 2\mathcal{O}_K$, *i.e.* 2 n'est pas premier. Cela implique que $\mathcal{O}_K$ (qui est de Dedekind) n'est pas factoriel (*cf* proposition 1.2.7).

Comme nous allons le voir, les anneaux de Dedekind ont néanmoins la propriété de factorisation, non plus des éléments non nuls en produit de facteurs premiers, mais des idéaux non nuls en produit d'idéaux premiers.

Lemme 3.3.2. Soient A un anneau nœthérien et $I \subset A$ un idéal non nul.
(1) L'idéal I contient un produit $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ d'idéaux premiers non nuls (non nécessairement distincts).
(2) Si A est de Dedekind, il n'existe qu'un nombre fini d'idéaux maximaux de A contenant I.

Démonstration. (1) On procède par « récurrence nœthérienne ». Soit $\mathscr{E}$ l'ensemble des idéaux non nuls qui ne contiennent pas un produit d'idéaux premiers non nuls. Supposons $\mathscr{E}$ non vide : il admet un élément I maximal pour l'inclusion (parce que A est nœthérien, *cf* proposition 1.1.4). On a bien sûr $I \neq A$ (parce que A contient au moins un idéal premier en vertu du théorème de Krull, *cf* théorème 1.0.1), et I lui-même n'est pas premier. Il existe donc $x, y \notin I$ tels que $xy \in I$. Les idéaux $I + xA$ et $I + yA$ contiennent I strictement : par maximalité de I dans $\mathscr{E}$, on a $I + xA, I + yA \notin \mathscr{E}$, ce qui implique l'existence de $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ et $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ premiers non nuls tels que $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset I + xA$ et $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subset I + yA$. On a alors

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m \subset (I + xA)(I + yA) \subset I$$

ce qui contredit $I \in \mathscr{E}$. Il en résulte que $\mathscr{E}$ est vide.
(2) D'après (1), il existe $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ des idéaux premiers non nuls (donc maximaux puisque A est de Dedekind) tels que $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset I$. Si $\mathfrak{m}$ est un idéal maximal de A tel que $I \subset \mathfrak{m}$, on a *a fortiori* $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{m}$. Si $\mathfrak{p}_i \neq \mathfrak{m}$ pour tout $i \in \{1, \ldots, n\}$, il existe $a_i \in \mathfrak{p}_i \backslash \mathfrak{m}$, et $a_1 \cdots a_n \in \mathfrak{p}_1 \cdots \mathfrak{p}_n \backslash \mathfrak{m}$ ce qui est absurde : il existe $i \in \{1, \ldots, n\}$ tel que $\mathfrak{p}_i = \mathfrak{m}$. □

Théorème 3.3.3. Soient A un anneau de Dedekind et $I \subset A$ un idéal non nul. Alors il existe des idéaux premiers non nuls deux à deux distincts $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ et des entiers $\alpha_1, \ldots, \alpha_n \in \mathbf{N}_{>0}$ tels que

$$I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n}$$

Cette décomposition est unique à l'ordre des facteurs près, et l'ensemble des idéaux premiers contenant I est précisément $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Démonstration. L'énoncé est trivial si A est un corps : supposons désormais que A n'en est pas un. Soit $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ l'ensemble des idéaux premiers contenant I (*cf* lemme 3.3.2 (2)). Pour $i \in \{1, \ldots, n\}$, on dispose de l'idéal $IA_{\mathfrak{p}_i}$ dans l'anneau de valuation discrète $A_{\mathfrak{p}_i}$ (*cf* théorème 3.2.3). Cet idéal est strict : il existe $\alpha_i \in \mathbf{N}_{>0}$ tel que $IA_{\mathfrak{p}_i} = \mathfrak{p}_i^{\alpha_i} A_{\mathfrak{p}_i}$. Posons $J = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n}$. Par construction, on a $IA_{\mathfrak{p}_i} = JA_{\mathfrak{p}_i}$ pour tout $i \in \{1, \ldots, n\}$. Par ailleurs, si $\mathfrak{m}$ est un idéal maximal n'appartenant pas à $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, on a $IA_{\mathfrak{m}} = A_{\mathfrak{m}} = JA_{\mathfrak{m}}$. Le principe local-global (proposition 1.3.16) implique donc que $I = J$, ce qu'on voulait.
Reste à prouver l'unicité à l'ordre près. Supposons $I = \mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_m^{\beta_m}$ avec $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ maximaux distincts et $\beta_1, \ldots, \beta_m \in \mathbf{N}_{>0}$. Pour $i \in \{1, \ldots, n\}$, on a $\mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_m^{\beta_m} \subset \mathfrak{p}_i$: il existe $j \in \{1, \ldots, m\}$ tel que $\mathfrak{p}_i = \mathfrak{q}_j$. Cela implique $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$. En échangeant les deux factorisations, on a l'inclusion inverse : on a $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$, donc $m = n$, et quitte à renuméroter, $\mathfrak{p}_i = \mathfrak{q}_i$ pour tout $i \in \{1, \ldots, n\}$. Enfin, on a $\mathfrak{p}_i^{\beta_i} A_{\mathfrak{p}_i} = IA_{\mathfrak{p}_i} = \mathfrak{p}_i^{\alpha_i} A_{\mathfrak{p}_i}$, ce qui implique $\alpha_i = \beta_i$ pour tout $i \in \{1, \ldots, n\}$. □

Remarque 3.3.4. Une autre façon de formuler l'unicité est de dire que les idéaux $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ qui apparaissent dans la factorisation sont précisément les idéaux maximaux qui contiennent I, et que pour tout $i \in \{1, \ldots, n\}$, la multiplicité α_i est la valuation de l'idéal $IA_{\mathfrak{p}_i}$ dans l'anneau de valuation $A_{\mathfrak{p}_i}$.

Exercice 3.3.5. Un anneau de Dedekind factoriel est principal [4].

Exemple 3.3.6. On reprend les notations de l'exemple 3.3.1. On a l'isomorphisme

$$\begin{aligned} \mathbf{Z}[X]/(X^2 + 5)\,\mathbf{Z}[X] &\xrightarrow{\sim} \mathcal{O}_K \\ X &\mapsto i\sqrt{5} \end{aligned}$$

4. Soient A de Dedekind et factoriel, et $\mathfrak{p} \subset A$ un idéal premier non nul. Soit $a \in \mathfrak{p} \backslash \{0\}$: comme A est factoriel, on a $a = p_1 \cdots p_n$ avec $p_1, \ldots, p_n$ premiers. Comme $a \in \mathfrak{p}$ et $\mathfrak{p}$ est premier, il existe $i \in \{1, \ldots, n\}$ tel que $p_i \in \mathfrak{p}$, de sorte que $p_i A \subset \mathfrak{p}$. Mais $p_i A$ est premier non nul et A de Dedekind (donc de dimension 1), on a nécessairement $\mathfrak{p} = p_i A$. Comme tous les idéaux premiers non nuls sont principaux, il en est de même de tous les idéaux en vertu du théorème 3.3.3, et A est principal.

Il induit un isomorphisme $\mathbf{F}_2[X]/(1+X)^2\,\mathbf{F}_2[X] \xrightarrow{\sim} \mathcal{O}_K/2\mathcal{O}_K$: notons $\mathfrak{p}$ l'idéal engendré par 2 et $\theta := 1 + i\sqrt{5}$ (c'est l'image par l'isomorphisme qui précède de l'idéal maximal $(1+X)$ de $\mathbf{F}_2[X]/(1+X)^2\,\mathbf{F}_2[X]$). L'isomorphisme induit est un isomorphisme $\mathcal{O}_K/\mathfrak{p} \xrightarrow{\sim} \mathbf{F}_2$, de sorte que $\mathfrak{p}$ est maximal. Par ailleurs, l'image de $\mathfrak{p}^2$ dans $\mathcal{O}_K/2\mathcal{O}_K$ est nulle : on a $\mathfrak{p}^2 \subset 2\mathcal{O}_K \subset \mathfrak{p}$. Comme $2\mathcal{O}_K$ n'est pas premier, on a $2\mathcal{O}_K \neq \mathfrak{p}$, ce qui montre que $2\mathcal{O}_K = \mathfrak{p}^2$.

Définition 3.3.7. Soient A un anneau intègre et K son corps des fractions.

(1) Un **idéal fractionnaire** est un sous-A-module $I \subseteq K$ tel qu'il existe $d \in A\backslash\{0\}$ avec $I \subseteq d^{-1}A$.

(2) Opérations sur les idéaux fractionnaires. Soient $I, J \subseteq K$ des idéaux fractionnaires : il existe $d, \delta \in A\backslash\{0\}$ tels que $I \subseteq d^{-1}A$ et $J \subseteq \delta^{-1}A$. On note $I + J$ (resp. IJ) le sous-A-module de K engendré par $I \cup J$ (resp. les éléments de la forme [a] xy avec $x \in I$ et $y \in J$). Alors $IJ \subseteq (d\delta)^{-1}A$ et $I \cap J \subseteq I + J \subseteq (d\delta)^{-1}A$ de sorte que IJ, $I \cap J$ et $I + J$ sont des idéaux fractionnaires.

(3) Si $I \subseteq K$ est un idéal fractionnaire, on pose
$$I^{-1} = \{x \in K,\ xI \subseteq A\}$$
c'est un sous-A-module de K. Si $I \neq \{0\}$, alors I^{-1} est fractionnaire (si $a \in I\backslash\{0\}$, on a $aI^{-1} \subseteq A$, de sorte que $I^{-1} \subseteq a^{-1}A$).

(4) Un idéal fractionnaire non nul $I \subseteq K$ est dit **inversible** si l'inclusion $II^{-1} \subseteq A$ est une égalité.

a. On a donc $IJ = \Big\{x \in K,\ (\exists n \in \mathbf{N})\ (\exists x_1, \dots, x_n \in I)\ (\exists y_1, \dots, y_n \in J)\ x = \sum_{k=1}^{n} x_k y_k\Big\}$.

Remarque 3.3.8. (1) Un idéal fractionnaire n'est autre qu'une partie de la forme $d^{-1}\mathfrak{a}$ où $\mathfrak{a} \subseteq A$ est un idéal de A et $d \in A\backslash\{0\}$. En particulier, tout idéal de A est un idéal fractionnaire. De même, pour tout $x \in K^\times$, l'ensemble xA est un idéal fractionnaire. Un tel idéal fractionnaire est dit **principal**. Un idéal fractionnaire principal est inversible, et $(xA)^{-1} = x^{-1}A$.

(2) Si $I \subset J \subset K$ sont des idéaux fractionnaires, on a $J^{-1} \subset I^{-1}$. En particulier, si $I \subset A$, on a $A \subset I^{-1}$.

(3) Si $I, J \subset K$ sont des idéaux fractionnaires non nuls inversibles, il en est de même du produit IJ, et $(IJ)^{-1} = I^{-1}J^{-1}$.

Corollaire 3.3.9. Dans un anneau de Dedekind, tout idéal fractionnaire non nul est inversible.

Démonstration. Soient A un anneau de Dedekind, K son corps des fractions et $I \subset K$ un idéal fractionnaire non nul. Commençons par le cas où $I \subset A$ est un idéal de A. Soit $x \in I\backslash\{0\} \subset A\backslash\{0\}$. D'après le théorème 3.3.3, il existe $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ maximaux dans A et $\alpha_1, \dots, \alpha_n \in \mathbf{N}_{>0}$ tels que $xA = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n}$. Comme $xA \subset I$, on a nécessairement $I = \mathfrak{p}_1^{\beta_1} \cdots \mathfrak{p}_n^{\beta_n}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout $i \in \{1, \dots, n\}$. Posons alors $J = \mathfrak{p}_1^{\alpha_1-\beta_1} \cdots \mathfrak{p}_n^{\alpha_n-\beta_n} \subset A$: on a $IJ = xA$, et donc $I(x^{-1}J) = A$, ce qui prouve de I est inversible et $I^{-1} = x^{-1}J$. Dans le cas général, on a $I = d^{-1}\mathfrak{a}$ avec $d \in A\backslash\{0\}$ et $\mathfrak{a} \subset A$. D'après ce qui précède, l'idéal $\mathfrak{a}$ est inversible : on a $\mathfrak{a}\mathfrak{a}^{-1} = A$, donc $I(d\mathfrak{a}^{-1}) = A$, de sorte que I est inversible, d'inverse $d\mathfrak{a}^{-1}$. □

Théorème 3.3.10. Soient A un anneau de Dedekind, $\mathscr{P}_A$ l'ensemble de ses idéaux premiers non nuls et K son corps des fractions. Si $I \subseteq K$ est un idéal fractionnaire non nul, il existe une unique famille $\big(v_\mathfrak{p}(I)\big)_{\mathfrak{p} \in \mathscr{P}_A} \in \mathbf{Z}^{(\mathscr{P}_A)}$ telle que
$$I = \prod_{\mathfrak{p} \in \mathscr{P}_A} \mathfrak{p}^{v_\mathfrak{p}(I)}$$
(le produit est fini vu qu'il n'y a qu'un nombre fini de $v_\mathfrak{p}(I)$ non nuls).

Démonstration. Il existe un idéal $\mathfrak{a} \subseteq A$ non nul et $d \in A\backslash\{0\}$ tels que $I = d^{-1}\mathfrak{a}$. En appliquant le théorème 3.3.3 aux idéaux $\mathfrak{a}, dA \subseteq A$, on en déduit l'existence de l'écriture. Pour l'unicité,

supposons que

$$\prod_{\mathfrak{p}\in\mathscr{P}_A}\mathfrak{p}^{n_\mathfrak{p}}=\prod_{\mathfrak{p}\in\mathscr{P}_A}\mathfrak{p}^{m_\mathfrak{p}}$$

avec $(n_\mathfrak{p})_{\mathfrak{p}\in\mathscr{P}_A},(m_\mathfrak{p})_{\mathfrak{p}\in\mathscr{P}_A}\in\mathbf{Z}^{(\mathscr{P}_A)}$. On a alors $\prod_{\mathfrak{p}\in\mathscr{P}_A}\mathfrak{p}^{n_\mathfrak{p}-m_\mathfrak{p}}=A$, soit encore

$$\prod_{\substack{\mathfrak{p}\in\mathscr{P}_A\\ n_\mathfrak{p}-m_\mathfrak{p}\geqslant 0}}\mathfrak{p}^{n_\mathfrak{p}-m_\mathfrak{p}}=\prod_{\substack{\mathfrak{p}\in\mathscr{P}_A\\ n_\mathfrak{p}-m_\mathfrak{p}<0}}\mathfrak{p}^{-n_\mathfrak{p}+m_\mathfrak{p}}\subseteq A$$

par unicité dans le théorème 3.3.3, cela implique $n_\mathfrak{p}-m_\mathfrak{p}=0$ *i.e.* $n_\mathfrak{p}=m_\mathfrak{p}$ pour tout $\mathfrak{p}\in\mathscr{P}_A$ (notons que les ensembles $\{\mathfrak{p}\in\mathscr{P}_A,\ n_\mathfrak{p}-m_\mathfrak{p}\geqslant 0\}$ et $\{\mathfrak{p}\in\mathscr{P}_A,\ n_\mathfrak{p}-m_\mathfrak{p}<0\}$ sont disjoints). □

Notation. Si A est un anneau intègre, on note $\mathsf{Fr}(A)$ l'ensemble de ses idéaux fractionnaires non nuls, et $\mathsf{Pr}(A)$ l'ensemble de ses idéaux fractionnaires principaux non nuls. On a $\mathsf{Pr}(A)\subseteq\mathsf{Fr}(A)$.

Proposition 3.3.11. Soit A un anneau de Dedekind et $\mathscr{P}_A$ l'ensemble de ses idéaux premiers non nuls.

(1) Muni de la loi $(I,J)\mapsto IJ$, l'ensemble $\mathsf{Fr}(A)$ est un groupe abélien d'élément unité l'idéal A et d'inverse $I\mapsto I^{-1}$. En outre, l'application

$$f_A\colon \mathbf{Z}^{(\mathscr{P}_A)}\to\mathsf{Fr}(A)$$
$$(n_\mathfrak{p})_{\mathfrak{p}\in\mathscr{P}_A}\mapsto\prod_{\mathfrak{p}\in\mathscr{P}_A}\mathfrak{p}^{n_\mathfrak{p}}$$

est un isomorphisme de groupes, d'inverse $I\mapsto\big(v_\mathfrak{p}(I)\big)_{\mathfrak{p}\in\mathscr{P}_A}$. En particulier, on a

$$v_\mathfrak{p}(IJ)=v_\mathfrak{p}(I)+v_\mathfrak{p}(J)$$
$$v_\mathfrak{p}(I^{-1})=-v_\mathfrak{p}(I)$$

pour tout $I,J\in\mathrm{Fr}(A)$ et $\mathfrak{p}\in\mathscr{P}_A$.

(2) Si $I,J\in\mathsf{Fr}(A)$, on a $I\subseteq J\Leftrightarrow(\forall\mathfrak{p}\in\mathscr{P}_A)\ v_\mathfrak{p}(I)\geqslant v_\mathfrak{p}(J)$. En particulier I est un idéal de A si et seulement si $v_\mathfrak{p}(I)\geqslant 0$ pour tout $\mathfrak{p}\in\mathscr{P}_A$.

Démonstration. (1) Rappelons que d'après la définition 3.3.7, si $I,J\in\mathsf{Fr}(A)$, alors $IJ\in\mathsf{Fr}(A)$ et $I^{-1}\in\mathsf{Fr}(A)$. La loi $(I,J)\mapsto IJ$ est associative, commutative et admet A comme élément neutre. Par ailleurs, tout élément est inversible d'après le corollaire 3.3.9 : $\mathsf{Fr}(A)$ est un groupe abélien. L'application f_A est un morphisme de groupes, d'inverse $I\mapsto\big(v_\mathfrak{p}(I)\big)_{\mathfrak{p}\in\mathscr{P}_A}$ (théorème 3.3.10) : c'est donc un isomorphisme.
(2) D'après le théorème 3.3.3, si $I\subseteq A$ est un idéal, on a $v_\mathfrak{p}(I)\geqslant 0$ pour tout $\mathfrak{p}\in\mathscr{P}_A$. La réciproque est évidente. Si $I,J\in\mathsf{Fr}(A)$, on a donc $I\subseteq J\Leftrightarrow IJ^{-1}\subset A\Leftrightarrow(\forall\mathfrak{p}\in\mathscr{P}_A)\ v_\mathfrak{p}(I)-v_\mathfrak{p}(J)=v_\mathfrak{p}(IJ^{-1})\geqslant 0$. □

Définition 3.3.12. Soit A un anneau de Dedekind. L'ensemble $\mathsf{Pr}(A)$ est un sous-groupe de $\mathsf{Fr}(A)$. On note

$$\mathsf{Cl}(A)=\mathsf{Fr}(A)/\mathsf{Pr}(A)$$

le groupe quotient, qu'on appelle le **groupe des classes d'idéaux** de A.

Exemple 3.3.13. Soit A un anneau de Dedekind.

(1) L'anneau A est principal si et seulement si $\mathsf{Cl}(A)=\{1\}$.
(2) Soit I un idéal fractionnaire. Alors la classe de I dans $\mathsf{Cl}(A)$ est d'ordre fini si et seulement s'il existe $n\in\mathbf{N}_{>0}$ tel que I^n soit principal.

3.4. **Théorème chinois.** Soit A un anneau.

Définition 3.4.1. Deux idéaux $I,J\subset A$ sont dits **premiers entre eux** lorsque $I+J=A$. On dit aussi que I est premier à J.

Proposition 3.4.2. (1) Deux idéaux maximaux distincts sont premiers entre eux.
(2) Si $I_1, \dots, I_n$ sont premiers à J, alors $I_1 \cdots I_n$ est premier à J.
(3) Si $I, J \subset A$ sont premiers entre eux et $n, m \in \mathbf{N}_{>0}$, alors I^n et J^m sont premiers entre eux.

Démonstration. (1) On a $I \subsetneq I + J \subset A$, donc $I + J = A$.
(2) Comme $I_k + J = A$ pour tout $k \in \{1, \dots, n\}$, on a $(I_1 + J)(I_2 + J) \cdots (I_n + J) = A$. Comme $(I_1 + J)(I_2 + J) \cdots (I_n + J) \subset I_1 \cdots I_n + J$, on a bien $I_1 \cdots I_n + J = A$.
(3) Appliqué à $I_k = I$ pour tout $k \in \{1, \dots, n\}$, le point (2) implique que I^n et J sont premiers entre eux. En remplaçant I par J et J par I^n, on en déduit de même que I^n et J^m sont premiers entre eux. □

Théorème 3.4.3. (des restes chinois). Soient A un anneau et $I_1, \dots, I_n \subset A$ des idéaux deux à deux premiers entre eux (*i.e.* tels que $i \neq j \Rightarrow I_i + I_j = A$). Alors :
(1) $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$;
(2) l'homomorphisme canonique d'anneaux

$$A/I_1 I_2 \cdots I_n \to \prod_{k=1}^{n} A/I_k$$

est un isomorphisme.

Démonstration. D'après la proposition 3.4.2, il suffit de traiter le cas $n = 2$: soient I et J deux idéaux premiers entre eux : il existe $e_I \in I$ et $e_J \in J$ tels que $e_I + e_J = 1$.
(1) On a toujours $IJ \subset I \cap J$. Soit $a \in I \cap J$, on a $a = a(e_I + e_J) = ae_I + ae_J$. Comme $a \in J$ et $e_I \in I$, on a $ae_I \in IJ$. De même $ae_J \in IJ$, d'où $a \in IJ$, ce qui prouve l'égalité.
(2) Considérons l'application naturelle $\varphi\colon A \to (A/I) \times (A/J)$. Si $x, y \in A$, on a $\varphi(xe_J + ye_I) = (x + I, y + J)$, ce qui montre que φ est surjective. Comme $\mathsf{Ker}(\varphi) = I \cap J = IJ$, elle induit donc l'isomorphisme $A/IJ \xrightarrow{\sim} (A/I) \times (A/J)$. □

Définition 3.4.4. Un anneau est dit **semi-local** s'il n'a qu'un nombre fini d'idéaux maximaux.

Remarque 3.4.5. Bien entendu, un anneau local est semi-local.

Exercice 3.4.6. Soient A un anneau de Dedekind et $I \subset A$ un idéal non nul. Alors A/I est est semi-local [5].

Proposition 3.4.7. Soient A un anneau de Dedekind, $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset A$ des idéaux maximaux et $I \subset A$ un idéal. Alors il existe $a \in A$ tel que $(\forall i \in \{1, \dots, n\})\, IA_{\mathfrak{p}_i} = aA_{\mathfrak{p}_i}$. En particulier, un anneau de Dedekind semi-local est principal.

Démonstration. C'est évident si A est un corps : supposons désormais que A n'est pas un corps. On a $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n} J$ avec $\alpha_1, \dots, \alpha_n \in \mathbf{N}$ et J premier à $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ (théorème 3.3.3). D'après le lemme 3.2.2, pour tout $i \in \{1, \dots, n\}$, l'anneau $A_{\mathfrak{p}_i}$ est de valuation discrète : soit $\pi_i \in \mathfrak{p}_i$ tel que $\mathfrak{p}_i A_{\mathfrak{p}_i} = \pi_i A_{\mathfrak{p}_i}$. On a alors $IA_{\mathfrak{p}_i} = \pi_i^{\alpha_i} A_{\mathfrak{p}_i}$ pour tout $i \in \{1, \dots, n\}$. Comme $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ sont deux à deux premiers entre eux, il en est de même de $\mathfrak{p}_1^{\alpha_1+1}, \dots, \mathfrak{p}_n^{\alpha_n+1}$: d'après le théorème des restes chinois (*cf* théorème 3.4.3), le morphisme naturel

$$A/\mathfrak{p}_1^{\alpha_1+1} \cdots \mathfrak{p}_n^{\alpha_n+1} \to (A/\mathfrak{p}_1^{\alpha_1+1}) \times \cdots \times (A/\mathfrak{p}_n^{\alpha_n+1})$$

est un isomorphisme : il existe $a \in A$ tel que $a \equiv \pi_i^{\alpha_i} \mod \mathfrak{p}_i^{\alpha_i+1}$ donc $aA_{\mathfrak{p}_i} = IA_{\mathfrak{p}_i}$ pour tout $i \in \{1, \dots, n\}$.
Si A est semi-local, on prend pour $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ l'ensemble des idéaux maximaux de A. D'après le principe local-global (proposition 1.3.16), on a $I = aA$. Comme A est intègre par définition, il est principal. □

5. Soit $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$ la décompositon de I en produit d'idéaux premiers non nuls. D'après le théorème chinois, on a $A/I \simeq \bigoplus_{i=1}^{r} A/\mathfrak{p}_i^{\alpha_i}$. L'anneau $A/\mathfrak{p}_i^{\alpha_i}$ est local, d'idéal maximal $\mathfrak{p}_i/\mathfrak{p}_i^{\alpha_i}$: l'anneau A/I est semi-local

Corollaire 3.4.8. Soient A un anneau de Dedekind, $I \subset A$ un idéal non nul et $a \in I\backslash\{0\}$. Alors il existe $b \in A$ tel que $I = aA + bA$.

Démonstration. Soient $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset A$ les idéaux maximaux contenant a (lemme 3.3.2 (2)). D'après la proposition 3.4.7, il existe $b \in A$ tel que $(\forall i \in \{1, \dots, n\})\, IA_{\mathfrak{p}_i} = bA_{\mathfrak{p}_i}$. Posons $J = aA + bA \subset A$. Si $\mathfrak{p}$ est un idéal maximal ne contenant pas a, on a $aA_{\mathfrak{p}} = A_{\mathfrak{p}}$: comme $a \in I$ et $a \in J$, cela implique $IA_{\mathfrak{p}} = JA_{\mathfrak{p}} = A_{\mathfrak{p}}$. Si $i \in \{1, \dots, n\}$, on a $aA_{\mathfrak{p}_i} \subset IA_{\mathfrak{p}_i}$, donc $IA_{\mathfrak{p}_i} = bA_{\mathfrak{p}_i} \subset JA_{\mathfrak{p}_i} \subset IA_{\mathfrak{p}_i}$, et donc $JA_{\mathfrak{p}_i} = IA_{\mathfrak{p}_i}$. Il résulte du principe local-global (proposition 1.3.16) que $I = J$. □

3.5. **Factorisation dans une extension, ramification.** Soient A un anneau de Dedekind et $K = \mathsf{Frac}(A)$. Le but de cette section est de comprendre la décomposition de l'idéal engendré par un idéal de A dans la clôture intégrale de A dans une extension finie séparable de K.

Notation. Si $\mathfrak{p}$ est un idéal maximal de A, on pose $k(\mathfrak{p}) = A/\mathfrak{p}$. On l'appelle le **corps résiduel de A en $\mathfrak{p}$**.

Définition 3.5.1. Soient A un anneau de Dedekind, et L/K une extension finie séparable de corps. On note B la clôture intégrale de A dans L. D'après le corollaire 2.4.6 (1) et le théorème 3.1.4, B est une A-algèbre finie et un anneau de Dedekind.

(1) Si $\mathfrak{p} \subset A$ et $\mathfrak{P} \subset B$ sont des idéaux premiers non nuls, on dit que $\mathfrak{P}$ **divise** $\mathfrak{p}$, ou que $\mathfrak{P}$ est **au-dessus** de $\mathfrak{p}$ (et on note $\mathfrak{p} \mid \mathfrak{P}$) si $\mathfrak{P} \cap A = \mathfrak{p}$.

(2) Comme B est de Dedekind, on a
$$\mathfrak{p}B = \prod_{\mathfrak{P}\mid\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$$
avec $e_{\mathfrak{P}} = v_{\mathfrak{P}}(\mathfrak{p}B) \in \mathbf{N}_{>0}$. L'entier $e_{\mathfrak{P}}$ s'appelle l'**indice de ramification** de $\mathfrak{p}$ en $\mathfrak{P}$.

(3) Si $\mathfrak{P} \mid \mathfrak{p}$, le corps $k(\mathfrak{P}) = B/\mathfrak{P}$ est une extension finie de $k(\mathfrak{p}) = A/\mathfrak{p}$: on l'appelle l'**extension résiduelle** en $\mathfrak{P}$. On pose $f_{\mathfrak{P}} = \big[k(\mathfrak{P}) : k(\mathfrak{p})\big]$. L'entier $f_{\mathfrak{P}}$ s'appelle le degré résiduel de $\mathfrak{p}$ en $\mathfrak{P}$.

(4) Si $e_{\mathfrak{P}} = 1$ et l'extension $k(\mathfrak{P})/k(\mathfrak{p})$ est séparable, on dit que $\mathfrak{p}$ (ou même L/K) est **non-ramifié** en $\mathfrak{P}$. On dit que $\mathfrak{p}$ est **ramifié** en $\mathfrak{P}$ dans le cas contraire. Si $\mathfrak{p}$ est non-ramifié en tous les idéaux premiers le divisant, on dit que $\mathfrak{p}$ est **non-ramifié**, ou que L/K est non ramifiée en $\mathfrak{p}$.

(5) Lorsqu'il n'y a qu'un seul idéal premier $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ et que $f_{\mathfrak{P}} = 1$, on dit que L/K est **totalement ramifiée** en $\mathfrak{p}$.

(6) Si l'idéal $\mathfrak{p}B$ est premier dans B, on dit que $\mathfrak{p}$ est **inerte** dans L/K. Si $e_{\mathfrak{P}} = f_{\mathfrak{P}} = 1$ pour tout $\mathfrak{P} \mid \mathfrak{p}$, on dit que $\mathfrak{p}$ est **totalement décomposé** dans L/K.

Théorème 3.5.2. Sous les hypothèses de la définition 3.5.1, on a
$$\dim_{k(\mathfrak{p})}(B/\mathfrak{p}B) = [L : K] = \sum_{\mathfrak{P}\mid\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}$$

Démonstration. On suppose que A n'est pas un corps (sinon c'est trivial). On a les isomorphismes $A/\mathfrak{p} \xrightarrow{\sim} A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ et $B/\mathfrak{p}B \xrightarrow{\sim} S^{-1}B/\mathfrak{p}S^{-1}B$ (avec $S = A\backslash\mathfrak{p}$) : quitte à remplacer A par $A_{\mathfrak{p}}$ (ce qui est licite en vertu de la proposition 2.1.13), on peut supposer A de valuation discrète, d'idéal maximal $\mathfrak{p}$ (*cf* lemme 3.2.2). L'anneau A est alors principal : le A-module B est donc libre de rang $[L : K]$ (*cf* corollaire 2.4.6 (2)). Il en résulte que $\dim_{k(\mathfrak{p})}(B/\mathfrak{p}B) = [L : K]$.

Pour $\mathfrak{P} \mid \mathfrak{p}$, les idéaux $\mathfrak{P}^{e_{\mathfrak{P}}}$ sont deux à deux premiers entre eux. D'après le lemme chinois, on a donc
$$B/\mathfrak{p}B = B/\prod_{\mathfrak{P}\mid\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}} \xrightarrow{\sim} \bigoplus_{\mathfrak{P}\mid\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}$$

Considérons la filtration $\mathfrak{P}^{e_{\mathfrak{P}}} \subsetneq \mathfrak{P}^{e_{\mathfrak{P}}-1} \subsetneq \cdots \subsetneq \mathfrak{P}^2 \subsetneq \mathfrak{P} \subsetneq B$. Comme $B_{\mathfrak{P}}$ est de valuation discrète (lemme 3.2.2), on a les isomorphismes $B_{\mathfrak{P}}/\mathfrak{P}B_{\mathfrak{P}} \xrightarrow{\sim} \mathfrak{P}^k B_{\mathfrak{P}}/\mathfrak{P}^{k+1}B_{\mathfrak{P}} \xleftarrow{\sim} \mathfrak{P}^k/\mathfrak{P}^{k+1}$ (le premier isomorphisme est induit par la multiplication par $\pi_{\mathfrak{P}}^k$, où $\pi_{\mathfrak{P}}$ est une uniformisante de $B_{\mathfrak{P}}$). Il en résulte que $\mathfrak{P}^k/\mathfrak{P}^{k+1}$ est un $k(\mathfrak{P})$-espace vectoriel de dimension 1, donc un $k(\mathfrak{p})$-espace vectoriel

de dimension $f_{\mathfrak{P}}$. Ainsi,

$$\dim_{k(\mathfrak{p})}(B/\mathfrak{P}^{e_{\mathfrak{P}}}) = \sum_{k=0}^{e_{\mathfrak{P}}-1} \dim_{k(\mathfrak{p})}(\mathfrak{P}^k/\mathfrak{P}^{k+1}) = e_{\mathfrak{P}} f_{\mathfrak{P}}$$

et donc

$$\dim_{k(\mathfrak{p})}(B/\mathfrak{p}B) = \sum_{\mathfrak{P}|\mathfrak{p}} \dim_{k(\mathfrak{p})}(B/\mathfrak{P}^{e_{\mathfrak{P}}}) = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}$$

□

Lemme 3.5.3. (d'évitement des idéaux premiers). Soient R un anneau, $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset R$ des idéaux premiers et $I \subset \bigcup_{i=1}^{n} \mathfrak{p}_i$ un idéal. Alors il existe $i \in \{1, \dots, n\}$ tel que $I \subset \mathfrak{p}_i$.

Démonstration. Quitte à supprimer ceux des $\mathfrak{p}_i$ qui n'apportent rien à la réunion, on peut supposer que $(\forall i \in \{1, \dots, n\})\, \mathfrak{p}_i \not\subset \bigcup_{j \neq i} \mathfrak{p}_j$: soit alors $a_i \in \mathfrak{p}_i \setminus \bigcup_{j \neq i} \mathfrak{p}_j$. Supposons en outre que pour tout $i \in \{1, \dots, n\}$, on a $I \not\subset \mathfrak{p}_i$: soit $x_i \in I \setminus \mathfrak{p}_i$. Posons alors $x = \sum_{i=1}^{n} x_i \prod_{j \neq i} a_j \in I$. Si $i \in \{1, \dots, n\}$, on a $a_i \in \mathfrak{p}_i$ donc $x \equiv x_i \prod_{j \neq i} a_j \mod \mathfrak{p}_i$. Comme $x_i \notin \mathfrak{p}_i$ et $a_j \notin \mathfrak{p}_i$ pour $j \neq i$, on a $x_i \prod_{j \neq i} a_j \notin \mathfrak{p}_i$ et donc $x \notin \mathfrak{p}_i$, de sorte que $x \in I \setminus \bigcup_{i=1}^{n} \mathfrak{p}_i$: cela contredit l'hypothèse. □

Remarque 3.5.4. La terminologie provient de la contraposée.

Théorème 3.5.5. Sous les hypothèses du théorème 3.5.2, supposons en outre l'extension L/K galoisienne. Le groupe $\mathsf{Gal}(L/K)$ agit transitivement sur l'ensemble des idéaux premiers divisant $\mathfrak{p}$. Les entiers $e_{\mathfrak{P}}$ et $f_{\mathfrak{P}}$ ne dépendent que de $\mathfrak{p}$ et pas de $\mathfrak{P}$: on les note $e_{\mathfrak{p}}$ et $f_{\mathfrak{p}}$ respectivement. Si $\mathsf{Gal}(L/K)_{\mathfrak{P}}$ désigne le stabilisateur de $\mathfrak{P}$, alors $\mathsf{Gal}(L/K)_{\sigma(\mathfrak{P})} = \sigma\, \mathsf{Gal}(L/K)_{\mathfrak{P}} \sigma^{-1}$ pour tout $\sigma \in \mathsf{Gal}(L/K)$: l'entier $g_{\mathfrak{p}} = \left[\mathsf{Gal}(L/K) : \mathsf{Gal}(L/K)_{\mathfrak{P}}\right]$ ne dépend que de $\mathfrak{p}$ et pas de $\mathfrak{P}$. On a $[L : K] = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$.

Démonstration. Soient $\mathfrak{P}$ et $\mathfrak{P}'$ deux idéaux premiers au-dessus de $\mathfrak{p}$ tels que $\mathfrak{P}' \neq \sigma(\mathfrak{P})$ pour tout $\sigma \in \mathsf{Gal}(L/K)$. Comme les idéaux $\mathfrak{P}'$ et $\sigma(\mathfrak{P})$ sont maximaux, on a donc $\mathfrak{P}' \not\subset \sigma(\mathfrak{P})$ pour tout $\sigma \in \mathsf{Gal}(L/K)$. D'après le lemme d'évitement des idéaux premiers, il existe $x \in \mathfrak{P}'$ tel que $x \notin \sigma(\mathfrak{P})$ pour tout $\sigma \in \mathsf{Gal}(L/K)$. Cela implique que $y = \mathsf{N}_{L/K}(x) = \prod_{\sigma \in \mathsf{Gal}(L/K)} \sigma(x) \notin \mathfrak{P}$. Mais cela contredit le fait que $y \in A \cap \mathfrak{P}' = \mathfrak{p} \subseteq \mathfrak{P}$. L'action de $\mathsf{Gal}(L/K)$ sur l'ensemble des idéaux premiers divisant $\mathfrak{p}$ est donc transitive. Il en résulte que les entiers $e_{\mathfrak{P}}$ et $f_{\mathfrak{P}}$ ne dépendent que de $\mathfrak{p}$ et pas de $\mathfrak{P}$. Il en résulte que $\mathsf{Gal}(L/K)_{\sigma(\mathfrak{P})} = \sigma\, \mathsf{Gal}(L/K)_{\mathfrak{P}} \sigma^{-1}$ pour tout $\sigma \in \mathsf{Gal}(L/K)$. En outre, on a $\#\{\mathfrak{P} \in \mathsf{Spec}(B),\ \mathfrak{P} \mid \mathfrak{p}\} = \left[\mathsf{Gal}(L/K) : \mathsf{Gal}(L/K)_{\mathfrak{P}}\right] = g_{\mathfrak{p}}$: on en déduit que

$$[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}} = \#\{\mathfrak{P} \in \mathsf{Spec}(B),\ \mathfrak{P} \mid \mathfrak{p}\} e_{\mathfrak{p}} f_{\mathfrak{p}} = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$$

grâce à la proposition 3.5.2. □

Proposition 3.5.6. (le cas monogène). Sous les hypothèses du théorème 3.5.2, supposons $B = A[\theta]$. Soit $F \in A[X]$ le polynôme minimal de θ sur K. Pour $\mathfrak{p}$ idéal maximal de A, la factorisation de la réduction $\overline{F}$ de F dans $k(\mathfrak{p})[X]$ s'écrit :

$$\overline{F}(X) = \prod_{i=1}^{s} f_i(X)^{r_i}$$

avec $f_1, \dots, f_s$ irréductibles deux à deux premiers entre eux. Alors la décomposition de $\mathfrak{p}B$ est

$$\mathfrak{p}B = \prod_{i=1}^{s} \mathfrak{P}_i^{r_i}$$

avec $\mathfrak{P}_i = \mathfrak{p}B + F_i(\theta)B$ (où $F_i \in A[X]$ désigne un relèvement quelconque de f_i). En outre, on a $B/\mathfrak{P}_i \simeq k(\mathfrak{p})[X]/(f_i(X))$.

Démonstration. Par hypothèse, on a l'isomorphisme

$$\begin{aligned} A[X]/(F(X)) &\xrightarrow{\sim} B \\ X &\mapsto \theta \end{aligned}$$

Il induit les isomorphismes $k(\mathfrak{p})[X]/(\overline{F}(X)) \xrightarrow{\sim} B/\mathfrak{p}B$ et donc $k(\mathfrak{p})[X]/(f_i(X)) \xrightarrow{\sim} B/\mathfrak{P}_i$ pour tout $i \in \{1,\dots,s\}$. Cela prouve déjà que $\mathfrak{P}_i$ est maximal dans B (car f_i est irréductible dans $k(\mathfrak{p})[X]$), divise $\mathfrak{p}$, et que $f_{\mathfrak{P}_i} = [k(\mathfrak{P}_i) : k(\mathfrak{p})] = \deg(f_i)$.
Par ailleurs, si $i \neq j$, on a $k(\mathfrak{p})[X] = f_i(X)k(\mathfrak{p})[X] + f_j(X)k(\mathfrak{p})[X]$ (car f_i et f_j sont premiers entre eux), donc $A[X] = F_i(X)A[X] + F_j(X)A[X] + \mathfrak{p}[X]$, ce qui implique $\mathfrak{P}_i + \mathfrak{P}_j = B$: les idéaux $\mathfrak{P}_1,\dots,\mathfrak{P}_s$ sont deux à deux premiers entre eux.
Réciproquement, soit $\mathfrak{P} \subset B$ maximal tel que $\mathfrak{P} \mid \mathfrak{p}$. Comme $F(X) \equiv \prod_{i=1}^{s} F_i(X) \mod \mathfrak{p}[X]$, on a $\prod_{i=1}^{s} F_i(\theta) \in \mathfrak{P}$: il existe $i \in \{1,\dots,s\}$ tel que $F_i(\theta) \in \mathfrak{P}$, et donc $\mathfrak{P}_i \subset \mathfrak{P}$, *i.e.* $\mathfrak{P}_i = \mathfrak{P}$ par maximalité de $\mathfrak{P}_i$. L'ensemble des idéaux maximaux de B qui divisent $\mathfrak{p}$ est donc précisément $\{\mathfrak{P}_1,\dots,\mathfrak{P}_s\}$.
Il reste donc à voir que pour tout $i \in \{1,\dots,s\}$, l'indice de ramification $e_{\mathfrak{P}_i}$ vaut r_i. D'après le théorème des restes chinois, on a l'isomorphisme

$$B/\mathfrak{p}B \simeq k(\mathfrak{p})[X]/(\overline{F}(X)) \xrightarrow{\sim} \prod_{i=1}^{s} k(\mathfrak{p})[X]/(f_i(X)^{r_i})$$

Pour $j \neq i$, on a $F_j(\theta) \notin \mathfrak{P}_i$ d'après ce qui précède : le localisé du facteur $k(\mathfrak{p})[X]/(f_j(X)^{r_j})$ en $\mathfrak{P}_i$ est nul. On a donc

$$B_{\mathfrak{P}_i}/\mathfrak{p}B_{\mathfrak{P}_i} \simeq k(\mathfrak{p})[X]/(f_i(X)^{r_i})$$

ce qui implique

$$e_{\mathfrak{P}_i} f_{\mathfrak{P}_i} = \dim_{\mathfrak{p}}(B_{\mathfrak{P}_i}/\mathfrak{p}B_{\mathfrak{P}_i}) = \dim_{\mathfrak{p}}(k(\mathfrak{p})[X]/(f_i(X)^{r_i})) = r_i \deg(f_i) = r_i f_{\mathfrak{P}_i}$$

et donc $e_{\mathfrak{P}_i} = r_i$. □

Théorème 3.5.7. Sous les hypothèses de la définition 3.5.1, supposons en outre que B est un A-module libre [a]. Les idéaux premiers de A en lesquels l'extension L/K est ramifiée sont précisément les diviseurs de l'idéal discriminant $\mathfrak{d}_{B/A}$. En particulier, il y en a un nombre fini.

a. En fait, cette hypothèse est superflue, on peut définir l'idéal discriminant sans, et le théorème est encore valide.

Démonstration. Soient $(x_1,\dots,x_d)$ une base de B sur A (donc $\mathfrak{d}_{B/A} = \mathrm{D}(x_1,\dots,x_d)A$) et $\mathfrak{p}$ un idéal premier non nul de A. L'extension L/K est non ramifiée en $\mathfrak{p}$ si et seulement si $B/\mathfrak{p}B \simeq \bigoplus_{\mathfrak{P}\mid\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}$ est un produit d'extensions séparables de $k(\mathfrak{p})$. Comme $\mathfrak{d}_{(B/\mathfrak{p}B)/k(\mathfrak{p})} = \mathrm{D}(x_1,\dots,x_d)A/\mathfrak{p}$ (parce que $x_1,\dots,x_d$ est une base de $B/\mathfrak{p}B$ sur $k(\mathfrak{p})$), il suffit de montrer que $B/\mathfrak{p}B \simeq \bigoplus_{\mathfrak{P}\mid\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}$ est un produit d'extensions séparables de $k(\mathfrak{p})$ si et seulement si on a $\mathfrak{d}_{(B/\mathfrak{p}B)/k(\mathfrak{p})} \neq \{0\}$. Comme on a $\mathfrak{d}_{(B/\mathfrak{p}B)/k(\mathfrak{p})} = \prod_{\mathfrak{P}\mid\mathfrak{p}} \mathfrak{d}_{(B/\mathfrak{P}^{e_{\mathfrak{P}}})/k(\mathfrak{p})}$, il s'agit donc de montrer que le morphisme $k(\mathfrak{p}) \to B/\mathfrak{P}^{e_{\mathfrak{P}}}$ est une extension séparable de corps si et seulement si $\mathfrak{d}_{(B/\mathfrak{P}^{e_{\mathfrak{P}}})/k(\mathfrak{p})} \neq 0$. L'implication résulte de la proposition 2.2.19. Réciproquement, supposons $\mathfrak{d}_{(B/\mathfrak{P}^{e_{\mathfrak{P}}})/k(\mathfrak{p})} \neq 0$. Supposons que $e_{\mathfrak{P}} > 1$, de sorte qu'on peut supposer que la base $(x_1,\dots,x_d)$ a des éléments dont l'image dans $B/\mathfrak{P}^{e_{\mathfrak{P}}}$ appartient à $\mathfrak{P}/\mathfrak{P}^{e_{\mathfrak{P}}}$. Cela implique que $\mathfrak{d}_{(B/\mathfrak{P}^{e_{\mathfrak{P}}})/(A/\mathfrak{p})} = 0$, ce qui n'est pas : on a nécessairement $e_{\mathfrak{P}} = 1$, de sorte que $B/\mathfrak{P}^{e_{\mathfrak{P}}} = k(\mathfrak{P})$ est un corps, extension finie de $k(\mathfrak{p})$. Si cette extension était non séparable, on aurait $\mathsf{Tr}_{k(\mathfrak{P})/k(\mathfrak{p})} = 0$ (*cf* remarque 2.4.2), de sorte que $\mathfrak{d}_{k(\mathfrak{P})/k(\mathfrak{p})} = 0$, ce qui n'est pas, et $k(\mathfrak{P})/k(\mathfrak{p})$ est séparable. □

Exemples 3.5.8. (1) Soient $d \in \mathbf{Z}\setminus\{0,1\}$ sans facteur carré et $K = \mathbf{Q}(\sqrt{d})$. On a vu que

$$d_K = \begin{cases} d & \text{si } d \equiv 1 \mod 4\,\mathbf{Z} \\ 4d & \text{si } d \not\equiv 1 \mod 4\,\mathbf{Z} \end{cases}$$

de sorte que les nombres premiers ramifiés dans K sont les diviseurs premiers de d, auxquels il faut adjoindre 2 si $d \not\equiv 1 \mod 4\,\mathbf{Z}$.
(2) Si p est un nombre premier impair, $\zeta \in \mathbf{C}$ une racine primitive p-ième de l'unité et $K = \mathbf{Q}(\zeta)$, on a vu que $\mathcal{O}_K = \mathbf{Z}[\zeta]$ et donc $d_K = (-1)^{\frac{p-1}{2}} p^{p-2}$. Il en résulte que p est l'unique nombre premier ramifié dans K.

4. Les théorèmes de finitude pour les corps de nombres

Dans tout ce qui suit, K désigne un corps de nombres.

Définition 4.0.1. Soit c la conjugaison complexe. On dit que $\sigma \in \mathsf{Hom}_{\mathbf{Q}\text{-alg}}(K, \overline{\mathbf{Q}})$ est un **plongement réel** si $c \circ \sigma = \sigma$ (*i.e.* si $\sigma(K) \subset \mathbf{R}$). Dans le cas contraire, on dit que σ est un **plongement imaginaire**, et $c \circ \sigma$ s'appelle le plongement complexe **conjugué**. On note r_1 le nombre de plongements réels et r_2 le nombre de *paires* de plongements complexes.

L'extension $K/\mathbf{Q}$ étant séparable, on a

$$\#\,\mathsf{Hom}_{\mathbf{Q}\text{-alg}}(K, \overline{\mathbf{Q}}) = [K : \mathbf{Q}] = r_1 + 2r_2$$

Remarque 4.0.2. Bien entendu, le couple (r_1, r_2) est invariant par isomorphisme de $\mathbf{Q}$-extension.

Proposition 4.0.3. Soient $\alpha \in K$ un élément primitif (*i.e.* tel que $K = \mathbf{Q}(\alpha)$) et $P \in \mathbf{Q}[X]$ son polynôme minimal sur $\mathbf{Q}$. Alors P a r_1 racines réelles et $2r_2$ racines complexes non réelles.

Démonstration. Les racines de P sont $\{\sigma(\alpha)\}_{\sigma \in \mathsf{Hom}_{\mathbf{Q}\text{-alg}}(K, \overline{\mathbf{Q}})}$ et $\sigma(\alpha) \in \mathbf{R} \Leftrightarrow \sigma(K) \subset \mathbf{R}$. □

Définition 4.0.4. On dit que K est **totalement réel** (resp. **imaginaire**) si $r_2 = 0$ (resp. $r_1 = 0$).

Exemples 4.0.5. (1) Si $d \in \mathbf{Z} \setminus \{0, 1\}$ est sans facteur carré, alors $\mathbf{Q}(\sqrt{d})$ est totalement réel (resp. imaginaire) si $d > 0$ (resp. $d < 0$).
(2) Si $n \geqslant 3$ et $\zeta \in \mathbf{C}$ est une racine n-ième primitive de l'unité, alors $\mathbf{Q}(\zeta)$ est totalement imaginaire.

Exercice 4.0.6. Si $K/\mathbf{Q}$ est galoisienne, alors K est soit totalement réel soit totalement imaginaire [6].

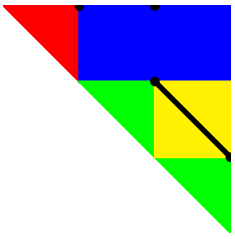
Proposition 4.0.7. Le signe de d_K est $(-1)^{r_2}$.

Démonstration. Il résulte de la proposition 2.2.12 que ce signe est celui de $\mathrm{D}(\alpha_1, \ldots, \alpha_n)$ où $\{\alpha_1, \ldots, \alpha_n\}$ est n'importe quelle $\mathbf{Q}$-base de K. Soient donc α un élément primitif de K, et $\alpha_1, \ldots, \alpha_n$ les racines de son polynôme minimal P. D'après la proposition 4.0.3, on peut supposer $\alpha_1, \ldots, \alpha_{r_1} \in \mathbf{R}$, $\alpha_{r_1+1}, \ldots, \alpha_{r_1+r_2} \notin \mathbf{R}$ et $\alpha_{r_1+r_2+k} = \overline{\alpha_{r_1+k}}$ pour $1 \leqslant k \leqslant r_2$. On a alors (*cf* définition 2.3.1)

$$\mathrm{D}(\alpha_1, \ldots, \alpha_n) = \mathsf{disc}(P) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2 = c^2 \prod_{k=1}^{r_2} (\alpha_{r_1+k} - \overline{\alpha_{r_1+k}})^2$$

où $c \in \mathbf{R}^\times$ est le produit des facteurs suivants :

- $\alpha_i - \alpha_j$ pour $1 \leqslant i < j \leqslant r_1$ (rouge) ;
- $(\alpha_i - \alpha_{r_1+j})(\alpha_i - \overline{\alpha_{r_1+j}})$ pour $1 \leqslant i \leqslant r_1$ et $1 \leqslant j \leqslant r_2$ (bleu) ;
- $(\alpha_{r_1+i} - \alpha_{r_1+j})(\overline{\alpha_{r_1+i}} - \overline{\alpha_{r_1+j}})$ et $(\alpha_{r_1+i} - \overline{\alpha_{r_1+j}})(\alpha_{r_1+i} - \overline{\alpha_{r_1+j}})$ pour $1 \leqslant i < j \leqslant r_2$ (vert et jaune).



Comme $\alpha_{r_1+k} - \overline{\alpha_{r_1+k}} \in i\,\mathbf{R}$ pour tout $k \in \{1, \ldots, r_2\}$, le signe de d_K est $(-1)^{r_2}$. □

6. Supposons K non totalement imaginaire : il existe un plongement réel $\sigma_0 \colon K \to \mathbf{R}$. Les autres plongements sont alors de la forme $\sigma_0 \circ g$ avec $g \in \mathsf{Gal}(K/\mathbf{Q})$: ils sont réels, et K est totalement réel.

4.1. **Finitude du groupe des classes.**

Définition 4.1.1. Le **groupe de classes** de K est le groupe $\mathsf{Cl}(\mathcal{O}_K)$ (*cf* définition 3.3.12. On le note [a] $\mathsf{Cl}(K)$.

a. C'est un petit abus de notation.

Théorème 4.1.2. Le groupe $\mathsf{Cl}(K)$ est fini.

Notation. On pose $h_K = \#\,\mathsf{Cl}(K)$.

Remarque 4.1.3. (1) Bien sûr, l'anneau $\mathcal{O}_K$ est principal si et seulement si $h_K = 1$. En général, il est très difficile de calculer h_K et $\mathsf{Cl}(K)$, même pour les extensions quadratiques.
(2) Le groupe des classes d'un anneau de Dedekind n'est pas fini en général. Cela dit, il l'est pour les anneaux finis sur $\mathbf{F}_p[X]$ (cas des corps de fonctions).

Exemple 4.1.4. Si $d \in \mathbf{N}_{>0}$ est sans facteur carré et $K = \mathbf{Q}(\sqrt{-d})$, alors

$$h_K = 1 \Leftrightarrow d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$$

$$h_K = 2 \Leftrightarrow d \in \{5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403, 427\}$$

En outre, $\lim\limits_{d\to\infty} h_K = +\infty$. Par contre, on conjecture que $h_{\mathbf{Q}(\sqrt{d})} = 1$ pour une infinité de d.

4.1.5. *Norme relative.* Soient A un anneau de Dedekind, $K = \mathsf{Frac}(A)$ et L une extension finie séparable de K. On note B la clôture intégrale de A dans L. On sait que B est un anneau de Dedekind de corps des fractions L, on dispose des théorèmes 3.3.10 (factorisation des idéaux fractionnaires) et 3.5.2 (sur la ramification).
Si $I \subset K$ est un idéal fractionnaire non nul, alors IB est un idéal fractionnaire non nul : cela fournit un morphisme de groupes $\mathsf{Fr}(A) \to \mathsf{Fr}(B)$. Si $I = xA$ est principal, il en est de même de $IB = xB$: le morphisme passe au quotient. On en déduit un morphisme de groupes

$$i_{B/A} \colon \mathsf{Cl}(A) \to \mathsf{Cl}(B)$$

Construisons un morphisme dans l'autre sens. Rappelons qu'on note $\mathscr{P}_A$ (resp. $\mathscr{P}_B$) l'ensemble des idéaux premiers non nuls de A (resp. B). Si $\mathfrak{P} \in \mathscr{P}_B$, on a $\mathfrak{p} := \mathfrak{P} \cap A \in \mathscr{P}_A$, et on dispose du degré résiduel $f_{\mathfrak{P}} := [k(\mathfrak{P}) : k(\mathfrak{p})]$. Posons alors

$$\mathsf{N}_{B/A}(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}}}$$

Comme les valuations induisent des isomorphismes de groupes $\mathsf{Fr}(A) \xrightarrow{\sim} \mathbf{Z}^{(\mathscr{P}_A)}$ et $\mathsf{Fr}(B) \xrightarrow{\sim} \mathbf{Z}^{(\mathscr{P}_B)}$ (proposition 3.3.11), cela définit donc un unique morphisme de groupes

$$\mathsf{N}_{B/A} \colon \mathsf{Fr}(B) \to \mathsf{Fr}(A)$$

Proposition 4.1.6. (1) (Transitivité) Soient M/L une extension finie séparable et C la clôture intégrale de A dans M (ou de B, c'est la même chose). Alors on a $\mathsf{N}_{B/A}(\mathsf{N}_{C/B}(J)) = \mathsf{N}_{C/A}(J)$ pour tout idéal fractionnaire non nul $J \subset M$.
(2) Si $I \subset K$ est un idéal fractionnaire non nul, on a $\mathsf{N}_{B/A}(i_{B/A}(I)) = I^n$ (où $n = [L/K]$).
(3) Si $x \in L^\times$, on a $\mathsf{N}_{B/A}(xB) = \mathsf{N}_{L/K}(x)A$.

Démonstration. (1) On peut supposer J maximal. On pose $\mathfrak{P} = B \cap J$ et $\mathfrak{p} = A \cap J = A \cap \mathfrak{P}$. On dispose des extensions $k(J)/k(\mathfrak{P})$ et $k(\mathfrak{P})/k(\mathfrak{p})$, donc $[k(J) : k(\mathfrak{P})][k(\mathfrak{P}) : k(\mathfrak{p})] = [k(J) : k(\mathfrak{p})]$. Comme $\mathsf{N}_{C/B}(J) = \mathfrak{P}^{[k(J):k(\mathfrak{P})]}$ et $\mathsf{N}_{B/A}(\mathfrak{P}) = \mathfrak{p}^{[k\mathfrak{P}):k(\mathfrak{p})]}$, on en déduit

$$\begin{aligned}\mathsf{N}_{B/A}(\mathsf{N}_{C/B}(J)) &= \mathsf{N}_{B/A}(\mathfrak{P}^{[k(J):k(\mathfrak{P})]}) = \mathsf{N}_{B/A}(\mathfrak{P})^{[k(J):k(\mathfrak{P})]} \\ &= \mathfrak{p}^{[k(\mathfrak{P}):k(\mathfrak{p})][k(J):k(\mathfrak{P})]} = \mathfrak{p}^{[k(J):k(\mathfrak{p})]} = \mathsf{N}_{C/A}(J)\end{aligned}$$

(2) On peut supposer $I = \mathfrak{p}$ maximal : on a $i_{B/A}(I) = \mathfrak{p}B = \prod\limits_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$ donc

$$\mathsf{N}_{B/A}(i_{B/A}(I)) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathsf{N}_{B/A}(\mathfrak{P})^{e_{\mathfrak{P}}} = \mathfrak{p}^{\sum\limits_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}} = I^n$$

en vertu du théorème 3.5.2.
(3) Commençons par traiter le cas où L/K est galoisienne, de groupe de Galois Γ. Montrons qu'alors, on a $i_{B/A}(\mathsf{N}_{B/A}(J)) = \mathsf{N}_{B/A}(J)B = \prod_{\gamma\in\Gamma}\gamma(J)$ pour tout idéal fractionnaire non nul $J \subset L$. Comme plus haut, on peut supposer $J = \mathfrak{P}$ premier non nul. Posons $\mathfrak{p} = A \cap \mathfrak{P}$: d'après le théorème 3.5.5, le groupe Γ agit transitivement sur l'ensemble des idéaux premiers divisant $\mathfrak{p}$, et les entiers $e_{\mathfrak{P}}$ et $f_{\mathfrak{P}}$ ne dépendent que de $\mathfrak{p}$ et pas de $\mathfrak{P}$ (on les note $e_{\mathfrak{p}}$ et $f_{\mathfrak{p}}$ respectivement). Notons $\Gamma_{\mathfrak{P}}$ le stabilisateur de $\mathfrak{P}$: on a $\#\Gamma = [L:K] = e_{\mathfrak{p}}f_{\mathfrak{p}}g_{\mathfrak{p}}$ avec $g_{\mathfrak{p}} = \big[\Gamma : \Gamma_{\mathfrak{P}}\big]$, donc $\#\Gamma_{\mathfrak{P}} = e_{\mathfrak{p}}f_{\mathfrak{p}}$. En outre, on a $\mathfrak{p}B = \prod_{\gamma\in\Gamma/\Gamma_{\mathfrak{P}}}\gamma(\mathfrak{P})^{e_{\mathfrak{p}}}$, ce qui implique

$$\mathsf{N}_{B/A}(J)B = \mathfrak{p}^{f_{\mathfrak{p}}}B = \prod_{\gamma\in\Gamma/\Gamma_{\mathfrak{P}}}\gamma(\mathfrak{P})^{e_{\mathfrak{p}}f_{\mathfrak{p}}} = \prod_{\gamma\in\Gamma/\Gamma_{\mathfrak{P}}}\gamma(\mathfrak{P})^{\#\Gamma_{\mathfrak{P}}} = \prod_{\gamma\in\Gamma}\gamma(\mathfrak{P})$$

ce qu'on voulait. Appliquée à $J = xB$ pour $x \in L^\times$, la formule qu'on vient d'obtenir s'écrit $\mathsf{N}_{B/A}(xB)B = \prod_{\gamma\in\Gamma}\gamma(x)B = \mathsf{N}_{L/K}(x)B$. Cela implique que les valuations des idéaux fractionnaires $\mathsf{N}_{B/A}(xB)$ et $\mathsf{N}_{L/K}(x)A$ sont les mêmes en tout idéal premier non nul de A : ils sont égaux.
Passons au cas général : soient M une clôture galoisienne de L/K et C la clôture intégrale de A dans M. Les extensions M/L et M/K sont galoisiennes : d'après ce qui précède, pour $x \in L$ on a

$$\mathsf{N}_{M/K}(x)A = \mathsf{N}_{C/A}(xC) = \mathsf{N}_{B/A}(\mathsf{N}_{C/B}(xC)) = \mathsf{N}_{B/A}(\mathsf{N}_{M/L}(x)B) = \mathsf{N}_{B/A}(x^dB) = \mathsf{N}_{B/A}(xB)^d$$

(où $d = [M : L]$). Par ailleurs, on a $\mathsf{N}_{M/K}(x) = \mathsf{N}_{L/K}(\mathsf{N}_{M/L}(x)) = \mathsf{N}_{L/K}(x^d) = \mathsf{N}_{L/K}(x)^d$ en vertu de la proposition 2.2.8. On a donc $\mathsf{N}_{L/K}(x)^dA = \mathsf{N}_{B/A}(xB)^d$, ce qui implique $\mathsf{N}_{L/K}(x)A = \mathsf{N}_{B/A}(xB)$ (en regardant les valuations $\mathfrak{p}$-adiques). □

Corollaire 4.1.7. Le morphisme $\mathsf{N}_{B/A}\colon \mathsf{Fr}(B) \to \mathsf{Fr}(A)$ induit un morphisme
$$\mathsf{N}_{B/A}\colon \mathsf{Cl}(B) \to \mathsf{Cl}(A)$$

Démonstration. Cela résulte de la proposition 4.1.6 (3), qui implique que $\mathsf{N}_{B/A}(\mathsf{Pr}(B)) \subset \mathsf{Pr}(A)$. □

Remarque 4.1.8. (1) D'après la proposition 4.1.6 (2), le morphisme $i_{B/A}\colon \mathsf{Fr}(A) \to \mathsf{Fr}(B)$ est injectif. Le morphisme induit $i_{B/A}\colon \mathsf{Cl}(A) \to \mathsf{Cl}(B)$ n'est pas injectif en général (des idéaux non principaux peuvent le devenir dans une extension). De même, l'application $\mathsf{N}_{B/A}$ n'est pas injective en général.
(2) Si $S \subset A$ est une partie multiplicative, et $J \subset L$ un idéal fractionnaire non nul, on a $\mathsf{N}_{S^{-1}B/S^{-1}A}(S^{-1}J) = S^{-1}\,\mathsf{N}_{B/A}(J)$.

4.1.9. *Norme absolue.* Désormais, K désigne un corps de nombres. Si $I \subset \mathcal{O}_K$ est un idéal non nul, alors $\mathsf{N}_{\mathcal{O}_K/\mathbf{Z}}(I)$ est un idéal de $\mathbf{Z}$: il est de la forme $\mathsf{N}(I)\,\mathbf{Z}$ avec $\mathsf{N}(I) \in \mathbf{Z}_{>0}$.

Définition 4.1.10. L'entier $\mathsf{N}(I)$ s'appelle le **norme absolue** de l'idéal I.

Remarque 4.1.11. Il résulte de la définition que $\mathsf{N}(IJ) = \mathsf{N}(I)\,\mathsf{N}(J)$ pour tout $I, J \subset \mathcal{O}_K$ des idéaux non nuls. Par ailleurs, la proposition 4.1.6 (3) implique que $\mathsf{N}(x\mathcal{O}_K) = \big|\mathsf{N}_{K/\mathbf{Q}}(x)\big|$ pour tout $x \in \mathcal{O}_K\backslash\{0\}$.

Exemple 4.1.12. Si $\mathfrak{p} \subset \mathcal{O}_K$ est premier non nul, $\mathfrak{p} \cap \mathbf{Z} = p\,\mathbf{Z}$ (*i.e.* $\mathfrak{p}$ divise p), on a $\mathsf{N}(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$.

Lemme 4.1.13. Soient A un anneau de valuation discrète et $\mathfrak{m}$ son idéal maximal. Supposons $A/\mathfrak{m}$ fini, de cardinal q. Alors $\#(A/\mathfrak{m}^n) = q^n$ pour tout $n \in \mathbf{N}_{>0}$.

Démonstration. Considérons le morphisme surjectif $A/\mathfrak{m}^{n+1} \to A/\mathfrak{m}^n$: son noyau est $\mathfrak{m}^n/\mathfrak{m}^{n+1}$, et on a $\#(A/\mathfrak{m}^{n+1}) = \#(A/\mathfrak{m}^n)\#(\mathfrak{m}^n/\mathfrak{m}^{n+1})$. Si π est une uniformisante de A, la multiplication par π^n induit un isomorphisme $A/\mathfrak{m} \xrightarrow{\sim} \mathfrak{m}^n/\mathfrak{m}^{n+1}$: on a donc $\#(A/\mathfrak{m}^{n+1}) = q\#(A/\mathfrak{m}^n)$, et on conclut par récurrence. □

Proposition 4.1.14. Pour tout idéal non nul $I \subset \mathcal{O}_K$, on a $\mathsf{N}(I) = \#(\mathcal{O}_K/I)$.

Démonstration. Soit $I = \prod_{i=1}^{n} \mathfrak{p}_i^{\alpha_i}$ la factorisation de I en produit d'idéaux premiers non nuls. D'après le théorème des restes chinois (*cf* théorème 3.4.3), on a $\mathcal{O}_K/I \simeq \bigoplus_{i=1}^{n} \mathcal{O}_K/\mathfrak{p}_i^{\alpha_i}$, de sorte que $\#(\mathcal{O}_K/I) = \prod_{i=1}^{n} \#\big(\mathcal{O}_K/\mathfrak{p}_i^{\alpha_i}\big)$. Mais d'après le lemme 4.1.13, on a

$$\#\big(\mathcal{O}_K/\mathfrak{p}_i^{\alpha_i}\big) = \#\big(\mathcal{O}_{K,\mathfrak{p}_i}/\mathfrak{p}_i^{\alpha_i}\mathcal{O}_{K,\mathfrak{p}_i}\big) = \big(\#k(\mathfrak{p}_i)\big)^{\alpha_i}$$

Si $\mathfrak{p}_i \cap \mathbf{Z} = p_i\,\mathbf{Z}$, le corps $k(\mathfrak{p}_i)$ est une extension de degré $f_{\mathfrak{p}_i}$ de $\mathbf{F}_{p_i}$: on a $\#k(\mathfrak{p}_i) = p_i^{f_{\mathfrak{p}_i}} = \mathsf{N}(\mathfrak{p}_i)$ pour tout $i \in \{1,\dots,n\}$, d'où $\#(\mathcal{O}_K/I) = \prod_{i=1}^{n} \mathsf{N}(\mathfrak{p}_i)^{\alpha_i} = \mathsf{N}(I)$. □

Lemme 4.1.15. Pour tout $c \in \mathbf{R}_{>0}$, il n'y a qu'un nombre fini d'idéaux non nuls $I \subseteq \mathcal{O}_K$ tels que $\mathsf{N}(I) \leqslant c$.

Démonstration. Il suffit de montrer que pour tout $N \in \mathbf{N}_{>0}$, il n'y a qu'un nombre fini d'idéaux non nuls $I \subset \mathcal{O}_K$ tels que $\mathsf{N}(I) = N$: soit I un tel idéal. D'après la proposition 4.1.14, on a $\#(\mathcal{O}_K/I) = N$, donc $N = 0$ dans le groupe $\mathcal{O}_K/I$, *i.e.* $N \in I$. L'ensemble des idéaux de $\mathcal{O}_K$ contenant $N\mathcal{O}_K$ est en bijection avec l'ensemble des idéaux de l'anneau quotient $\mathcal{O}_K/N\mathcal{O}_K$. Comme ce dernier est fini (de cardinal N^n d'après la proposition 4.1.14), il n'a qu'un nombre fini d'idéaux. □

4.1.16. *Preuve du théorème 4.1.2.*

Définition 4.1.17. On note $\sigma_1,\dots,\sigma_{r_1}$ les plongements réels, et on choisit $\sigma_{r_1+1},\dots,\sigma_{r_1+r_2}$ des plongements imaginaires deux à deux non conjugués (*i.e.* tels que $\sigma_i \neq c\circ\sigma_j$ pour $i,j \in \{r_1+1,\dots,r_1+r_2\}$ tels que $i \neq j$). On a alors

$$\mathsf{Hom}_{\mathbf{Q}\text{-alg}}(K,\overline{\mathbf{Q}}) = \big\{\sigma_1,\dots,\sigma_{r_1},\sigma_{r_1+1},\dots,\sigma_{r_1+r_2},c\circ\sigma_{r_1+1},\dots,c\circ\sigma_{r_1+r_2}\big\}$$

On note alors $\sigma\colon K \to \mathbf{R}^n$ le composé des applications

$$K \to \mathbf{R}^{r_1}\times\mathbf{C}^{r_2}$$
$$x \mapsto \big(\sigma_1(x),\dots,\sigma_{r_1}(x),\sigma_{r_1+1}(x),\dots,\sigma_{r_1+r_2}(x)\big)$$

et

$$\mathbf{R}^{r_1}\times\mathbf{C}^{r_2} \xrightarrow{\sim} \mathbf{R}^n$$
$$(x_1,\dots,x_{r_1},z_{r_1+1},\dots,z_{r_1+r_2}) \mapsto \big(x_1,\dots,x_{r_1},\Re(z_{r_1+1}),\dots,\Re(z_{r_1+r_2}),\Im(z_{r_1+1}),\dots,\Im(z_{r_1+r_2})\big)$$

qu'on appelle **plongement canonique**. C'est un morphisme $\mathbf{Q}$-linéaire injectif.

Lemme 4.1.18. Soit $M \subset K$ un sous-groupe de type fini. Alors $\sigma(M)$ est un sous-groupe discret de $\mathbf{R}^n$.

Démonstration. Soit I le sous-$\mathcal{O}_K$-module de K engendré par M. Comme M est engendré par un nombre fini d'éléments, il en est de même de I : c'est un idéal fractionnaire. Il existe donc $a \in \mathbf{N}_{>0}$ tel que $M \subseteq I \subseteq a^{-1}\mathcal{O}_K$. On a alors $\sigma(M) \subseteq a^{-1}\sigma(\mathcal{O}_K)$: il suffit de voir que $\sigma(\mathcal{O}_K)$ est discret. Soient $\rho \in \mathbf{R}_{>0}$ et $B_\rho = \big\{x \in \mathbf{R}^n,\ \|x\| \leqslant \rho\big\}$ la boule fermée de centre 0 et de rayon ρ. Si $x \in \mathcal{O}_K$ est tel que $\sigma(x) \in B_\rho$, alors $|\sigma_i(x)| \leqslant \rho$ pour $i \in \{1,\dots,r_1\}$ et $|\Re(\sigma_i(x))|, |\Im(\sigma_i(x))| \leqslant \rho$ *i.e.* $|\sigma_i(x)| \leqslant \sqrt{2}\rho$ pour $i \in \{r_1+1,\dots,n\}$. Pour $k \in \{1,\dots,n\}$, notons a_k le k-ième polynôme symétrique en $\sigma_1(x),\dots,\sigma_n(x)$. Comme $x \in \mathcal{O}_K$, on a $a_k \in \mathbf{Z}$. Par ailleurs, on a $|a_k| \leqslant \binom{n}{k}(\sqrt{2}\rho)^k \leqslant 2^{3n/2}\rho^k$: si $\rho < \frac{1}{(2\sqrt{2})^n}$, on a $|a_k| < 1$ et donc $a_k = 0$ pour tout $k \in \{1,\dots,n\}$. Comme $x^n - a_1x^{n-1} + \cdots + (-1)^n a_n = 0$, on a $x = 0$, de sorte que $\sigma(\mathcal{O}_K) \cap B_{\frac{1}{(2\sqrt{2})^n}} = \{0\}$. Cela implique que 0 est isolé dans $\sigma(\mathcal{O}_K)$. Comme c'est un sous-groupe de $\mathbf{R}^n$, tous les points de $\sigma(\mathcal{O}_K)$ sont isolés, et $\sigma(\mathcal{O}_K)$ est discret. □

Dans ce qui suit, μ désigne la mesure de Lebesgue de $\mathbf{R}^n$.

Lemme 4.1.19. Soit $M \subset K$ un sous-groupe libre de rang n. Alors $\sigma(M)$ est un réseau de $\mathbf{R}^n$, de volume

$$\mu(\sigma(M)) = 2^{-r_2} \left|\det\left([\sigma_i(x_j)]_{1\leqslant i,j\leqslant n}\right)\right|$$

pour toute base $(x_1, \dots, x_n)$ de M sur $\mathbf{Z}$.

Démonstration. L'application σ est un morphisme injectif de groupes : comme M est un $\mathbf{Z}$-module libre de rang n, il en est de même de $\sigma(M)$. D'après le lemme 4.1.18, c'est un sous-groupe discret de $\mathbf{R}^n$: c'est donc un réseau en vertu de la proposition 1.6.3. La famille $(\sigma(x_1), \dots, \sigma(x_n))$ est une base du réseau $\sigma(M)$. On a donc $\mu(\sigma(M)) = |\delta|$ avec $\delta = \det\big(\sigma(x_1), \dots, \sigma(x_n)\big)$. Or on a

$$\delta = \begin{vmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(x_1) & \cdots & \sigma_{r_1}(x_n) \\ \Re(\sigma_{r_1+1}(x_1)) & \cdots & \Re(\sigma_{r_1+1}(x_1)) \\ \vdots & & \vdots \\ \Re(\sigma_{r_1+r_2}(x_1)) & \cdots & \Re(\sigma_{r_1+r_2}(x_n)) \\ \Im(\sigma_{r_1+1}(x_1)) & \cdots & \Im(\sigma_{r_1+1}(x_n)) \\ \vdots & & \vdots \\ \Im(\sigma_{r_1+r_2}(x_1)) & \cdots & \Im(\sigma_{r_1+r_2}(x_n)) \end{vmatrix} = \begin{vmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(x_1) & \cdots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \cdots & \sigma_{r_1+1}(x_1) \\ \vdots & & \vdots \\ \sigma_{r_1+r_2}(x_1) & \cdots & \sigma_{r_1+r_2}(x_n) \\ \Im(\sigma_{r_1+1}(x_1)) & \cdots & \Im(\sigma_{r_1+1}(x_n)) \\ \vdots & & \vdots \\ \Im(\sigma_{r_1+r_2}(x_1)) & \cdots & \Im(\sigma_{r_1+r_2}(x_n)) \end{vmatrix}$$

$$= \frac{1}{(-2i)^{r_2}} \begin{vmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_n) \\ \vdots & & \vdots \\ \sigma_{r_1+r_2}(x_1) & \cdots & \sigma_{r_1+r_2}(x_n) \\ c(\sigma_{r_1+1}(x_1)) & \cdots & c(\sigma_{r_1+1}(x_n)) \\ \vdots & & \vdots \\ c(\sigma_{r_1+r_2}(x_1)) & \cdots & c(\sigma_{r_1+r_2}(x_n)) \end{vmatrix}$$

car $\Im(\sigma_i(x_j)) = \frac{\sigma_i(x_j) - c(\sigma_i(x_j))}{2i}$. On a donc $\delta = (-2i)^{-r_2} \det\big([\sigma_i(x_j)]_{1\leqslant i,j\leqslant n}\big)$. □

Rappelons que d_K désigne le discriminant absolu de K (*cf* définition 2.5.2).

Proposition 4.1.20. Soit $I \subset \mathcal{O}_K$ un idéal non nul. Alors $\sigma(I)$ est un réseau de $\mathbf{R}^n$, de volume

$$\mu(\sigma(I)) = 2^{-r_2}\sqrt{|d_K|}\,\mathsf{N}(I)$$

(en particulier, $\sigma(\mathcal{O}_K)$ est un réseau de $\mathbf{R}^n$ de volume $\mu(\sigma(\mathcal{O}_K)) = 2^{-r_2}\sqrt{|d_K|}$).

Démonstration. Le sous-groupe $I \subset \mathcal{O}_K$ est d'indice fini égal à $\mathsf{N}(I)$. D'après le théorème de la base adaptée (théorème 1.5.9), il existe une base $(e_1, \dots, e_n)$ de $\mathcal{O}_K$ et $a_1 \mid a_2 \mid \cdots \mid a_n \in \mathbf{N}_{>0}$ tels que $(a_1e_1, \dots, a_ne_n)$ soit une base de I sur $\mathbf{Z}$ (en particulier, I est libre de rang n). D'après le lemme 4.1.19 appliqué au sous-groupe $M = I$ de $\mathcal{O}_K$, le sous-groupe $\sigma(I)$ est un réseau de $\mathbf{R}^n$, tel que $\mu(\sigma(I)) = 2^{-r_2}\,|\delta|$ avec

$$\delta = \det\big([\sigma_i(a_je_j)]_{1\leqslant i,j\leqslant n}\big) = \det\big([\sigma_i(e_j)]_{1\leqslant i,j\leqslant n}\big)\prod_{j=1}^{n} a_j.$$

On conclut en observant que $d_K = \mathrm{D}(e_1, \dots, e_n) = \det\big([\sigma_i(e_j)]_{1\leqslant i,j\leqslant n}\big)^2$ et $\mathsf{N}(I) = \prod_{j=1}^{n} a_j$. □

Lemme 4.1.21. Pour $a, b \in \mathbf{N}$ et $\rho \in \mathbf{R}_{>0}$, posons

$$B_{a,b}(\rho) = \left\{(x_1, \dots, x_a, z_1, \dots, z_b) \in \mathbf{R}^a \times \mathbf{C}^b,\ \sum_{i=1}^{a} |x_i| + 2\sum_{j=1}^{b} |z_j| \leqslant \rho\right\}$$

Le volume de $B_{a,b}(\rho)$ est $2^a\left(\frac{\pi}{2}\right)^b \frac{\rho^N}{N!}$ avec $N = a + 2b$.

Démonstration. Notons $v_{a,b}(\rho)$ le volume de $B_{a,b}(\rho)$. On procède par récurrence sur (a,b). On a déjà $v_{1,0}(\rho) = \int_{-\rho}^{\rho} \mathrm{d}x_1 = 2\rho$ et $v_{0,1}(\rho) = \int_{|x+iy|\leqslant\rho/2} \mathrm{d}x\,\mathrm{d}y = \pi(\rho/2)^2$. Supposons $a \in \mathbf{N}_{>0}$ et $v_{a-1,b}(\rho) = 2^{a-1}\big(\frac{\pi}{2}\big)^b \frac{\rho^{N-1}}{(N-1)!}$. On a

$$\begin{aligned} v_{a,b}(\rho) &= \int_{-\rho}^{\rho} v_{a-1,b}(\rho - |x_a|)\,\mathrm{d}x_a = 2\int_0^{\rho} v_{a-1,b}(\rho - x_a)\,\mathrm{d}x_a \\ &= 2\int_0^{\rho} 2^{a-1}\Big(\frac{\pi}{2}\Big)^b \frac{(\rho-x_a)^{N-1}}{(N-1)!}\,\mathrm{d}x_a = 2^a\Big(\frac{\pi}{2}\Big)^b \Big[-\frac{(\rho-x_a)^N}{N!}\Big]_{x_a=0}^{x_a=\rho} = 2^a\Big(\frac{\pi}{2}\Big)^b \frac{\rho^N}{N!} \end{aligned}$$

De même, supposons $b > 0$ et $v_{a,b-1}(\rho) = 2^a\big(\frac{\pi}{2}\big)^{b-1} \frac{\rho^{N-2}}{(N-2)!}$. En posant $z_b = x + iy = re^{i\theta}$, on a

$$\begin{aligned} v_{a,b}(\rho) &= \int_{|x+iy|\leqslant\rho/2} v_{a,b-1}(\rho - 2\,|x+iy|)\,\mathrm{d}x\,\mathrm{d}y = \int_0^{2\pi}\int_0^{\rho/2} v_{a,b-1}(\rho-2r)r\,\mathrm{d}r\,\mathrm{d}\theta \\ &= 2\pi\int_0^{\rho/2} 2^a\Big(\frac{\pi}{2}\Big)^{b-1}\frac{(\rho-2r)^{N-2}}{(N-2)!}r\,\mathrm{d}r \\ &= 2^{a+2}\Big(\frac{\pi}{2}\Big)^b\Bigg(\underbrace{\Big[-\frac{(\rho-2r)^{N-1}}{2(N-1)!}r\Big]_{r=0}^{r=\rho/2}}_{0} + \int_0^{\rho/2}\frac{(\rho-2r)^{N-1}}{2(N-1)!}\,\mathrm{d}r\Bigg) \\ &= 2^{a+2}\Big(\frac{\pi}{2}\Big)^b\Big[-\frac{(\rho-2r)^N}{4N!}\Big]_{r=0}^{r=\rho/2} = 2^a\Big(\frac{\pi}{2}\Big)^b\frac{\rho^N}{N!} \end{aligned}$$

□

Définition 4.1.22. La **constante de Minkowski** de K est

$$C_K = \Big(\frac{4}{\pi}\Big)^{r_2}\frac{n!}{n^n} \in \mathbf{R}_{>0}$$

Lemme 4.1.23. Soit $I \subset \mathcal{O}_K$ un idéal non nul. Alors il existe $x \in I\backslash\{0\}$ tel que

$$\big|\mathsf{N}_{K/\mathbf{Q}}(x)\big| \leqslant C_K\sqrt{|d_K|}\,\mathsf{N}(I)$$

Démonstration. L'ensemble $B_{r_1,r_2}(\rho) \subset \mathbf{R}^{r_1}\times\mathbf{C}^{r_2} \simeq \mathbf{R}^n$ est compact (car fermé et borné), mesurable, convexe et symétrique par rapport à 0. D'après le lemme 4.1.21, son volume est

$$\mu(B_{r_1,r_2}(\rho)) = 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{\rho^n}{n!} = \frac{2^{r_1+r_2}}{C_K}\frac{\rho^n}{n^n}$$

Choisissons $\rho \in \mathbf{R}_{>0}$ tel que $\frac{\rho^n}{n^n} = 2^{r_2}C_K\mu(\sigma(I))$, de sorte que $\mu(B_{r_1,r_2}(\rho)) = 2^n\mu(\sigma(I))$: d'après le corollaire 1.6.8, $\sigma(I)\cap\big(B_{r_1,r_2}(\rho)\backslash\{0\}\big) \neq \varnothing$: il existe $x \in I\backslash\{0\}$ tel que $\sigma(x) \in B_{r_1,r_2}(\rho)$. On a alors

$$\begin{aligned} \big|\mathsf{N}_{K/\mathbf{Q}}(x)\big| &= \prod_{k=1}^n |\sigma_k(x)| = \Bigg(\prod_{i=1}^{r_1}|\sigma_i(x)|\Bigg)\Bigg(\prod_{j=r_1+1}^{r_1+r_2}|\sigma_j(x)|^2\Bigg) \\ &\leqslant \Bigg(\frac{1}{n}\sum_{i=1}^{r_1}|\sigma_i(x)| + \frac{2}{n}\sum_{j=r_1+1}^{r_1+r_2}|\sigma_j(x)|\Bigg)^n \leqslant \frac{\rho^n}{n^n} = 2^{r_2}C_K\mu(\sigma(I)) \end{aligned}$$

(la première inégalité résultant du fait que la moyenne géométrique est majorée par la moyenne arithmétique). Mais d'après la proposition 4.1.20, on a $\mu(\sigma(I)) = 2^{-r_2}\sqrt{|d_K|}\,\mathsf{N}(I)$, de sorte que $\big|\mathsf{N}_{K/\mathbf{Q}}(x)\big| \leqslant C_K\sqrt{|d_K|}\,\mathsf{N}(I)$, ce qu'on voulait. □

Théorème 4.1.24. Toute classe du groupe $\mathsf{Cl}(K)$ contient un représentant $I \subseteq \mathcal{O}_K$ tel que

$$\mathsf{N}(I) \leqslant C_K\sqrt{|d_K|}$$

Démonstration. Soit J un représentant de la classe considérée. Quitte à multiplier J par un élément de $K^\times$ convenable (ce qui ne change pas la classe), on peut supposer que $J^{-1} \subseteq \mathcal{O}_K$. D'après le lemme 4.1.23, il existe $x \in J^{-1}\backslash\{0\}$ tel que $\big|\mathsf{N}_{K/\mathbf{Q}}(x)\big| \leqslant C_K\sqrt{|d_K|}\,\mathsf{N}(J^{-1})$. Posons $I = xJ$:

c'est un idéal de $\mathcal{O}_K$, dans la même classe que J. On a $IJ^{-1} = x\mathcal{O}_K$, donc $\mathsf{N}(I)\,\mathsf{N}(J^{-1}) = \mathsf{N}(x\mathcal{O}_K) = \big|\mathsf{N}_{K/\mathbf{Q}}(x)\big| \leqslant C_K\sqrt{|d_K|}\,\mathsf{N}(J^{-1})$ d'où $\mathsf{N}(I) \leqslant C_K\sqrt{|d_K|}$. Remarque : avec les notations qui précèdent, on a $\mathcal{O}_K \subset J$, de sorte que $\mathsf{N}(J)$ n'est pas défini. □

Démonstration du théorème 4.1.2. En vertu du théorème 4.1.24, toute classe du groupe $\mathsf{Cl}(K)$ contient un représentant $I \subset \mathcal{O}_K$ de norme inférieure à $C_K\sqrt{|d_K|}$. Mais d'après le lemme 4.1.15, il n'y a qu'un nombre fini de tels idéaux : le groupe $\mathsf{Cl}(K)$ est fini. □

Remarque 4.1.25. Il résulte des théorèmes 3.3.3 et 4.1.24 que le groupe $\mathsf{Cl}(K)$ est engendré par les classes des idéaux premiers non nuls $\mathfrak{p} \subset \mathcal{O}_K$ tels que $\mathsf{N}(\mathfrak{p}) = p^f \leqslant C_K\sqrt{|d_K|}$, où $\mathfrak{p} \cap \mathbf{Z} = p\,\mathbf{Z}$ et $k(\mathfrak{p}) \simeq \mathbf{F}_{p^f}$.

Corollaire 4.1.26. (1) On a $|d_K| \geqslant \frac{\pi^n}{4}$ avec $n = [K : \mathbf{Q}]$.
(2) Si $K/\mathbf{Q}$ est non ramifiée, on a $K = \mathbf{Q}$.

Démonstration. (1) On peut supposer $n \geqslant 2$. Le théorème 4.1.24 appliqué à la classe de $\mathcal{O}_K$ implique que $1 \leqslant C_K\sqrt{|d_K|}$, donc $|d_K| \geqslant \frac{1}{C_K^2} = \big(\frac{\pi}{4}\big)^{2r_2}\frac{n^{2n}}{n!^2} \geqslant \big(\frac{\pi}{4}\big)^n\frac{n^{2n}}{n!^2} =: a_n$. On a $\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\big(1+\frac{1}{n}\big)^{2n}$. Comme $\big(1+\frac{1}{n}\big)^n \geqslant 2$, on a $\frac{a_{n+1}}{a_n} \geqslant \pi$, si bien que $a_n \geqslant a_2\pi^{n-2} = \frac{\pi^n}{4}$.
(2) Si $K/\mathbf{Q}$ est non ramifiée, on a $|d_K| = 1$ (*cf* théorème 3.5.7), donc $\pi^n \leqslant 4$ d'après (1), ce qui implique $n = 1$ *i.e.* $K = \mathbf{Q}$. □

Corollaire 4.1.27. (Libération des idéaux) Si K est un corps de nombres et $I \subset \mathcal{O}_K$ un idéal, il existe un corps de nombres $L \supset K$ tel que $I\mathcal{O}_L$ soit principal.

Démonstration. C'est trivial si $I = \{0\}$: supposons désormais $I \neq \{0\}$. Comme $\mathsf{Cl}(K)$ est fini, l'image $[I]$ de I dans $\mathsf{Cl}(K)$ est d'ordre fini, disons r : il existe $\alpha \in \mathcal{O}_K$ tel que $I^h = \alpha\mathcal{O}_K$. Soient alors $\beta \in \overline{\mathbf{Q}}$ tel que $\beta^h = \alpha$ et $L = K(\beta)$. On a $\beta \in \mathcal{O}_L$, et $(I\mathcal{O}_L)^h = \alpha\mathcal{O}_L = (\beta\mathcal{O}_L)^h$: comme $\mathcal{O}_L$ est un anneau de Dedekind, cela implique que $I\mathcal{O}_L = \beta\mathcal{O}_L$ est principal. □

Remarque 4.1.28. Soit $\overline{\mathbf{Z}} \subset \overline{\mathbf{Q}}$ l'anneau des entiers algébriques, *i.e.* la clôture intégrale de $\mathbf{Z}$ dans $\mathbf{C}$. C'est un anneau non noethérien, mais le corollaire qui précède montre que tout idéal de type fini I de $\overline{\mathbf{Z}}$ est principal. En effet, soit $x_1, \ldots, x_r \in \overline{\mathbf{Z}}$ un système de générateurs de I. Posons $K = \mathbf{Q}(x_1, \ldots, x_r)$: c'est un corps de nombres. Si I_0 désigne l'idéal de $\mathcal{O}_K$ engendré par $x_1, \ldots, x_r$, on a $I = I_0\overline{\mathbf{Z}}$. D'après le corollaire 4.1.27, il existe un corps de nombres $L \supset K$ et $\alpha \in \mathcal{O}_L$ tels que $I_0\mathcal{O}_L = \alpha\mathcal{O}_L$: on a $I\overline{\mathbf{Z}} = I_0\overline{\mathbf{Z}} = \alpha\overline{\mathbf{Z}}$.

Exemples 4.1.29. (1) Soit $K = \mathbf{Q}(\sqrt{-163})$. Comme $-163 \equiv 1 \mod 4\,\mathbf{Z}$, on a $\mathcal{O}_K = \mathbf{Z}[\alpha]$ avec $\alpha = \frac{1+\sqrt{-163}}{2}$ et $d_K = -163$. D'après la remarque 4.1.25, le groupe $\mathsf{Cl}(K)$ est engendré par les idéaux premiers $\mathfrak{p} \subset \mathcal{O}_K$ au-dessus de p tel que $\mathsf{N}(\mathfrak{p}) = p^{f_\mathfrak{p}} \leqslant C_K\sqrt{|d_K|} = \frac{2\sqrt{163}}{\pi} < 9$. On a donc $p \in \{2, 3, 5, 7\}$. Le polynôme minimal de α sur $\mathbf{Q}$ est $P(X) = X^2 + X + 41$. Ce dernier n'a pas de racine dans $\mathbf{F}_p$ et donc $\mathfrak{p} = p\mathcal{O}_K$ est principal donc d'image triviale dans $\mathsf{Cl}(K)$ pour tout $p \in \{2, 3, 5, 7\}$. Il en résulte que $h_K = 1$, *i.e.* $\mathcal{O}_K$ est principal.
(2) Soit $K = \mathbf{Q}(\sqrt{-5})$. Comme $-5 \equiv 3 \mod 4\,\mathbf{Z}$, on a $\mathcal{O}_K = \mathbf{Z}[\alpha]$ avec $\alpha = \sqrt{-5}$ et $d_K = -20$. Le groupe $\mathsf{Cl}(K)$ est engendré par les idéaux premiers $\mathfrak{p} \subset \mathcal{O}_K$ au-dessus de p tel que $\mathsf{N}(\mathfrak{p}) = p^{f_\mathfrak{p}} \leqslant C_K\sqrt{|d_K|} = \frac{4\sqrt{5}}{\pi} < 3$. On a donc $p = 2$. Comme $\mathcal{O}_K/2\mathcal{O}_K \simeq \mathbf{Z}[X]/(2, X^2+5) \simeq \mathbf{F}_2[X]/(X+1)^2$, on a $2 = \mathfrak{p}_2^2$ avec $\mathfrak{p}_2 = (2, \alpha+1)$, donc $\mathsf{N}(\mathfrak{p}_2) = 2$. Ainsi, $\mathsf{Cl}(K)$ est engendré par la classe de $\mathfrak{p}_2$, qui est d'ordre 1 ou 2. Si cette classe était triviale, l'idéal $\mathfrak{p}_2$ serait principal, engendré par un élément $x = a + b\alpha \in \mathcal{O}_K$, avec $a, b \in \mathbf{Z}$. On aurait $\big|\mathsf{N}_{K/\mathbf{Q}}(x)\big| = \mathsf{N}(\mathfrak{p}_2) = 2$, *i.e.* $a^2 + 5b^2 = 2$, donc $b = 0$ et $a^2 = 2$, ce qui est impossible : l'idéal $\mathfrak{p}_2$ n'est pas principal, et $h_K = 2$.

4.2. Le théorème des unités.

Proposition 4.2.1. Soient K un corps de nombres et $x \in \mathcal{O}_K$. Alors $x \in \mathcal{O}_K^\times$ si et seulement si $\mathsf{N}_{K/\mathbf{Q}}(x) \in \{\pm 1\}$.

Démonstration. Cela résulte du corollaire 2.2.6, et du fait que $\mathbf{Z}^\times = \{\pm 1\}$. □

Théorème 4.2.2. Le groupe des unités $\mathcal{O}_K^\times$ est un $\mathbf{Z}$-module de type fini. Ses éléments de torsion sont les racines de l'unité dans K, et son rang est égal à $r_1 + r_2 - 1$.

Exemple 4.2.3. Soit $d \in \mathbf{Z}_{>0}$ sans facteur carré et K le corps quadratique imaginaire $\mathbf{Q}(\sqrt{-d})$. Alors $r_1 = 0$ et $r_2 = 1$, de sorte que $\mathcal{O}_K^\times$ est un groupe fini et cyclique. Plus précisément, on voit facilement que

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1, \pm i\} = \mu_4 & \text{si } d = 1 \\ \{\pm 1, \pm j, \pm j^2\} = \mu_6 & \text{si } d = 3 \\ \{\pm 1\} & \text{sinon} \end{cases}$$

En effet, si $d \equiv 1, 2 \mod 4\,\mathbf{Z}$ et $d > 1$, on a $\mathcal{O}_K = \mathbf{Z}[\sqrt{-d}]$, et $\mathsf{N}_{L/K}(a + b\sqrt{-d}) = a^2 + db^2 = 1 \Leftrightarrow (a, b) \in \{(\pm 1, 0)\}$. Si $d \equiv 3 \mod 4\,\mathbf{Z}$ et $d > 3$, on a $\mathcal{O}_K = \mathbf{Z}[\alpha]$ avec $\alpha = \frac{1+\sqrt{-d}}{2}$, et $\mathsf{N}_{L/K}(a + b\alpha) = a^2 + ab + \frac{1+d}{4}b^2 = \left(a + \frac{b}{2}\right)^2 + \frac{d}{4}b^2 = 1 \Leftrightarrow (a, b) \in \{(\pm 1, 0)\}$.

Remarque 4.2.4. Il est en général très difficile de trouver des générateurs du groupe $\mathcal{O}_K^\times$.

Définition 4.2.5. Les notations étant les mêmes que celles de la définition 4.1.17, on pose

$$\ell \colon K^\times \to \mathbf{R}^{r_1+r_2}$$
$$x \mapsto \big(\ln(|\sigma_1(x)|), \dots, \ln(|\sigma_{r_1+r_2}(x)|)\big)$$

C'est un morphisme de groupes qu'on appelle le **plongement logarithmique**.

Lemme 4.2.6. Soit $B \subset \mathbf{R}^{r_1+r_2}$ une partie compacte. Alors $\mathcal{O}_K^\times \cap \ell^{-1}(B)$ est fini.

Démonstration. Il existe $C \in \mathbf{R}_{>0}$ tel que $B \subseteq [-C, C]^{r_1+r_2}$. Soit $x \in \mathcal{O}_K^\times \cap \ell^{-1}(B)$: on a $e^{-C} \leqslant |\sigma_i(x)| \leqslant e^C$ pour tout $i \in \{1, \dots, n\}$ (en posant $\sigma_i = c \circ \sigma_{i-r_2}$ si $r_1 + r_2 + 1 \leqslant i \leqslant n$). En particulier, si a_k désigne le k-ième polynôme symétrique élémentaire en $\sigma_1(x), \dots, \sigma_n(x)$, on a $|a_k| \leqslant \binom{n}{k} e^{kC}$: les coefficients de $P_{x,\mathbf{Q}}$ sont bornés. Comme x est entier sur $\mathbf{Z}$, on a $P_{x,\mathbf{Q}} \in \mathbf{Z}[X]$: il y a un nombre fini de $P_{x,\mathbf{Q}}$ possibles et donc un nombre fini de x possibles. □

Lemme 4.2.7. Soient

$$\psi \colon \mathbf{R}^{r_1+r_2} \to \mathbf{R}$$
$$(t_1, \dots, t_{r_1+r_2}) \mapsto \sum_{i=1}^{r_1} t_i + 2 \sum_{j=r_1+1}^{r_1+r_2} t_j$$

et $H = \mathsf{Ker}(\psi)$. Alors le groupe $\mathsf{Ker}\left(\ell_{|\mathcal{O}_K^\times}\right)$ est cyclique, et $\ell(\mathcal{O}_K^\times)$ est un sous-groupe discret de H.

Démonstration. D'après le lemme 4.2.6 appliqué à $B = \{0\}$, le sous-groupe $\mathsf{Ker}\left(\ell_{|\mathcal{O}_K^\times}\right) = \mathcal{O}_K^\times \cap \ell^{-1}(\{0\})$ est fini. Soit N son ordre : comme $x^N = 1$ pour tout $x \in \mathsf{Ker}\left(\ell_{|\mathcal{O}_K^\times}\right)$, on a $\mathsf{Ker}\left(\ell_{|\mathcal{O}_K^\times}\right) \subset \mu_N(K)$. Mais comme $\#\mu_N(K) \leqslant N$, on a nécessairement $\mathsf{Ker}\left(\ell_{|\mathcal{O}_K^\times}\right) = \mu_N(K)$, et c'est un groupe cyclique.

Comme $|\sigma_j(x)| = |c \circ \sigma_j(x)|$ pour tout $x \in K$ et tout $i \in \{1, \dots, n\}$, on a

$$\ln(\big|\mathsf{N}_{K/\mathbf{Q}}(x)\big|) = \sum_{i=1}^{r_1} \ln(|\sigma_i(x)|) + 2 \sum_{j=r_1+1}^{r_1+r_2} \ln(|\sigma_j(x)|) = \psi(\ell(x))$$

D'après la proposition 4.2.1, pour $x \in \mathcal{O}_K$, on a $x \in \mathcal{O}_K^\times \Leftrightarrow \mathsf{N}_{K/\mathbf{Q}}(x) \in \{\pm 1\}$. On a donc

$$x \in \mathcal{O}_K^\times \Rightarrow \big|\mathsf{N}_{K/\mathbf{Q}}(x)\big| = 1 \Rightarrow \psi(\ell(x)) = \ln(\big|\mathsf{N}_{K/\mathbf{Q}}(x)\big|) = 0$$

et donc $\ell(x) \in H$. Reste à voir que le sous-groupe $\ell(\mathcal{O}_K^\times)$ est discret dans H : cela résulte du lemme 4.2.6. □

Démonstration du théorème 4.2.2. La première partie du théorème résulte du lemme 4.2.7. Comme ℓ induit un isomorphisme $\mathcal{O}_K^\times/\big(\mathcal{O}_K^\times\big)_{\mathsf{tors}} \xrightarrow{\sim} \ell(\mathcal{O}_K^\times)$, il s'agit de voir que $\ell(\mathcal{O}_K^\times) \simeq \mathbf{Z}^{r_1+r_2-1}$. Comme $\ell(\mathcal{O}_K^\times)$ est un sous-groupe discret de $H = \mathsf{Ker}(\psi) \simeq \mathbf{R}^{r_1+r_2-1}$, on sait déjà que $\ell(\mathcal{O}_K^\times) \simeq \mathbf{Z}^r$ avec $r \leqslant r_1 + r_2 - 1$ (proposition 1.6.3). Pour conclure, il s'agit donc de prouver que $r = r_1 + r_2 - 1$, *i.e.*

que $\ell(\mathcal{O}_K^\times)$ est un *réseau* de H. Il suffit pour cela de montrer que $(\forall f \in H^\vee \backslash \{0\})\ f(\ell(\mathcal{O}_K^\times)) \neq \{0\}$. Comme

$$H \to \mathbf{R}^{r_1+r_2-1}$$
$$(t_1, \dots, t_{r_1+r_2}) \mapsto (t_1, \dots, t_{r_1+r_2-1})$$

est un isomorphisme, on peut écrire

$$f(t_1, \dots, t_{r_1+r_2}) = \sum_{i=1}^{r_1+r_2-1} c_i t_i$$

avec $c_1, \dots, c_{r_1+r_2-1} \in \mathbf{R}$ non tous nuls.

Interlude : construction d'éléments de $\mathcal{O}_K$. Fixons $\alpha \geqslant \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|}$ un réel auxiliaire. Étant donné $\underline{\lambda} = (\lambda_1, \dots, \lambda_{r_1+r_2-1}) \in \mathbf{R}_{>0}^{r_1+r_2-1}$, soit $\lambda_{r_1+r_2} \in \mathbf{R}_{>0}$ tel que

$$\left(\prod_{i=1}^{r_1} \lambda_i\right)\left(\prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2\right) = \alpha$$

et $\quad B(\underline{\lambda}) = \left\{ \begin{array}{c} (y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} \\ (\forall i \in \{1, \dots, r_1\})\ |y_i| \leqslant \lambda_i,\ (\forall j \in \{1, \dots, r_2\})\ |z_j| \leqslant \lambda_{r_1+j} \end{array} \right\}$

c'est une partie compacte, convexe, symétrique par rapport à 0 dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2} \simeq \mathbf{R}^n$. Elle est mesurable, de volume

$$\mu(B(\underline{\lambda})) = \left(\prod_{i=1}^{r_1} 2\lambda_i\right)\left(\prod_{j=1}^{r_2} \pi\lambda_{r_1+j}^2\right) = 2^{r_1}\pi^{r_2}\alpha \geqslant 2^{n-r_2}\sqrt{|d_K|} = 2^n \mu(\sigma(\mathcal{O}_K))$$

D'après le corollaire 1.6.8, il existe $x_{\underline{\lambda}} \in \mathcal{O}_K \backslash \{0\}$ tel que $\sigma(x_{\underline{\lambda}}) \in B(\underline{\lambda})$. Cet élément jouit des propriétés suivantes :

(i) $1 \leqslant \left|\mathsf{N}_{K/\mathbf{Q}}(x_{\underline{\lambda}})\right| \leqslant \alpha$;

(ii) $\left|f(\ell(x_{\underline{\lambda}})) - \sum_{i=1}^{r_1+r_2-1} c_i \ln(\lambda_i)\right| \leqslant \left(\sum_{i=1}^{r_1+r_2-1} |c_i|\right) \ln(\alpha)$.

En effet, comme $x_{\underline{\lambda}} \in \mathcal{O}_K \backslash \{0\}$, on a $\left|\mathsf{N}_{K/\mathbf{Q}}(x_{\underline{\lambda}})\right| \geqslant 1$, et $\left|\mathsf{N}_{K/\mathbf{Q}}(x_{\underline{\lambda}})\right| = \prod_{i=1}^{n} \left|\sigma_i(x_{\underline{\lambda}})\right| \leqslant \alpha$, ce qui prouve (i). Par aileurs, pour tout $i \in \{1, \dots, r_1 + r_2\}$, on a

$$\lambda_i \geqslant \left|\sigma_i(x_{\underline{\lambda}})\right| = \left|\mathsf{N}_{K/\mathbf{Q}}(x_{\underline{\lambda}})\right| \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} \left|\sigma_j(x_{\underline{\lambda}})\right|^{-1} \geqslant \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} \lambda_j^{-1} = \lambda_i/\alpha$$

de sorte que $\ln(\lambda_i) - \ln(\alpha) \leqslant \ln(\left|\sigma_i(x_{\underline{\lambda}})\right|) \leqslant \ln(\lambda_i)$ et donc $0 \leqslant \ln(\lambda_i) - \ln(\left|\sigma_i(x_{\underline{\lambda}})\right|) \leqslant \ln(\alpha)$ pour tout $i \in \{1, \dots, n\}$. On a donc

$$\begin{aligned} \left|f(\ell(x_{\underline{\lambda}})) - \sum_{i=1}^{r_1+r_2-1} c_i \ln(\lambda_i)\right| &= \left|\sum_{i=1}^{r_1+r_2-1} c_i\big(\ln(\left|\sigma_i(x_{\underline{\lambda}})\right|) - \ln(\lambda_i)\big)\right| \\ &\leqslant \sum_{i=1}^{r_1+r_2-1} |c_i| \left|\ln(\left|\sigma_i(x_{\underline{\lambda}})\right|) - \ln(\lambda_i)\right| \\ &\leqslant \left(\sum_{i=1}^{r_1+r_2-1} |c_i|\right) \ln(\alpha) \end{aligned}$$

Retour à la preuve du théorème 4.2.2. Fixons $\beta > \left(\sum_{i=1}^{r_1+r_2-1} |c_i|\right) \ln(\alpha)$ un deuxième réel auxiliaire. Pour $m \in \mathbf{N}_{>0}$, choisissons $\underline{\lambda}_m = (\lambda_{m,1}, \dots, \lambda_{m,r_1+r_2-1}) \in \mathbf{R}_{>0}^{r_1+r_2-1}$ tel que

$$\sum_{i=1}^{r_1+r_2-1} c_i \ln(\lambda_{m,i}) = 2m\beta$$

D'après ce qui précède, il existe $x_{\underline{\lambda}_m} \in \mathcal{O}_K\backslash\{0\}$ tel que les propriétés (i) et (ii) ci-dessus sont vérifiées avec $\underline{\lambda} = \underline{\lambda}_m$. En particulier, la propriété (ii) s'écrit $\left|f\big(\ell\big(x_{\underline{\lambda}_m}\big)\big) - 2m\beta\right| < \beta$, soit encore

$$(2m-1)\beta < f\big(\ell\big(x_{\underline{\lambda}_m}\big)\big) < (2m+1)\beta$$

de sorte que les $\big\{f\big(\ell\big(x_{\underline{\lambda}_m}\big)\big)\big\}_{m\in\mathbf{N}_{>0}}$ sont deux à deux distincts. Par ailleurs, pour $m \in \mathbf{N}_{>0}$, on a $\mathsf{N}\left(x_{\underline{\lambda}_m}\mathcal{O}_K\right) = \left|\mathsf{N}_{K/\mathbf{Q}}\left(x_{\underline{\lambda}_m}\right)\right| \leqslant \alpha$ d'après (i). Mais d'après le lemme 4.1.15, il n'y a qu'un nombre fini d'idéaux de $\mathcal{O}_K$ de norme inférieure à α : il existe $m, m' \in \mathbf{N}_{>0}$ distincts tels que $x_{\underline{\lambda}_m}\mathcal{O}_K = x_{\underline{\lambda}'_m}\mathcal{O}_K$. Il existe donc $u \in \mathcal{O}_K^\times$ tel que $x_{\underline{\lambda}'_m} = u x_{\underline{\lambda}_m}$. On a alors

$$f(\ell(u)) = f\big(\ell\big(x_{\underline{\lambda}'_m}\big)\big) - f\big(\ell\big(x_{\underline{\lambda}'_m}\big)\big) \neq 0$$

ce qu'on voulait. □

Définition 4.2.8. (1) Une famille de $r_1 + r_2 - 1$ éléments $u_1, \dots, u_{r_1+r_2-1} \in \mathcal{O}_K^\times$ telle que $(\ell(u_1), \dots, \ell(u_{r_1+r_2-1}))$ forment une base de $\mathcal{O}_K^\times/\big(\mathcal{O}_K^\times\big)_{\mathsf{tors}}$ s'appelle un **système d'unités fondamentales** (elle induit alors un isomorphisme $\mathcal{O}_K^\times \simeq \mathbb{\mu}(K) \times \mathbf{Z}^{r_1+r_2-1}$.
Une **unité fondamentale** est un élément de $\mathcal{O}_K^\times$ que l'on peut compléter en un système d'unités fondamentales.

(2) Le **régulateur** de K est le volume R_K du réseau $\ell(\mathcal{O}_K^\times) \subset H$. Si $(u_1, \dots, u_{r_1+r_2-1})$ est un système d'unités fondamentales, on a

$$R_K = \left|\det\left(\ell(u_1), \dots, \ell(u_{r_1+r_2-1})\right)\right|$$

Il est indépendant du choix de la famille $u_1, \dots, u_{r_1+r_2-1}$. Les coordonnées des vecteurs $\ell(u_1), \dots, \ell(u_{r_1+r_2-1})$ de $\mathbf{R}^{r_1+r_2}$ fournissent une matrice $M \in \mathsf{M}_{(r_1+r_2)\times(r_1+r_2-1)}(\mathbf{R})$: le réel R_K est le déterminant de la matrice obtenue en retirant à M n'importe quelle de ses lignes.

4.2.9. *Unités des corps quadratiques réels.* Soient $d \in \mathbf{N}_{>1}$ sans facteur carré et $K = \mathbf{Q}(\sqrt{d})$ le corps quadratique réel associé (on a $r_1 = 2$ et $r_2 = 0$). Comme $K \subset \mathbf{R}$, on a $\mathbb{\mu}(K) = \{\pm 1\}$, et le théorème des unités (*cf* théorème 4.2.2) implique que $\mathcal{O}_K^\times \simeq \{\pm1\} \times \mathbf{Z}$: il existe $\alpha = u + v\sqrt{d} \in \mathcal{O}_K^\times$ tel que $\mathcal{O}_K^\times = \pm\alpha^{\mathbf{Z}}$. Les unités fondamentales de K sont alors

$$\{\alpha = u + v\sqrt{d}, -\alpha = -u - v\sqrt{d}, \alpha^{-1} = \mathsf{N}_{K/\mathbf{Q}}(\alpha)(u - v\sqrt{d}), -\alpha^{-1} = -\mathsf{N}_{K/\mathbf{Q}}(\alpha)(u - v\sqrt{d})\}$$

(on a $\mathsf{N}_{K/\mathbf{Q}}(\alpha) = u^2 - dv^2 \in \{\pm1\}$). Supposons que α est la plus grande (pour l'ordre sur $\mathbf{R}$) de ces unités fondamentales. On a nécessairement $u, v > 0$. Comme $\alpha^{-1} < \alpha$, on a en outre $\alpha > 1$: les unités fondamentales sont $-\alpha < -\alpha^{-1} < \alpha^{-1} < \alpha$. Les unités > 1 sont alors les α^n avec $n \in \mathbf{N}_{>0}$, ce qui implique que α est la plus petite unité > 1.

Supposons $d \equiv 2, 3 \mod 4\,\mathbf{Z}$: on a $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$, ce qui implique que $u, v \in \mathbf{Z}$. Si $z = x + y\sqrt{d} \in \mathcal{O}_K$ (avec $x, y \in \mathbf{Z}$ donc), on a $\mathsf{N}_{K/\mathbf{Q}}(z) = x^2 - dy^2$, de sorte que

$$x + y\sqrt{d} \in \mathcal{O}_K^\times \Leftrightarrow x^2 - dy^2 = \pm 1$$

L'équation diophantienne qui précède s'appelle l'équation de **Pell-Fermat**. D'après ce qui précède, si $\alpha = u + v\sqrt{d}$ est l'unité fondamentale > 1, l'ensemble des solutions est $\{\pm(u_n, v_n),\ n \in \mathbf{Z}\}$ avec $u_n + v_n\sqrt{d} = (u + v\sqrt{d})^n$.

Remarque 4.2.10. (1) Géométriquement, l'ensemble des solutions de l'équation de Pell-Fermat correspond à l'ensemble des points à coordonnées entières sur les hyperboles d'équations $x^2 - dy^2 = 1$ et $x^2 - dy^2 = -1$.

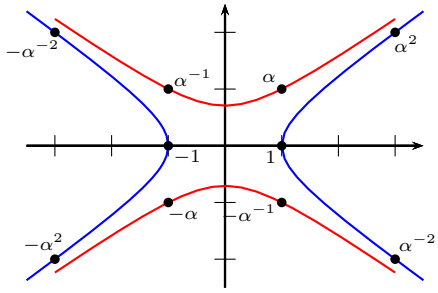
(2) Il est parfaitement possible que l'équation $x^2 - dy^2 = -1$ n'ait pas de solution dans $\mathbf{Z}^2$ (c'est équivalent à $\mathsf{N}_{K/\mathbf{Q}}(\mathcal{O}_K^\times) = \{1\}$). En effet, modulo d, une solution fournit une racine carré de -1 modulo d : il est nécessaire que $\left(\frac{-1}{d}\right) = -1$. Par exemple, si d est premier et $d \equiv 3 \mod 4$ (*eg* $d = 3$), on a $\left(\frac{-1}{d}\right) = (-1)^{\frac{d-1}{2}} = -1$.

(3) Lorsque l'équation $x^2 - dy^2 = -1$ a des solutions dans $\mathbf{Z}^2$, alors toute unité fondamentale α vérifie $\mathsf{N}_{K/\mathbf{Q}}(\alpha) = -1$ (sinon on aurait $\mathsf{N}_{K/\mathbf{Q}}(\mathcal{O}_K^\times) = \{1\}$, ce qui n'est pas).

(4) Même lorsque d est « petit », les coefficients d'une unité fondamentale peuvent très bien être « grands ». Par exemple, on a $\alpha = 1520 + 273\sqrt{31}$ pour $d = 31$, $\alpha = 24335 + 3588\sqrt{46}$ pour $d = 46$, $\alpha = 48842 + 5967\sqrt{67}$ pour $d = 67$ et $2143295 + 221064\sqrt{94}$ pour $d = 94$. *A contrario*, ils peuvent aussi être « petits » : on a $\alpha = 9 + \sqrt{82}$ pour $d = 82$.

Exemple 4.2.11. Supposons $d = 2$. Alors $\alpha := 1 + \sqrt{2}$ vérifie $\mathsf{N}_{K/\mathbf{Q}}(\alpha) = -1$: c'est une unité. Montrons que c'est la plus petite dans $]1, +\infty[$ (ce qui implique que α est une unité fondamentale). Si $1 < z = a + b\sqrt{2} < 1 + \sqrt{2}$ est une unité (avec $a, b \in \mathbf{Z}$), on a $\sqrt{2} - 1 = \alpha^{-1} < b\sqrt{2} - a < 1$ (car $\mathsf{N}_{K/\mathbf{Q}}(z) = -1$, *cf* remarque précédente) : on en déduit $b = 1$ (en additionnant) puis $a = 0$ ce qui est impossible.

Par exemple, $\alpha^8 = 577 + 408\sqrt{2}$ fournit la solution $(577, 408)$ à l'équation $x^2 - 2y^2 = 1$.



Remarque 4.2.12. Comme $\mathsf{N}_{K/\mathbf{Q}}(u_n + v_n\sqrt{d}) = u_n^2 - dv_n^2 = \pm 1$, on a $\left|\left(\frac{u_n}{v_n}\right)^2 - d\right| = \frac{1}{v_n^2}$, d'où $\left|\frac{u_n}{v_n} - \sqrt{d}\right| < \frac{1}{2v_n^2}$ (parce que $\frac{u_n}{v_n}, \sqrt{d} > 1$), de sorte que $\frac{u_n}{v_n}$ est une très bonne approximation rationnelle de $\sqrt{d}$. Plus précisément, la suite $\{(u_n, v_n)\}_{n \in \mathbf{N}_{>0}}$ correspond au développement en fraction continue de $\sqrt{d}$.

4.2.13. *Unités des extensions cyclotomiques.* Soient $n \in \mathbf{N}_{>2}$, $\zeta_n \in \mathbf{C}$ un racine n-ième primitive de l'unité et $K = \mathbf{Q}(\zeta_n)$ l'extension cyclotomique engendrée. Rappelons que $[K : \mathbf{Q}] = \varphi(n)$, que $K/\mathbf{Q}$ est galoisienne, et qu'on a l'isomorphisme

$$\begin{aligned}(\mathbf{Z}/n\mathbf{Z})^\times &\to \mathsf{Gal}(K/\mathbf{Q})\\ k &\mapsto \sigma_k\end{aligned}$$

où σ_k est caractérisé par $\sigma_k(\zeta_n) = \zeta_n^k$. Comme $\zeta_n^k \notin \mathbf{R}$ pour tout $k \in (\mathbf{Z}/n\mathbf{Z})^\times$, le corps K est totalement imaginaire : on a $r_1 = 0$ et $r_2 = \frac{\varphi(n)}{2}$. D'après le théorème des unités, on a $\mathcal{O}_K^\times \simeq \mathbb{\mu}(K) \times \mathbf{Z}^{\frac{\varphi(n)}{2}-1}$.

Soit u un générateur de $\mathbb{\mu}(K)$: c'est une racine N-ième de l'unité. Comme $\zeta_n \in \mathbb{\mu}(K)$, on a $n \mid N$. Par ailleurs, on a $\mathbf{Q}(u) \subset K$, de sorte que $[\mathbf{Q}(u) : \mathbf{Q}] \mid [K : \mathbf{Q}]$, *i.e.* $\varphi(N) \mid \varphi(n)$. Si $N = \prod_{k=1}^r p_i^{\alpha_i}$ est la décomposition de N en facteurs premiers (avec $\alpha_i \in \mathbf{N}_{>0}$ pour tout $i \in \{1, \dots, r\}$), celle de n est (quitte à permuter les facteurs) de la forme $n = \prod_{k=1}^s p_i^{\beta_i}$ avec $1 \leqslant s \leqslant r$ et $0 < \beta_i \leqslant \alpha_i$ pour tout $i \in \{1, \dots, s\}$. On a donc $\prod_{k=1}^r p_i^{\alpha_i - 1}(p_i - 1) \mid \prod_{k=1}^s p_i^{\beta_i - 1}(p_i - 1)$, ce qui implique $\prod_{k=1}^s p_i^{\alpha_i - \beta_i} \prod_{i=s+1}^r p_i^{\alpha_i - 1}(p_i - 1) \mid 1$. On a nécessairement $\alpha_i = \beta_i$ pour $1 \leqslant i \leqslant s$, et si $s < r$, on a $r = s + 1$, $p_r = 2$ et $\alpha_r = 1$. En résumé, on a $N = n$ ou $N = 2n$ (si n est impair), *i.e.* $N = \mathsf{ppcm}(2, n)$. On a donc :

$$\mathbb{\mu}(K) = \begin{cases} \mathbb{\mu}_n & \text{si } 2 \mid n \\ \mathbb{\mu}_{2n} = \{\pm 1\} \times \mathbb{\mu}_n = \{\pm\zeta_n^k,\ k \in (\mathbf{Z}/n\mathbf{Z})^\times\} & \text{si } 2 \nmid n \end{cases}$$

Bien entendu, la recherche de systèmes d'unités fondamentales est plus ardue. Si $k \in \mathbf{N}_{>0}$, posons

$$u_k = \frac{\zeta_n^k - 1}{\zeta_n - 1} = 1 + \zeta_n + \cdots + \zeta_n^{k-1} \in \mathbf{Z}[\zeta_n] \subset \mathcal{O}_K$$

si k est premier à n, alors ζ_n^k est encore une racine primitive n-ième de l'unité, de sorte que $\frac{\zeta_n - 1}{\zeta_n^k - 1} \in \mathcal{O}_K$, ce qui implique que $u_k \in \mathcal{O}_K^\times$.

Définition 4.2.14. Le **groupe des unités cyclotomiques** est le sous-groupe de $\mathcal{O}_K^\times$ engendré par $\{u_k\}_{k \in (\mathbf{Z}/n\mathbf{Z})^\times}$.

Remarque 4.2.15. Les unités $\{u_k\}_{k\in(\mathbf{Z}/n\,\mathbf{Z})^\times}$ ne sont pas indépendantes dans $\mathcal{O}_K^\times/\mathbb{\mu}(K)$: on a $u_1 = 1$ et $u_{n-k} = -\zeta_n^{-k}u_k$: on peut se restreindre à $\{u_k\}_{\substack{1<k\leqslant n/2\\ \mathsf{pgcd}(k,n)=1}}$.

Lorsque n est une puissance d'un nombre premier, on sait que le groupe des unités cyclotomiques est d'indice fini dans $\mathcal{O}_K^\times$ (c'est faux en général).

Posons $K^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$: c'est le sous-corps de K des invariants par la conjugaison complexe. On a $[K : K^+] = 2$, l'extension $K^+/\mathbf{Q}$ est galoisienne de groupe $(\mathbf{Z}/n\,\mathbf{Z})^\times/\{\pm 1\}$, elle est de degré $\frac{\varphi(n)}{2}$. On a bien sûr $K^+ \subset \mathbf{R}$, de sorte que $K^+/\mathbf{Q}$ est totalement réelle. D'après le théorème des unités, rang du $\mathbf{Z}$-module $\mathcal{O}_{K^+}^\times$ est $\frac{\varphi(n)}{2} - 1$, égal à celui de $\mathcal{O}_K^\times$. Cela implique que le quotient $\mathcal{O}_K^\times/\mathcal{O}_{K^+}^\times$ est fini.

Proposition 4.2.16. Si $n = p$ est premier impair, l'application
$$\langle\zeta_p\rangle \times \mathcal{O}_{K^+}^\times \to \mathcal{O}_K^\times$$
est un isomorphisme.

Démonstration. On a $\langle\zeta_p\rangle \cap \mathcal{O}_{K^+}^\times = \{1\}$ (parce que $p > 2$ et $K^+ \subset \mathbf{R}$), de sorte que c'est un morphisme injectif : il s'agit de prouver la surjectivité. Soit $u \in \mathcal{O}_K^\times$. Comme $\mathcal{O}_K^\times/\mathcal{O}_{K^+}^\times$ est fini, il existe $r \in \mathbf{N}_{>0}$ tel que $u^r \in \mathcal{O}_{K^+}^\times$. On a alors $\overline{u}^r = u^r$, donc $\frac{\overline{u}}{u} \in \mathbb{\mu}(K) = \{\pm\zeta_p^k,\, k \in (\mathbf{Z}/n\,\mathbf{Z})^\times\}$: il existe $k \in (\mathbf{Z}/p\,\mathbf{Z})^\times$ tel que $\overline{u} = \pm\zeta_p^k u$.
Écrivons $u = \sum_{i=0}^{p-2} a_i\zeta_p^i \in \mathbf{Z}[\zeta_p]$: on a $\overline{u} = \sum_{i=0}^{p-2} a_i\zeta_p^{-i} \equiv \sum_{i=0}^{p-2} a_i \mod (\zeta_p - 1)\,\mathbf{Z}[\zeta_p]$. Cela implique que $\overline{u} \equiv u \mod (\zeta_p - 1)\,\mathbf{Z}[\zeta_p]$. Si on avait $\overline{u} = -\zeta_p^k u$, cela impliquerait $u \equiv -\zeta_p^k u \mod (\zeta_p - 1)\,\mathbf{Z}[\zeta_p]$, et donc $\zeta_p - 1 \mid 1 + \zeta_p^k$ (car u est inversible), d'où $\zeta_p - 1 \mid 2$ et $p \mid 2$, ce qui n'est pas. On a nécessairement $\overline{u} = \zeta_p^k u$.
Comme p est impair, 2 est inversible dans $(\mathbf{Z}/p\,\mathbf{Z})^\times$: il existe $\ell \in (\mathbf{Z}/p\,\mathbf{Z})^\times$ tel que $k = 2\ell$. On a alors $\overline{u} = \zeta_p^{2\ell}u$: si $v = \zeta_p^\ell u \in \mathcal{O}_K^\times$, on a $\overline{v} = v$ donc $v \in \mathcal{O}_{K^+}^\times$, et $u = \zeta_p^{-\ell}v$. □

4.3. **Le premier cas du théorème de Fermat.**

Théorème 4.3.1. (Grand théorème de Fermat) Soient $n \in \mathbf{N}_{\geqslant 3}$ et $x, y, z \in \mathbf{Z}$ tels que $x^n + y^n = z^n$. Alors $xyz = 0$.

Remarque 4.3.2.
(1) Il est très facile de paramétrer les solutions dans le cas $n = 1$. Dans le cas $n = 2$, les solutions sont (à permutation de x et y près) les triplets de la forme $(d(u^2 - v^2), 2duv, d(u^2 + v^2))$ avec $d \in \mathbf{N}_{>0}$ et $u, v \in \mathbf{Z}$ premiers entre eux.
(2) Pour pouver le théorème 4.3.1, il suffit de traiter le cas $n = 4$ (facile en utilisant le cas $n = 2$) et le cas n premier impair.
(3) S'appuyant sur de nombreux travaux, ce théorème a été prouvé par Wiles et Taylor-Wiles en 1995.

Fixons désormais $p > 2$ premier, $\zeta \in \mathbf{C}$ une racine primitive p-ième de l'unité et posons $K = \mathbf{Q}(\zeta)$. Rappelons (*cf* exemple 2.5.6) que $\mathcal{O}_K = \mathbf{Z}[\zeta]$.

Lemme 4.3.3. Si $\alpha \in \mathcal{O}_K$, alors $\alpha^p \in \mathbf{Z} + p\,\mathbf{Z}[\zeta]$.

Démonstration. Écrivons $\alpha = \sum_{i=0}^{p-2} a_i\zeta^i$ avec $a_0, \ldots, a_{p-2} \in \mathbf{Z}$. On a $\alpha^p \equiv \sum_{i=0}^{p-2} a_i^p\zeta^{ip} \mod p\,\mathbf{Z}[\zeta]$ d'où $\alpha^p \in \mathbf{Z} + p\,\mathbf{Z}[\zeta]$ (car $\zeta^p = 1$). □

Définition 4.3.4. On dit que p est **régulier** si $p \nmid h_K$.

Si p est régulier et $I \subset \mathcal{O}_K$ un idéal tel que I^p soit principal, alors I est déjà principal.

Théorème 4.3.5. Supposons p régulier et soit $x, y, z \in \mathbf{Z}$ tels que $x^p + y^p = z^p$. Alors $p \mid xyz$ (premier cas du théorème de Fermat).

Démonstration. Raisonnons pas l'absurde : soit $x, y, z \in \mathbf{Z}$ tels que $x^p + y^p = z^p$ et $p \nmid xyz$. Quitte à les diviser par leur pgcd, on peut supposer x, y et z premiers entre eux dans leur ensemble. Cela implique immédiatement qu'ils sont en fait deux à deux premiers entre eux.
Comme les cubes non nuls de $\mathbf{Z}/9\,\mathbf{Z}$ sont ± 1, une somme de deux cubes n'est pas un cube non nul modulo 9 : l'hypothèse implique que $p \neq 3$.
Si $x \equiv y \equiv -z \mod p\,\mathbf{Z}$, alors $z^p = x^p + y^p \equiv x + y \mod p\,\mathbf{Z}$, ce qui implique $z \equiv -2z \mod p\,\mathbf{Z}$, *i.e.* $p \mid 3z$, ce qui contredit $p \neq 3$ et $p \nmid z$: quitte à écrire $x^p + (-z)^p = (-y)^p$, on peut supposer que $x \not\equiv y \mod p\,\mathbf{Z}$.
On dispose de la factorisation

$$(*) \qquad z^p = \prod_{i=0}^{p-1} (x + \zeta^i y)$$

Lemme 4.3.6. On a $0 \leqslant i < j < p \Rightarrow \mathsf{pgcd}(x + \zeta^i y, x + \zeta^j y) = 1$.

Démonstration. Suposons le contraire : il existe $\mathfrak{p} \subset \mathcal{O}_K$ un idéal maximal avec $x + \zeta^i y, x + \zeta^j y \in \mathfrak{p}$. Cela implique $y\zeta^i(\zeta^{j-i} - 1) \in \mathfrak{p}$. Si on avait $y \in \mathfrak{p}$, on aurait aussi $x \in \mathfrak{p}$, de sorte que $x, y \in \mathbf{Z} \cap \mathfrak{p}$, contredisant le fait que x et y sont premiers entre eux : on a $y \notin \mathfrak{p}$. Comme ζ^i est une unité, on a aussi $\zeta^i \notin \mathfrak{p}$: on a nécessairement $\zeta^{j-i} - 1 \in \mathfrak{p}$. Comme $p = \mathsf{N}_{K/\mathbf{Q}}(\zeta^{j-i} - 1)$, cela implique que $\mathbf{Z} \cap \mathfrak{p} = p\,\mathbf{Z}$. Comme $x + \zeta^i y \mid z^p$, on a $z^p \in \mathfrak{p}$, donc $z \in \mathbf{Z} \cap \mathfrak{p}$, d'où $p \mid z$, contrairement à l'hypothèse. □

D'après le lemme 4.3.6, la factorisation $(*)$ implique que les idéaux $\{(x + \zeta^i y)\,\mathbf{Z}[\zeta]\}_{0 \leqslant i < p}$ sont des puissances p-ièmes d'idéaux. En particulier, il existe $I \subset \mathcal{O}_K$ tel que $I^p = (x + \zeta y)\,\mathbf{Z}[\zeta]$. Comme p est régulier et I^p est principal, il en est de même de I : il existe donc $\alpha \in \mathcal{O}_K$ et $u \in \mathcal{O}_K^\times$ tels que $x + \zeta y = u\alpha^p$.

D'après la proposition 4.2.16, il existe $k \in \{0, \dots, p-1\}$ et $v \in \mathcal{O}_{K^+}^\times$ tels que $u = \zeta^k v$. Par ailleurs, on a $\alpha^p \in \mathbf{Z} + p\,\mathbf{Z}[\zeta]$ en vertu du lemme 4.3.3 : il existe $\alpha_0 \in \mathbf{Z}$ tel que $x + \zeta y \equiv \zeta^k \alpha_0 v \mod p\,\mathbf{Z}[\zeta]$. En appliquant la conjugaison complexe, il vient aussi $x + \zeta^{-1} y \equiv \zeta^{-k} \alpha_0 v$, de sorte que $\zeta^{-k} x + \zeta^{1-k} y \equiv \zeta^k x + \zeta^{k-1} y \mod p\,\mathbf{Z}[\zeta]$, et donc $x + y\zeta - x\zeta^{2k} - y\zeta^{2k-1} \equiv 0 \mod p\,\mathbf{Z}[\zeta]$. Si $a = 2k - 1$, on a donc

$$(**) \qquad x + y\zeta - y\zeta^a - x\zeta^{a+1} \equiv 0 \mod p\,\mathbf{Z}[\zeta]$$

Premier cas : $\overline{a} \notin \{0, \pm 1, -2\}$: on a $\{\overline{a}, \overline{a} + 1\} \cap \{0, \pm 1\}$, et 1, ζ, ζ^a et ζ^{a+1} sont deux à deux distincts dans $\{1, \zeta, \dots, \zeta^{p-2}\}$. Comme $\mathbf{Z}[\zeta]$ est libre de base $\{1, \zeta, \dots, \zeta^{p-2}\}$ sur $\mathbf{Z}$, il en est de même de $\mathcal{O}_K/p\mathcal{O}_K$ sur $\mathbf{Z}/p\,\mathbf{Z}$. La congruence $(**)$ implique donc $p \mid x$ et $p \mid y$, ce qui n'est pas.
Deuxième cas : $\overline{a} = 0$. La congruence $(**)$ se réécrit $x - y + (y - x)\zeta \equiv 0 \mod p\,\mathbf{Z}[\zeta]$ *i.e.* $x \equiv y \mod p\,\mathbf{Z}$, ce qui n'est pas par hypothèse.
Troisième cas : $\overline{a} = 1$. La congruence $(**)$ se réécrit $x - x\zeta^2 \equiv 0 \mod p\,\mathbf{Z}[\zeta]$: on a $p \mid x$, ce qui n'est pas.
Quatrième cas : $\overline{a} = -1$. La congruence $(**)$ se réécrit $y\zeta - y\zeta^{-1} \equiv 0 \mod p\,\mathbf{Z}[\zeta]$ *i.e.* $y - y\zeta^2 \equiv 0 \mod p\,\mathbf{Z}[\zeta]$: on a $p \mid y$, ce qui n'est pas.
Cinquième cas : $\overline{a} = -2$. La congruence $(**)$ se réécrit $x + y\zeta - y\zeta^{p-2} - x\zeta^{p-1} \equiv 0 \mod p\,\mathbf{Z}[\zeta]$ *i.e.* $2x + (x + y)\zeta + x\zeta^2 + \cdots + x\zeta^{p-3} + (x - y)\zeta^{p-2} \equiv 0 \mod p\,\mathbf{Z}[\zeta]$ (parce que $1 + \zeta + \cdots + \zeta^{p-1} = 0$) : on a $p \mid x$, ce qui n'est pas.
On en déduit une contradiction, ce qui achève la preuve. □

Remarque 4.3.7. Voici la liste des nombres premiers inférieurs à 100, le nombre de classes de l'extension cyclotomique associée : les nombres irréguliers sont en rouge.

p	3	5	7	11	13	17
h_K	1	1	1	1	1	1
p	19	23	29	31	37	41
h_K	1	3	8	9	37	121
p	43	47	53	59	61	67
h_K	211	695	4889	41241	76301	853513
p	71	73	79	83	89	97
h_K	3882809	11957417	100146415	838216959	13379363737	411322842001

4.4. **Comptage des idéaux d'un corps de nombres.**

4.4.1. *Préliminaire : nombre de points à coordonnées entières de certains domaines de l'espace euclidien.* Soient $n \in \mathbf{N}_{>0}$ et μ la mesure de Lebesgue sur $\mathbf{R}^n$.

Définition 4.4.2. Soit $k \in \mathbf{N}_{>0}$. Une partie $S \subset \mathbf{R}^n$ est dite *k-Lipschitz-paramétrisable* s'il existe une famille finie $\{\varphi_i \colon [0,1]^k \to \mathbf{R}^n\}_{i\in I}$ d'applications lipschitziennes (*i.e.* telles qu'il existe $C \in \mathbf{R}_{\geqslant 0}$ tel que $\|\varphi_i(x) - \varphi_i(y)\|_2 \leqslant C\,\|x-y\|_2$ pour tout $x, y \in [0,1]^k$) dont les images recouvrent S.

Théorème 4.4.3. Soient $\Lambda \subset \mathbf{R}^n$ un réseau et $B \subset \mathbf{R}^n$ une partie mesurable. On suppose que la frontière ∂B de B est $(n-1)$-Lipschitz-paramétrisable. Alors

$$\#(\Lambda \cap tB) = \frac{\mu(B)}{\mu(\Lambda)} t^n + \mathsf{O}(t^{n-1})$$

quand t tend vers $+\infty$.

Démonstration. Soient $\mathbf{e}$ une base de Λ et $D_{\mathbf{e}}$ le domaine fondamental associé. On a $\mu(\Lambda) = \mu(D_{\mathbf{e}})$. Si $\lambda \in \Lambda \cap tB$, alors $(\lambda + D_{\mathbf{e}}) \cap tB \neq \varnothing$. En outre, on a soit $(\lambda + D_{\mathbf{e}}) \subset t\mathring{B}$, soit $(\lambda + D_{\mathbf{e}}) \cap t\partial B \neq \varnothing$. Notons $n(t)$ (resp. $m(t)$, resp. $b(t)$) le nombre de $\lambda \in \Lambda$ tels que $\lambda \in tB$ (resp. $(\lambda + D_{\mathbf{e}}) \subset t\mathring{B}$, resp. $(\lambda + D_{\mathbf{e}}) \cap t\partial B \neq \varnothing$) : d'après ce qui précède, on a

$$m(t) \leqslant n(t) \leqslant m(t) + b(t)$$

On a en outre $m(t)\mu(\Lambda) \leqslant \mu(tB) \leqslant (m(t) + b(t))\mu(\Lambda)$ *i.e.* $m(t) \leqslant \frac{\mu(B)}{\mu(\Lambda)} t^n \leqslant m(t) + b(t)$: il en résulte que $\left| n(t) - \frac{\mu(B)}{\mu(\Lambda)} t^n \right| \leqslant b(t)$. Il s'agit donc de montrer que $b(t) = \mathsf{O}(t^{n-1})$.
Soit $\{\varphi_i \colon [0,1]^k \to \mathbf{R}^n\}_{i\in I}$ une famille finie d'applications lipschitziennes dont les images recouvrent ∂B (avec constante de Lipschitz C). Les applications $\{t\varphi_i \colon [0,1]^k \to \mathbf{R}^n\}_{i\in I}$ paramétrisent la frontière $t\partial B$ de tB. Divisons chaque côté de $[0,1]^{n-1}$ en $\lfloor t \rfloor$ segments de longueur $\frac{1}{\lfloor t \rfloor}$: cela divise $[0,1]^{n-1}$ en $\lfloor t \rfloor^{n-1}$ petits cubes. L'image de chacun de ces petits cubes par φ_i a un diamètre inférieur à $C\frac{\sqrt{n}}{\lfloor t \rfloor}$, de sorte que l'image de chacun de ces petits cubes par $t\varphi_i$ est de diamètre inférieur à C' (avec $C' \sim \sqrt{n}C$ quand t tend vers $+\infty$). Le nombre de $\lambda \in \Lambda$ qui appartiennent à l'image de l'un de ces petits cubes est donc borné par une constante C'' (qui ne dépend que de Λ et C'). On a donc $b(t) \leqslant \#I C'' \lfloor t \rfloor^{n-1}$, *i.e.* $b(t) = \mathsf{O}(t^{n-1})$. □

4.4.4. *Le nombre d'idéaux dans une classe.* Soit K un corps de nombres de degré $n = r_1 + 2r_2$. Si $c \in \mathsf{Cl}(K)$ est une classe d'idéaux et $x \in \mathbf{R}_{>0}$, on note $N_K(x,c)$ le nombre d'idéaux $I \subset \mathcal{O}_K$ dont l'image dans $\mathsf{Cl}(K)$ est c, et tels que $\mathsf{N}(I) \leqslant x$. Le but de ce numéro est de prouver le théorème suivant :

Théorème 4.4.5. On a $N_K(x,c) = \frac{2^{r_1}(2\pi)^{r_2} R_K}{\#\mathbb{\mu}(K)\sqrt{|d_K|}} x + \mathsf{O}\left(x^{1-\frac{1}{n}}\right)$ (où R_K désigne le régulateur de K, *cf* définition 4.2.8).

Démonstration. Soit $J \subset \mathcal{O}_K$ un représentant de c^{-1}. D'après le théorème 4.1.24, on peut supposer que $\mathsf{N}(J) \leqslant C_K\sqrt{|d_K|}$, où $C_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}$ est la constante de Minkowski de K. Si $I \subset \mathcal{O}_K$ appartient à c vérifie $\mathsf{N}(I) \leqslant x$, alors IJ est principal, et de norme $\leqslant x\,\mathsf{N}(J)$, donc de la forme $\alpha\mathcal{O}_K$ avec $\alpha \in J$ et $N_{K/\mathbf{Q}}(\alpha) \leqslant x\,\mathsf{N}(J)$. Réciproquement, si $\alpha \in J$ vérifie $\mathsf{N}_{K/\mathbf{Q}}(\alpha) \leqslant x\,\mathsf{N}(J)$, alors $I = \alpha J^{-1} \subset \mathcal{O}_K$ (car $\alpha \in J$), et $\mathsf{N}(I) = \mathsf{N}_{K/\mathbf{Q}}(\alpha)\,\mathsf{N}(J)^{-1} \leqslant x$. Il s'agit donc de compter le nombre d'idéaux principaux $\alpha\mathcal{O}_K \subset J$ de norme $\leqslant x\,\mathsf{N}(J)$. Bien entendu, on peut se restreindre aux idéaux non nuls.

On note $\sigma_1, \ldots, \sigma_n$ les éléments de $\mathsf{Hom}_{K\text{-alg}}(K, \overline{\mathbf{Q}})$ (*cf* définition 4.1.17). On fixe $(e_{J,1}, \ldots, e_{J,n})$ une base de J sur $\mathbf{Z}$ (c'est donc une base de K sur $\mathbf{Q}$), et $u_1, \ldots, u_r$ un système d'unités fondamentales (où $r = r_1 + r_2 - 1$, *cf* définition 4.2.8). Soit $\ell \colon K^\times \to \mathbf{R}^{r+1}$ le plongement logarithmique, le groupe $\ell(\mathcal{O}_K^\times)$ est un réseau de $H = \mathsf{Ker}(\psi)$ où $\psi \colon \mathbf{R}^{r+1} \to \mathbf{R}$; $(t_1, \ldots, t_{r+1}) \mapsto \sum_{i=1}^{r_1} t_i + 2\sum_{j=r_1+1}^{r+1} t_j$.

Si $\alpha \in \mathcal{O}_K \backslash \{0\}$, on a

$$\widetilde{\ell}(\alpha) := \left(\ln|\sigma_1(\alpha)| - \tfrac{1}{n}\ln\left|\mathsf{N}_{K/\mathbf{Q}}(\alpha)\right|, \dots, \ln|\sigma_{r+1}(\alpha)| - \tfrac{1}{n}\ln\left|\mathsf{N}_{K/\mathbf{Q}}(\alpha)\right| \right) \in H$$

(car $\left|\mathsf{N}_{K/\mathbf{Q}}(\alpha)\right| = \prod_{i=1}^{r_1} |\sigma_i(\alpha)| \prod_{j=r_1+1}^{r+1} |\sigma_j(\alpha)|^2$). Comme $\big(\ell(u_1), \dots, \ell(u_r)\big)$ est une base de H sur $\mathbf{R}$, il existe $c_1, \dots, c_r \in \mathbf{R}$ uniques tels que

$$\widetilde{\ell}(\alpha) = \sum_{j=1}^{r} c_j \ell(u_j)$$

i.e. $(\forall i \in \{1, \dots, r+1\}) \sum_{j=1}^{r} c_j \ln|\sigma_i(u_j)| = \ln|\sigma_i(\alpha)| - \frac{1}{n}\ln\left|\mathsf{N}_{K/\mathbf{Q}}(\alpha)\right|$. Comme $\sigma_{i+r_2} = \overline{\sigma}_i$ pour $r_1 + 1 \leqslant i \leqslant r_1 + r_2$, l'égalité qui précède est valide pour tout $i \in \{1, \dots, n\}$. Par ailleurs, si $u = \zeta u_1^{n_1} \cdots u_r^{n_r} \in \mathcal{O}_K^\times$ (avec $\zeta \in \mathbb{\mu}(K)$ et $n_1, \dots, n_r \in \mathbf{Z}$), on a

$$\widetilde{\ell}(\alpha u) = \widetilde{\ell}(\alpha) + \widetilde{\ell}(u) = \widetilde{\ell}(\alpha) + \sum_{j=1}^{r} n_j \ell(u_j) = \sum_{j=1}^{r} (c_j + n_j)\ell(u_j)$$

Il en résulte que si $I \subset \mathcal{O}_K$ est un idéal principal, il admet modulo $\mathbb{\mu}(K)$ un unique générateur α tel que $\widetilde{\ell}(\alpha) = \sum_{j=1}^{r} c_j \ell(u_j)$ avec $0 \leqslant c_j < 1$ pour tout $i \in \{1, \dots, r\}$. Ainsi $\#\mathbb{\mu}(K) N_K(x, c)$ est le cardinal de l'ensemble des n-uples $(x_1, \dots, x_n) \in \mathbf{Z}^n$ tels que $\alpha = x_1 e_{J,1} + \cdots + x_n e_{J,n} \in J$ vérifie

$$\begin{cases} \mathsf{N}_{K/\mathbf{Q}}(\alpha) \leqslant x\,\mathsf{N}(J) & \text{(condition de norme)} \\ \widetilde{\ell}(\alpha) = \sum_{j=1}^{r} c_j \ell(u_j) \text{ avec } 0 \leqslant c_j < 1 \text{ pour tout } i \in \{1, \dots, r\} & \text{(condition de régulateur)} \end{cases}$$

Si $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{R}^n$, on pose $\alpha(\mathbf{x}) = \sum_{j=1}^{n} x_j e_{J,j} \in \mathbf{C}$ et $\alpha^{(i)}(\mathbf{x}) = \sum_{j=1}^{n} x_j \sigma_i(e_{J,j})$ pour tout $i \in \{1, \dots, n\}$. On pose $\mathsf{N}(\alpha(\mathbf{x})) = \alpha^{(1)}(\mathbf{x}) \cdots \alpha^{(n)}(\mathbf{x}) \in \mathbf{C}$. Lorsque $\mathbf{x} \in \mathbf{Q}^n$, on a $\alpha(\mathbf{x}) \in K$, $\alpha^{(i)}(\mathbf{x}) = \sigma_i(\alpha(\mathbf{x}))$ pour tout $i \in \{1, \dots, n\}$ et $\mathsf{N}(\alpha(\mathbf{x})) = \mathsf{N}_{K/\mathbf{Q}}(\alpha(\mathbf{x}))$. Bien entendu, la famille $(e_{J,1}, \dots, e_{J,n})$ est libre sur $\mathbf{Q}$, mais pas sur $\mathbf{R}$ *a priori* : il est parfaitement possible que $\alpha^{(i)}(\mathbf{x}) = 0$ (et donc $\mathsf{N}(\alpha(\mathbf{x})) = 0$) sans que $\mathbf{x}$ soit nul (on sait seulement que ça n'arrive pas lorsque $\mathbf{x} \in \mathbf{Q}^n$). On pose enfin

$$\widetilde{\ell}(\alpha(\mathbf{x})) = \left(\ln\left|\alpha^{(1)}(\mathbf{x})\right| - \tfrac{1}{n}\ln|\mathsf{N}(\alpha(\mathbf{x}))|, \dots, \ln\left|\alpha^{(r+1)}(\mathbf{x})\right| - \tfrac{1}{n}\ln|\mathsf{N}(\alpha(\mathbf{x}))| \right) \in \mathbf{R}^{r+1}$$

Considérons donc la région B_x de $\mathbf{R}^n$ définie par

$$B_x = \left\{ \mathbf{x} = (x_1, \dots, x_n) \in \mathbf{R}^n, \begin{cases} |\mathsf{N}(\alpha(\mathbf{x}))| \leqslant x\,\mathsf{N}(J) \\ (\forall i \in \{1, \dots, n\})\ \alpha^{(i)}(\mathbf{x}) \neq 0 \\ (\exists (c_j)_{1 \leqslant j \leqslant r} \in [0, 1[^r)\ \widetilde{\ell}(\alpha(\mathbf{x})) = \sum_{j=1}^{r} c_j \ell(u_j) \end{cases} \right\}$$

(noter la deuxième condition, présente pour donner un sens à la troisième). D'après ce qui précède, on a

$$\#\mathbb{\mu}(K) N_K(x, c) = \#(\mathbf{Z}^n \cap B_x)$$

Lemme 4.4.6. Si $\lambda \in \mathbf{R}_{>0}$, on a $B_{\lambda^n x} = \lambda B_x$, et donc $B_x = \sqrt[n]{x} B_1$.

Démonstration. Si $\mathbf{x} \in \mathbf{R}^n$, on a $\alpha^{(i)}(\lambda \mathbf{x}) = \lambda \alpha^{(i)}(\mathbf{x})$ donc $\mathsf{N}(\alpha(\lambda \mathbf{x})) = \lambda^n\, \mathsf{N}(\alpha(\mathbf{x}))$, ce qui implique $\widetilde{\ell}(\alpha(\lambda \mathbf{x})) = \widetilde{\ell}(\alpha(\mathbf{x}))$, et donc le lemme. □

Posons $M = \sup_{1 \leqslant i, j \leqslant r} |\ln|\sigma_i(u_j)||$.

Lemme 4.4.7. Si $\mathbf{x} \in B_1$, on a $\left|\alpha^{(i)}(\mathbf{x})\right| \leqslant e^{rM}\, \mathsf{N}(J)^{\frac{1}{n}}$ pour tout $i \in \{1, \dots, n\}$.

Démonstration. Comme $\ln\left(\frac{\left|\alpha^{(i)}(\mathbf{x})\right|}{|\mathsf{N}(\alpha(\mathbf{x}))|^{\frac{1}{n}}}\right) = \sum_{j=1}^{r} c_j \ln|\sigma_i(u_j)| \leqslant rM$, on a $\left|\alpha^{(i)}(\mathbf{x})\right| \leqslant e^{rM}\, |\mathsf{N}(\alpha(\mathbf{x}))|^{\frac{1}{n}}$. Comme $|\mathsf{N}(\alpha(\mathbf{x}))| \leqslant \mathsf{N}(J)$, on a donc $\left|\alpha^{(i)}(\mathbf{x})\right| \leqslant e^{rM} N(J)^{\frac{1}{n}}$. □

Lemme 4.4.8. La frontière ∂B_1 est $(n-1)$-Lipschitz-paramétrisable.

Démonstration. On a $\overline{B}_1 = \left\{\mathbf{x} \in \mathbf{R}^n,\ |\mathsf{N}(\alpha(\mathbf{x}))| \leqslant \mathsf{N}(J),\ (\forall i \in \{1,\dots,n\})\ \alpha^{(i)}(\mathbf{x}) \neq 0,\ \widetilde{\ell}(\alpha(\mathbf{x})) \in \sum_{j=1}^{r}[0,1]\ell(u_j)\right\}$: il résulte du lemme 4.4.7 que ∂B_1 est réunion finie de parties compactes des hypersurfaces $\mathsf{N}(\alpha(\mathbf{x})) = \pm\mathsf{N}(J)$ et $\ell(u_j)^*(\widetilde{\ell}(\alpha(\mathbf{x}))) \in \{0,1\}$ pour $j \in \{1,\dots,r\}$ (où $(\ell(u_j)^*)_{1\leqslant j\leqslant r}$ est la base duale de la base $(\ell(u_j))_{1\leqslant j\leqslant r}$ de H). Il s'agit donc de montrer que chacune de ces parties est $(n-1)$-Lipschitz-paramétrisable. Les équations définissant les hypersurfaces sont polynômiales : elles sont de classe $\mathscr{C}^\infty$. Il suffit donc de montrer que ce sont des variétés, *i.e.* que les équations définissent des submersions, soit encore que leurs différentielles ne s'annulent pas sur ∂B_1.
On a $\mathsf{N}(\alpha(\mathbf{x})) = \alpha^{(1)}(\mathbf{x})\cdots\alpha^{(n)}(\mathbf{x})$, donc $\mathrm{dln}(\mathsf{N}(\alpha))_{\mathbf{x}}(\mathbf{h}) = \sum_{i=1}^{n}\mathrm{dln}(\alpha_{\mathbf{x}}^{(i)})(\mathbf{h})$. Comme $\alpha^{(i)}$ est une forme linéaire, on a $\mathrm{d}\alpha_{\mathbf{x}}^{(i)} = \alpha^{(i)}$: on a $\frac{\mathrm{d}\,\mathsf{N}(\alpha)_{\mathbf{x}}(\mathbf{h})}{\mathsf{N}(\alpha(\mathbf{x}))} = \sum_{i=1}^{n}\frac{\alpha^{(i)}(\mathbf{h})}{\alpha^{(i)}(\mathbf{x})}$, et donc $\frac{\mathrm{d}\,\mathsf{N}(\alpha)_{\mathbf{x}}(\mathbf{x})}{\mathsf{N}(\alpha(\mathbf{x}))} = n$, *i.e.* $\mathrm{d}\,\mathsf{N}(\alpha)_{\mathbf{x}}(\mathbf{x}) = n\,\mathsf{N}(\alpha(\mathbf{x})) \neq 0$, en particulier $\mathrm{d}\,\mathsf{N}(\alpha)_{\mathbf{x}} \neq 0$. Cela prouve que les compacts des hypersurfaces d'équations $\mathsf{N}(\alpha(\mathbf{x})) = \pm\mathsf{N}(J)$ sont des variétés.
Pour $j \in \{1,\dots,r\}$, l'application $\ell(u_j)^*$ est une forme linéaire non nulle, donc une submersion : le cas hypersurfaces d'équations $\ell(u_j)^*(\widetilde{\ell}(\alpha(\mathbf{x}))) \in \{0,1\}$ résulte donc de la surjectivité de $\widetilde{\ell}(\alpha)$: $\mathbf{R}^n \to H$ (qui résulte de sa continuité et du fait que $\widetilde{\ell}(\mathcal{O}_K^\times)$ est un réseau de H (*cf* théorème 4.2.2 et sa preuve). □

D'après les lemmes 4.4.6 et 4.4.8, on peut appliquer le théorème 4.4.3 au réseau $\Lambda = \mathbf{Z}^n \subset \mathbf{R}^n$ et $B = B_1$. On a donc

$$\#\mathbb{\mu}(K)N_K(x,c) = \#(\mathbf{Z}^n \cap \sqrt[n]{x}B_1) = \mu(B_1)x + \mathsf{O}\left(x^{1-\frac{1}{n}}\right)$$

(parce que $\mu(\mathbf{Z}^n) = 1$).
Il reste donc à montrer que $\mathrm{vol}(B_1) = \frac{2^{r_1}(2\pi)^{r_2}R_K}{\sqrt{|d_K|}}$. Commençons par observer que dans la définition de B_x, les conditions $(\forall i \in \{1,\dots,n\})\ \alpha^{(i)}(\mathbf{x}) \neq 0$ définissent des sous-variétés de dimension $\leqslant n-1$: on a $\mathrm{vol}(B_1) = \mathrm{vol}(B_1^*)$, où B_1^* est la réunion de B_1 et de

$$\left\{\mathbf{x} = (x_1,\dots,x_n) \in \mathbf{R}^n,\ \begin{cases}(\exists i \in \{1,\dots,n\})\ \alpha^{(i)}(\mathbf{x}) = 0\\ (\forall j \in \{1,\dots,n\})\ \left|\alpha^{(j)}(\mathbf{x})\right| \leqslant e^{rM}\,\mathsf{N}(J)^{\frac{1}{n}}\end{cases}\right\}$$

(ce dernier ensemble est de mesure nulle : il ne sert qu'à se débarrasser de la condition de non annulation des $\alpha^{(i)}$). Pour calculer $\mathrm{vol}(B_1^*)$ on effectue le changement de variables suivant : on pose

$$\begin{aligned}\varphi\colon\ &\mathbf{R}^n \to \mathbf{R}^n\\ &\mathbf{x} \mapsto \big(\alpha^{(1)}(\mathbf{x}),\dots,\alpha^{(r_1)}(\mathbf{x}),\\ &\qquad\Re(\alpha^{(r_1+1)}(\mathbf{x})),\dots,\Re(\alpha^{(r_1+r_2)}(\mathbf{x})),\\ &\qquad\qquad\Im(\alpha^{(r_1+1)}(\mathbf{x})),\dots,\Im(\alpha^{(r_1+r_2)}(\mathbf{x}))\big)\end{aligned}$$

D'après la proposition 4.1.20, le jacobien de φ est égal à $2^{-r_2}\sqrt{|d_K|}\,\mathsf{N}(J)$., donc

$$\mathrm{vol}(B_1) = \frac{2^{r_2}}{\sqrt{|d_K|}\,\mathsf{N}(J)}\int_{\varphi(B_1^*)}\mathrm{d}y_1\cdots\mathrm{d}y_n = \frac{2^{r_1+r_2}}{\sqrt{|d_K|}\,\mathsf{N}(J)}\int_{\varphi(B_1^*)\cap\mathbf{R}_{\geqslant 0}^{R_1}\times\mathbf{R}^{2r_2}}\mathrm{d}y_1\cdots\mathrm{d}y_n$$

On passe maintenant en polaires : on pose $y_j = \rho_j$ pour $1 \leqslant j \leqslant r_1$ et $u_j + iu_{j+r_2} = \rho_j e^{i\theta_j}$ pour $r_1+1 \leqslant j \leqslant r_1+r_2$ (on a $\rho_i \geqslant 0$ pour tout[7] $i \in \{1,\dots,r_1+r_2\}$ et $\theta_i \in [0,2\pi[$ pour $i \in \{r_1+1,\dots,r_1+r_2\}$). Le jacobien de cette transformation est $\rho_{r_1+1}\cdots\rho_{r_1+r_2}$ de sorte que

$$\mathrm{vol}(B_1) = \frac{2^{r_1+r_2}(2\pi)^{r_2}}{\sqrt{|d_K|}\,\mathsf{N}(J)}\int_{C_1}\rho_{r_1+1}\cdots\rho_{r_1+r_2}\,\mathrm{d}\rho_1\cdots\mathrm{d}\rho_{r_1+r_2}$$

où C_1 est le domaine défini par $0 \leqslant \prod_{i=1}^{n}\rho_i^{e_i} \leqslant \mathsf{N}(J)$ et $\ln(\rho_i) - \frac{1}{n}\sum_{j=1}^{n}e_j\ln(\rho_j) = \sum_{k=1}^{r}c_k\ln|\sigma_i(u_k)|$ pour $i \in \{1,\dots,r_1+r_2\}$ (avec $e_i = 1$ si $1 \leqslant i \leqslant r_1$ et $e_i = 2$ si $r_1+1 \leqslant i \leqslant r_1+r_2$). On fait de

7. On s'est restreints à la partie de $\varphi(B_1^*)$ sur laquelle $y_i \geqslant 0$ pour avoir $\rho_i \geqslant 0$ pour $i \in \{1,\dots,r_1\}$.

nouveau un changement de variables en posant $\tau_i = \rho_i^{e_i}$, dont le jacobien vaut $\frac{1}{2^{r_2}\rho_{r_1+1}\cdots\rho_{r_1+r_2}}$: on a

$$\mathrm{vol}(B_1) = \frac{2^{r_2}(2\pi)^{r_2}}{\sqrt{|d_K|}\,\mathsf{N}(J)} \int_{D_1} \mathrm{d}\tau_1 \cdots \mathrm{d}\tau_{r_1+r_2}$$

où D_1 est le domaine défini par $0 < \prod_{i=1}^{r_1+r_2} \tau_i \leqslant \mathsf{N}(J)$ et $\ln(\tau_i) - \frac{e_i}{n} \sum_{j=1}^{n} \ln(\tau_j) = e_i \sum_{k=1}^{r} c_k \ln|\sigma_i(u_k)|$ pour $i \in \{1, \ldots, r_1 + r_2\}$. Posons enfin $u = \prod_{i=1}^{r_1+r_2} \tau_i$: le changement de variable $(\tau_1, \ldots, \tau_{r_1+r_2}) \mapsto (c_1, \ldots, c_r, u)$, dont le jacobien est précisément le régulateur R_K. On a donc

$$\mathrm{vol}(B_1) = \frac{2^{r_2}(2\pi)^{r_2}}{\sqrt{|d_K|}\,\mathsf{N}(J)} \int_{u=0}^{N(J)} \left(\int_{[0,1[^r} R_K \,\mathrm{d}c_1 \cdots \mathrm{d}c_r \right) \mathrm{d}u = \frac{2^{r_2}(2\pi)^{r_2}}{\sqrt{|d_K|}} R_K$$

et on a fini. □

Corollaire 4.4.9. Le nombre $N_K(x)$ d'idéaux de $\mathcal{O}_K$ de norme $\leqslant x$ vérifie

$$N_K(x) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{\#\mathbb{\mu}(K)\sqrt{|d_K|}} x + \mathsf{O}\left(x^{1-\frac{1}{n}}\right)$$

5. Théorie analytique

5.1. **Séries de Dirichlet.** Si $(a_n)_{n\in\mathbf{N}}$ est une suite d'entiers de nature combinatoire (par exemple $u_n = \#X_n$ où $\{X_n\}_{n\in\mathbf{N}}$ est une suite d'ensembles finis), il est souvent judicieux d'introduire la **série génératrice** associée, *i.e.* la série

$$S(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbf{Z}[\![X]\!]$$

Dans les bons cas, cette série a des propriétés analytiques (rayon de convergence non nul, équation fonctionnelle), et les propriétés assymptotiques de S fournissent des renseignements sur la suite $(a_n)_{n\in\mathbf{N}}$.

Exemple 5.1.1. Soient $r \in \mathbf{N}_{>0}$ et $\alpha_1, \dots, \alpha_r \in \mathbf{N}_{>0}$ premiers entre eux dans leur ensemble. On pose $X_n = \{(x_1, \dots, x_r) \in \mathbf{N}^r, \alpha_1 x_1 + \cdots + \alpha_r x_r = n\}$, $a_n = \#X_n$ et $S(X) = \sum\limits_{n=0}^{\infty} a_n X^n$. Comme $\frac{1}{1-X^\alpha} = 1 + X^\alpha + X^{2\alpha} + \cdots$, on a

$$S(X) = \frac{1}{(1-X^{\alpha_1})\cdots(1-X^{\alpha_r})}$$

En décomposant la fraction rationnelle en éléments simples, cela permet de trouver une formule pour a_n, grâce à la formule $a_n = \frac{1}{n!}S^{(n)}(0)$, ainsi que l'équivalent $a_n \sim \frac{n^{r-1}}{\alpha_1\cdots\alpha_r(r-1)!}$ dans n tend vers $+\infty$.

Pour les applications arithmétiques, on considère plutôt des fonctions du type suivant :

Définition 5.1.2. Soit $f\colon \mathbf{N}_{>0} \to \mathbf{C}$ une application. La **série de Dirichelet** associée est $F(s) = \sum\limits_{n=1}^{\infty} \frac{f(n)}{n^s}$.

Exemple 5.1.3. La **fonction zêta de Riemann** correspond au cas où $f = 1$: on a $\zeta(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$.

5.1.4. *Abscisses de convergence.*

Lemme 5.1.5. Si $f(n) = \mathsf{O}(n^k)$, la serie de Dirichelet associée converge absolument sur le demi-plan $\{s \in \mathbf{C}, \Re(s) > k+1\}$.

Démonstration. Si $s = x + iy$, on a $\left|\frac{f(n)}{n^s}\right| = \frac{|f(n)|}{n^x} = \mathsf{O}(n^{k-x})$: si $x > k+1$, la série $F(s)$ converge absolument. □

Ce phénomène est typique des séries de Dirichelet.

Définition 5.1.6. L'**abscisse de convergence simple (resp. absolue)** d'une série de Dirichelet F, est le plus grand élément $\sigma_c(f) \in \mathbf{R} \cup \{\pm\infty\}$ (resp. $\sigma_a(f) \in \mathbf{R} \cup \{\pm\infty\}$) tel que la série F diverge en tout point du demi-plan $\{s \in \mathbf{C}, \Re(s) < \sigma_c(f)\}$ (resp. $\inf\left\{\sigma \in \mathbf{R},\ \sum\limits_{n=1}^{\infty} \frac{|f(n)|}{n^\sigma} < \infty\right\}$).

Remarque 5.1.7. Une série de Dirichelet F converge absolument sur le demi-plan

$$\{s \in \mathbf{C}, \Re(s) > \sigma_a(f)\}$$

Proposition 5.1.8. Une série de Dirichelet F converge simplement sur le demi-plan

$$\{s \in \mathbf{C}, \Re(s) > \sigma_c(f)\}$$

La convergence est uniforme sur les secteurs de la forme $\{s \in \mathbf{C}, |\arg(s - s_0)| \leqslant \theta\}$, pour $\Re(s_0) > \sigma_c(f)$ et $\theta \in \left[0, \frac{\pi}{2}\right[$. En particulier, F est holomorphe sur son demi-plan de convergence, et pour tout $k \in \mathbf{N}$, on a $F^{(k)}(s) = \sum\limits_{n=1}^{\infty} \frac{f(n)(-\ln(n))^k}{n^s}$ pour $\Re(s) > \sigma_c(f)$. Par ailleurs, on a $\sigma_a(f) - 1 \leqslant \sigma_c(f) \leqslant \sigma_a(f)$.

Démonstration. Montrons la convergence uniforme sur les secteurs

$$\Delta_{s_0}(\theta) := \{s \in \mathbf{C},\ |\arg(s - s_0)| \leqslant \theta\}$$

(cela implique la convergence simple sur le demi-plan de convergence $\{s \in \mathbf{C},\ \Re(s) > \sigma_c(f)\}$, qui est réunion de ces secteurs). Quitte à translater par s_0, on peut supposer $s_0 = 0$. Soit $\varepsilon \in \mathbf{R}_{>0}$. Comme la série $\sum_{n=1}^{\infty} f(n)$ converge, il existe $N \in \mathbf{N}_{>0}$ tel que pour tout $p, q \in \mathbf{N}_{>0}$ tels que $N < p \leqslant q$ on ait $|\Sigma_{p,q}| \leqslant \varepsilon$ où $\Sigma_{p,q} := \sum_{n=p}^{q} f(n)$. Si $s \in \Delta_0(\theta)\backslash\{0\}$, on a $\Re(s) > 0$. En effectuant une transformation d'Abel, on a

$$\begin{aligned}\sum_{n=p}^{q} \frac{f(n)}{n^s} &= \sum_{n=p}^{q} \frac{\Sigma_{p,n} - \Sigma_{p,n-1}}{n^s} = \sum_{n=p}^{q} \frac{\Sigma_{p,n}}{n^s} - \sum_{n=p}^{q} \frac{\Sigma_{p,n-1}}{n^s} \\ &= \sum_{n=p}^{q} \frac{\Sigma_{p,n}}{n^s} - \sum_{n=p-1}^{q-1} \frac{\Sigma_{p,n}}{(n+1)^s} = \frac{\Sigma_{p,q}}{q^s} + \sum_{n=p}^{q-1} \Sigma_{p,n}\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)\end{aligned}$$

(avec la convention $\Sigma_{p,p-1} = 0$). Cela implique

$$\left|\sum_{n=p}^{q} \frac{f(n)}{n^s}\right| \leqslant \varepsilon\left(\frac{1}{q^{\Re(s)}} + \sum_{n=p}^{q-1}\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right|\right)$$

Comme $\frac{1}{n^s} - \frac{1}{(n+1)^s} = e^{-s\ln(n)} - e^{-s\ln(n+1)} = s\int_{\ln(n)}^{\ln(n+1)} e^{-ts}\,\mathrm{d}t$, on a

$$\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| \leqslant |s| \int_{\ln(n)}^{\ln(n+1)} e^{-t\Re(s)}\,\mathrm{d}t = \frac{|s|}{\Re(s)}\left(\frac{1}{n^{\Re(s)}} - \frac{1}{(n+1)^{\Re(s)}}\right)$$

De sorte que

$$\left|\sum_{n=p}^{q} \frac{f(n)}{n^s}\right| \leqslant \varepsilon\left(\frac{1}{q^{\Re(s)}} + \frac{|s|}{\Re(s)}\left(\frac{1}{p^{\Re(s)}} - \frac{1}{(q+1)^{\Re(s)}}\right)\right) \leqslant \varepsilon\left(1 + \frac{|s|}{\Re(s)}\right)$$

Comme $|\arg(s)| \leqslant \theta$, on a $\frac{\Re(s)}{|s|} = \cos(\arg(s)) \geqslant \cos(\theta)$, et donc

$$\left|\sum_{n=p}^{q} \frac{f(n)}{n^s}\right| \leqslant \varepsilon\left(1 + \frac{1}{\cos(\theta)}\right)$$

(valable aussi pour $s = 0$). La série définissant f vérifie donc le critère de Cauchy uniforme sur $\Delta_0(\theta)$: elle converge uniformément sur $\Delta_0(\theta)$.
D'après un théorème de Weiersterass, une série de fonctions holomorphes qui converge uniformément sur tout compact K d'un domaine Ω est holomorphe sur Ω, et on peut dériver terme à terme. Comme tout compact du demi-plan de convergence $\{s \in \mathbf{C},\ \Re(s) > \sigma_c(f)\}$ est inclus dans un secteur $\Delta_{s_0}(\theta)$ convenable (exercice facile), la fonction F est holomorphe sur son demi-plan de convergence.
L'inégalité $\sigma_c(f) \leqslant \sigma_a(f)$ est évidente. Soit maintenant $\sigma > \sigma_c(f) + 1$: il existe $\sigma_0 \in]\sigma_c(f), \sigma - 1[$. Comme $\sigma_0 > \sigma_c(f)$, la série $\sum_{n=1}^{\infty} \frac{f(n)}{n^{\sigma_0}}$ converge d'après ce qui précède : en particulier, la suite $\left\{\frac{f(n)}{n^{\sigma_0}}\right\}_{n\in\mathbf{N}_{>0}}$ est bornée, disons par M. On a alors $\frac{|f(n)|}{n^{\sigma}} = \frac{|f(n)|}{n^{\sigma_0}}\frac{1}{n^{\sigma-\sigma_0}} \leqslant \frac{M}{n^{\sigma-\sigma_0}}$. Comme $\sigma - \sigma_0 > 1$, la série de terme général $\left\{\frac{M}{n^{\sigma-\sigma_0}}\right\}_{n\in\mathbf{N}_{>0}}$ est convergente, ce qui prouve l'absolue convergence de la série $\sum_{n=1}^{\infty} \frac{f(n)}{n^{\sigma}}$. On a donc $\sigma \geqslant \sigma_a(f)$, ce qui prouve que $\sigma_a(f) \leqslant \sigma_c(f) + 1$. □

Remarque 5.1.9. (1) La série de Dirichelet converge pour $\Re(s) > \sigma_c(f)$ et diverge pour $\Re(s) < \sigma_c(f)$. C'est un résultat analogue au théorème d'Abel sur le rayon de convergence d'une série entière.
(2) Dans les exemples intéressants, les séries de Dedekind admettent des prolongements méromorphes sur des domaines strictement plus grands que leur demi-plan de convergence. C'est le cas, par exemple, de la fonction zêta de Riemann.

Proposition 5.1.10. Soient $f\colon \mathbf{N}_{>0} \to \mathbf{C}$ et $F(s)$ la série de Dirichelet associée. Supposons que pour tout $N \in \mathbf{N}$, on ait $\lim_{\sigma\to\infty} N^\sigma F(\sigma) = 0$. Alors $f = 0$.

Démonstration. On montre que $f(n) = 0$ par récurrence sur $n \in \mathbf{N}_{>0}$. Soit $N \in \mathbf{N}_{>0}$ tel que $f(1) = \cdots = f(N-1) = 0$ (condition vide si $N = 1$). Fixons $\sigma_0 > \sigma_a(f)$: la série $F(\sigma) = \sum_{n=N}^{\infty} \frac{f(n)}{n^\sigma}$ converge uniformément sur $[\sigma_0, +\infty[$ (*cf* proposition 5.1.8). On a donc

$$\lim_{\sigma\to\infty} N^\sigma F(\sigma) = \sum_{n=N}^{\infty} \lim_{\sigma\to\infty} N^\sigma \frac{f(n)}{n^\sigma} = f(N)$$

(car $\lim_{\sigma\to\infty} \left(\frac{N}{n}\right)^\sigma = 0$ si $n > N$). L'hypothèse implique donc que $f(N) = 0$. □

Corollaire 5.1.11. Soient $f, g\colon \mathbf{N}_{>0} \to \mathbf{C}$ et $F(s), G(s)$ les séries de Dirichelet associées. S'il existe $\sigma_0 \in \mathbf{R}$ tel que $(\forall \sigma \in [\sigma_0, +\infty[)\, F(\sigma) = G(\sigma)$, alors $f = g$. En particulier, si $\sigma_c(f) < +\infty$, la fonction f est entièrement déterminée par la série de Dirichelet $F(s)$.

5.1.12. *Produits eulériens.* Dans les applications arithmétiques, les fonctions $f\colon \mathbf{N}_{>0} \to \mathbf{C}$ qu'on considère ne sont pas arbitraires.

Définition 5.1.13. Une application $f\colon \mathbf{N}_{>0} \to \mathbf{C}$ est dite **multiplicative** (resp. **totalement multiplicative**) si $(\forall m, n \in \mathbf{N}_{>0})\ \mathsf{pgcd}(m, n) = 1 \Rightarrow f(mn) = f(n)f(m)$ (resp. $(\forall m, n \in \mathbf{N}_{>0})\, f(mn) = f(n)f(m)$).

Proposition 5.1.14. Soient $f\colon \mathbf{N}_{>0} \to \mathbf{C}$ multiplicative et $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ la série de Dirichelet associée. Alors

$$F(s) = \prod_{p\in\mathscr{P}} \left(\sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} \right)$$

pour tout $s \in \mathbf{C}$ tel que $\Re(s) > \sigma_a(f)$ (où $\mathscr{P}$ désigne l'ensemble des nombres premiers). En outre, le produit infini converge uniformément sur tout demi-plan de la forme $\{s \in \mathbf{C},\ \Re(s) > \sigma_0\}$ où $\sigma_0 > \sigma_a(f)$.

Démonstration. Pour $N \in \mathbf{N}_{>0}$, posons $\mathcal{E}_N = \{n \in \mathbf{N}_{>0},\ v_p(n) \neq 0 \Rightarrow p \leqslant N\}$: c'est l'ensemble des entiers non nuls dont tous les diviseurs premiers sont inférieurs à N. Bien entendu, on a $\{1, \ldots, N\} \subset \mathcal{E}_N$. Si $p \in \mathscr{P}$ et $\Re(s) > \sigma_a(f)$, on a $\sum_{k=0}^{\infty} \left|\frac{f(p^k)}{p^{ks}}\right| \leqslant \sum_{n=1}^{\infty} \left|\frac{f(n)}{n^s}\right| < +\infty$, de sorte que la série $\sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}}$ converge absolument. Par multiplicativité de f, on a alors

$$\prod_{\substack{p\in\mathscr{P}\\ p\leqslant N}} \left(\sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} \right) = \sum_{n\in\mathcal{E}_N} \frac{f(n)}{n^s}$$

ce qui implique que

$$\left| F(s) - \prod_{\substack{p\in\mathscr{P}\\ p\leqslant N}} \left(\sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} \right) \right| = \left| \sum_{n\notin\mathcal{E}_N} \frac{f(n)}{n^s} \right| \leqslant \sum_{n\notin\mathcal{E}_N} \frac{|f(n)|}{n^{\Re(s)}} \leqslant \sum_{n=N+1}^{\infty} \frac{|f(n)|}{n^{\Re(s)}}$$

La convergence absolue de $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ implique que $F(s) = \prod_{p\in\mathscr{P}} \left(\sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} \right)$ (en faisant tendre N vers $+\infty$). De plus, la convergence du produit infini est uniforme sur les demi-plans de la forme $\{s \in \mathbf{C},\ \Re(s) > \sigma_0\}$ pour $\sigma_0 > \sigma_a(f)$. □

Corollaire 5.1.15. Sous les hypothèse de la proposition 5.1.14, si f est totalement multiplicative, alors
$$F(s) = \prod_{p\in\mathscr{P}} \left(1 - \frac{f(p)}{p^s}\right)^{-1}$$
pour tout $s \in \mathbf{C}$ tel que $\Re(s) > \sigma_a(f)$.

Démonstration. Comme f est totalement multiplicative, pour $p \in \mathscr{P}$, on a $f(p^k) = f(p)^k$ pour tout $k \in \mathbf{N}$: la série $\sum\limits_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} = \sum\limits_{k=0}^{\infty} \left(\frac{f(p)}{p^s}\right)^k$ est géométrique de raison $\frac{f(p)}{p^s}$. Comme elle converge absolument, on a $\left|\frac{f(p)}{p^s}\right| < 1$, et sa somme vaut $\left(1 - \frac{f(p)}{p^s}\right)^{-1}$. □

Exemple 5.1.16. On a $\zeta(s) = \prod\limits_{p\in\mathscr{P}} (1 - p^{-s})^{-1}$ pour tout $s \in \mathbf{C}$ tel que $\Re(s) > 1$.

5.1.17. *Produit de deux séries de Dirichelet.* Soient $f\colon \mathbf{N}_{>0} \to \mathbf{C}$ et $g\colon \mathbf{N}_{>0} \to \mathbf{C}$ deux applications, et F, G les séries de Dirichelet associées.

Définition 5.1.18. Le **produit de convolution** de f et g est l'application
$$\begin{aligned} f * g\colon \mathbf{N}_{>0} &\to \mathbf{C} \\ n &\mapsto \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big) \end{aligned}$$

Proposition 5.1.19. (1) On a $\sigma_a(f * g) \leqslant \max(\sigma_a(f), \sigma_a(g))$.
(2) Pour tout $s \in \mathbf{C}$ tel que $\Re(s) > \max(\sigma_a(f), \sigma_a(g))$, on a
$$\sum_{n=1}^{\infty} \frac{(f * g)(n)}{n^s} = F(s)G(s)$$

Démonstration. Soit $s \in \mathbf{C}$ tel que $\sigma := \Re(s) > \max(\sigma_a(f), \sigma_a(g))$. Pour $N \in \mathbf{N}_{>0}$, on a
$$\begin{aligned} \sum_{1\leqslant n\leqslant N} \left|\frac{(f * g)(n)}{n^s}\right| &= \sum_{1\leqslant n\leqslant N} \frac{|(f * g)(n)|}{n^\sigma} = \sum_{1\leqslant n\leqslant N} \frac{1}{n^\sigma} \left|\sum_{d|n} f(d) g\Big(\frac{n}{d}\Big)\right| \\ &\leqslant \sum_{1\leqslant n\leqslant N} \sum_{\substack{d,\delta\in\mathbf{N}_{>0} \\ d\delta=n}} \frac{|f(d)|\,|g(\delta)|}{(d\delta)^\sigma} \leqslant \left(\sum_{d=1}^{N} \frac{|f(d)|}{d^\sigma}\right)\left(\sum_{\delta=1}^{N} \frac{|g(\delta)|}{\delta^\sigma}\right) \end{aligned}$$

Comme les séries $F(s)$ et $G(s)$ convergent absolument, il en est de même de la série $\sum\limits_{n=1}^{\infty} \frac{(f*g)(n)}{n^s}$: cela prouve (1).
Pour (2), le fait que la série double $\sum\limits_{n,m\in\mathbf{N}_{>0}} \frac{f(n)g(m)}{(nm)^s}$ converge absolument implique que l'on peut regrouper les termes arbitrairement. □

Exemple 5.1.20. Rappelons que la **fonction de Möbius** est l'application $\mu\colon \mathbf{N}_{>0} \to \mathbf{C}$ définie par $\mu(n) = 0$ si n est divisible par un carré > 1, et $\mu(p_1 \cdots p_r) = (-1)^r$ si $p_1, \ldots, p_r$ sont des nombres premiers deux à deux distincts. Si $f\colon \mathbf{N}_{>0} \to \mathbf{C}$ est une application et $g\colon \mathbf{N}_{>0} \to \mathbf{C}$ est définie par $g(n) = \sum\limits_{d|n} f(d)$, on a $f(n) = \sum\limits_{d|n} \mu(d) g\Big(\frac{n}{d}\Big)$ (formule d'inversion de Möbius). En particulier, pour tout $n \in \mathbf{N}_{>0}$, on a $(\mu * \mathbf{1})(n) \sum\limits_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$. Il en résulte que pour $\Re(s) > 1$, on a $\zeta(s)\left(\sum\limits_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right) = 1$: cela implique que $\zeta(s) \neq 0$, et que
$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

(comme $\mu(n) = \mathsf{O}(1)$, les abscisses de convergence absolue des deux séries sont < 1, *cf* lemme 5.1.5).

5.2. **Produits de Weierstass.** Soit f une fonction holomorphe sur $\mathbf{C}$. Si $r \in \mathbf{R}_{>0}$, on pose $M_r(f) = \sup_{|z|=r} |f(z)|$. On dit que f est d'**ordre fini** s'il existe $k \in \mathbf{R}_{\geqslant 0}$ et $r_0 \in \mathbf{R}_{>0}$ tels que $(\forall r \geqslant r_0)\ M_r(f) \leqslant e^{r^k}$. Dans ce cas, on pose

$$\rho_f = \limsup_{r\to\infty} \frac{\ln(\ln(M_r(f)))}{\ln(r)}$$

Pour $m \in \mathbf{N}_{>0}$, posons [8]

$$E(z,m) = (1-z)e^{z+\frac{z^2}{2}+\cdots+\frac{z^m}{m}}$$

On a alors :

Théorème 5.2.1. (de factorisation de Weierstass). Soient f holomorphe d'ordre fini et $\{a_n\}_{0\leqslant n\leqslant N}$ (avec N entier éventuellement infini) l'ensemble des zéros non nuls de f, comptés avec multiplicité. Alors il existe $P \in \mathbf{C}[X]$ de degré $\leqslant \rho_f$ et $m \in \mathbf{N}_{\leqslant \rho_f}$ tels que

$$f(z) = z^{\mathrm{ord}_0(f)} e^{P(z)} \prod_{n=0}^{N} E\Big(\frac{z}{a_n}, m\Big)$$

Démonstration. Voir [6, Théorème 15.10] et [1, IV.3.3]. □

Exemple 5.2.2. (1) On a $\sin(z) = \pi z \prod_{n\neq 0} \big(1-\frac{z}{n}\big)e^{\frac{z}{n}} = \pi z \prod_{n=1}^{\infty} \big(1-\frac{z^2}{n^2}\big)$;

(2) on a $\cos(z) = \prod_{n\neq 0} \big(1-\frac{z}{2n-1}\big)e^{\frac{2z}{2n-1}} = \prod_{n=1}^{\infty} \big(1-\frac{4z^2}{(2n-1)^2}\big)$;

Corollaire 5.2.3. Si f est d'ordre fini, et telle que $0 < \rho_f < 1$, alors f a une infinité de zéros.

Démonstration. Raisonnons par l'absurde : soient $a_1, \ldots, a_N$ les zéros non nuls de f (comptés avec multiplicité). Comme $\rho_f < 1$, on a nécessairement $m = 0$ dans la factorisation de Weierstrass de f : cette dernière s'écrit donc $f(z) = cz^{\mathrm{ord}_0(f)} \prod_{n=1}^{N} \big(1-\frac{z}{a_n}\big)$ *i.e.* $f(z) \in \mathbf{C}[z]$. Mais cela implique $\rho_f = 0$, contrairement à l'hypothèse. □

5.3. **La fonction Gamma.**

Définition 5.3.1. Pour $s \in \mathbf{C}$ tel que $\Re(s) > 0$, on pose

$$\Gamma(s) = \int_0^{\infty} t^{s-1} e^{-t}\, \mathrm{d}t$$

(l'intégrale est absolument convergente).

Proposition 5.3.2. (1) Pour tout $s \in \mathbf{C}$ tel que $\Re(s) > 0$, on a $\Gamma(s+1) = s\Gamma(s)$. On a $\Gamma(n) = (n-1)!$ pour tout $n \in \mathbf{N}_{>0}$.

(2) La fonction Γ admet un prolongement méromorphe sur $\mathbf{C}$, de pôles $\{-n\}_{n\in\mathbf{N}}$. Pour tout $n \in \mathbf{N}$, le pôle $-n$ est simple, de résidu $\frac{(-1)^n}{n!}$.

(3) Pour tout $s \in \mathbf{C}\setminus\mathbf{Z}$, on a

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$$

En particulier, on a $\Gamma\big(\frac{1}{2}\big) = \sqrt{\pi}$ et Γ n'a pas de zéro.

(4) On a

$$\Gamma(s) = \frac{2^{s-1}}{\sqrt{\pi}} \Gamma\Big(\frac{s}{2}\Big)\Gamma\Big(\frac{s+1}{2}\Big)$$

8. Observons que l'argument de l'exponentielle est la série $-\ln(1-z)$ tronquée à l'ordre m : en un sens, on peut voir $E(z,m)$ comme une approximation de 1 au voisinage de 0.

Démonstration. (1) résulte d'une intégration par parties. La formule pour $\Gamma(n)$ s'en déduit par récurrence, en partant de $\Gamma(1) = \int_0^\infty e^{-t}\,\mathrm{d}t = 1$.
(2) D'après (1), pour $n \in \mathbf{N}$, on a $\Gamma(s) = \frac{\Gamma(s+n+1)}{s(s+1)\cdots(s+n)}$: cela permet de prolonger Γ en une fonction méromorphe sur $\{s \in \mathbf{C}, \Re(s) > -n-1\}$, dont les pôles sont au plus simples, inclus dans $\{-n, -n+1, \ldots, -1, 0\}$. Par ailleurs, on a $\lim\limits_{s\to -n} \frac{\Gamma(s+n+1)}{s(s+1)\cdots(s+n-1)} = \frac{\Gamma(1)}{(-n)(-n+1)\cdots(-1)} = \frac{(-1)^n}{n!}$, de sorte que $\Gamma(s) \sim \frac{(-1)^n}{n!(s+n)}$ quand $s \to -n$. Cela prouve que le pôle $-n$ est simple, de résidu $\frac{(-1)^n}{n!}$.
(3) Considérons la fonction $f(s) = \Gamma(s)\Gamma(1-s)\sin(\pi s)$. Comme $s \mapsto \Gamma(s)\Gamma(1-s)$ est méromorphe de pôles $\mathbf{Z}$ tous simples, et $s \mapsto \sin(\pi s)$ est holomorphe de zéros $\mathbf{Z}$ tous simples, la fonction f est holomorphe sur $\mathbf{C}$. Par ailleurs, on a $f(s+1) = f(s)$: il existe une fonction holomorphe F définie sur $\mathbf{C}^\times$ telle que $f(s) = F(e^{2i\pi s})$. Par ailleurs, si $s = x + iy$ est tel que $0 \leqslant x \leqslant 1$ et $|y| \geqslant 1$, on a $|\Gamma(s)| = \frac{|\Gamma(x+1+iy)|}{|x+iy|} \leqslant \Gamma(x+1)$ et donc $|\Gamma(s)| \leqslant M := \max\limits_{x\in[1,2]} \Gamma(x)$. Comme $1 - s = 1 - x - iy$, on a aussi $|\Gamma(1-s)| \leqslant M$. Par ailleurs, on a $|\sin(\pi s)| \leqslant e^{\pi|y|}$, de sorte que $|f(s)| \leqslant M^2 e^{\pi|y|}$. Comme la fonction f est holomorphe sur $\mathbf{C}$, elle est bornée sur $\{s \in \mathbf{C},\ \Re(s) \in [0,1],\ \Im(s) \in [-1,1]\}$: on a donc $f(s) = \mathsf{O}(e^{\pi|y|})$ pour tout $s = x+iy$ tel que $0 \leqslant x \leqslant 1$. Par 1-périodicité de f, c'est vrai pour tout $s \in \mathbf{C}$. Il en résulte que $F(z) = \mathsf{O}\left(|z|^{-1/2}\right)$ quand $|z| \to 0$ (ce qui implique que F se prolonge en une fonction holomorphe sur $\mathbf{C}$), et que $F(z) = \mathsf{O}(\sqrt{|z|})$ quand $|z| \to \infty$, ce qui implique qu'elle est constante (avec les majorations de Cauchy des coefficients [9]). Comme $\Gamma(s) \sim \frac{1}{s}$ quand $s \to 0$ et $\Gamma(1) = 1$, on a $f(s) \sim \frac{\sin(\pi s)}{s} \underset{s\to 0}{\longrightarrow} \pi$, et $f = \pi$.
Avec $s = \frac{1}{2}$, la formule donne $\Gamma\left(\frac{1}{2}\right)^2 = \pi$, et donc $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$ vu que $\Gamma(x) > 0$ pour $x \in \mathbf{R}_{>0}$. La formule implique aussi que Γ ne s'annule pas.
(4) Considérons la fonction

$$g(s) = \frac{2^{s-1}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)}{\Gamma(s)}$$

Les pôles du numérateur et du dénominateurs sont les mêmes, tous simples. Il en résulte que g est holomorphe sur $\mathbf{C}$, sans pôles ni zéros. On a

$$g(s+1) = \frac{2^s\Gamma\left(\frac{s+1}{2}\right)\Gamma\left(\frac{s}{2}+1\right)}{\Gamma(s+1)} = \frac{2^s\frac{s}{2}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}+1\right)}{s\Gamma(s)} = g(s)$$

en vertu de (1), et g est 1-périodique. Il existe donc une fonction holomorphe G définie sur $\mathbf{C}^\times$ telle que $g(s) = G(e^{2i\pi s})$. D'après (3), on peut écrire

$$g(s) = \frac{2^{s-1}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)\Gamma(1-s)\sin(\pi s)}{\pi}$$

Si $s = x + iy$ avec $0 \leqslant x \leqslant 1$ et $|y| \geqslant 1$, on a $\left|\Gamma\left(\frac{s}{2}\right)\right| \leqslant M$, $\left|\Gamma\left(\frac{s+1}{2}\right)\right| \leqslant M$, $|\Gamma(1-s)| \leqslant M$, $|\sin(\pi s)| \leqslant e^{\pi|y|}$, de sorte que $|g(s)| \leqslant \frac{M^3}{2\pi}|2^s|\,e^{\pi|y|} = \mathsf{O}(e^{\pi|y|})$ (car $|2^s| = 2^x \leqslant 2$). Comme en (3), cela implique que g est constante. Comme $g(1) = \Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$, on a $g = \sqrt{\pi}$. □

Définition 5.3.3. La **constante d'Euler** est le nombre

$$\gamma = \sum_{k=1}^{\infty}\left(\frac{1}{k} - \ln\left(1+\frac{1}{k}\right)\right) = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \ln(n)\right) \approx 0.5772156649$$

Remarque 5.3.4. On ignore si γ est un nombre rationnel ou non.

9. Pour $r \in \mathbf{R}_{>0}$, on a $|F^{(k)}(0)| \leqslant \frac{k!}{r^k}\max\limits_{|z|=r}|F(z)| = \mathsf{O}(r^{1/2-k})$ donc $F^{(k)}(0) = 0$ pour tout $k \in \mathbf{N}_{>0}$ en faisant tendre r vers $+\infty$: on a $F = F(0)$.

Proposition 5.3.5. (1) **(Stirling)**. Pour $x \in \mathbf{R}_{>0}$, on a $\Gamma(x) \sim \left(\frac{x}{e}\right)^x \sqrt{2\pi x}$ quand $x \to \infty$.
(2) (Schlömilch) La fonction $\frac{1}{\Gamma(z)}$, holomorphe sur $\mathbf{C}$ (*cf* proposition 5.3.2 (4)), a pour factorisation de Weierstrass

$$\frac{1}{\Gamma(z)} = z e^{\gamma z} \prod_{n=1}^{\infty} \left(1 + \frac{z}{n}\right) e^{-\frac{z}{n}}$$

et $\Gamma'(1) = -\gamma$.

Démonstration. (1) On fait le changement de variable $t = x + u\sqrt{x}$: on a $t \in \mathbf{R}_{\geqslant 0} \Leftrightarrow u \geqslant -\sqrt{x}$. On a alors

$$\Gamma(x) = \int_{-\sqrt{x}}^{\infty} (x + u\sqrt{x})^x e^{-x-u\sqrt{x}} \sqrt{x}\, \mathrm{d}u = \left(\frac{x}{e}\right)^x \sqrt{x} I_{\sqrt{x}}$$

avec $I_y = \int_{-y}^{\infty} f_y(u)\, \mathrm{d}u$ où $f_y(u) = \left(1 + \frac{u}{y}\right)^{y^2} e^{-yu} = \exp\left(y^2 \ln\left(1 + \frac{u}{y}\right) - yu\right)$. Quand $y \to \infty$, on a $\ln\left(1+\frac{u}{y}\right) = \frac{u}{y} - \frac{u^2}{2y^2} + \mathsf{O}\left(\frac{1}{y^3}\right)$, donc $y^2 \ln\left(1+\frac{u}{y}\right) - yu = -\frac{u^2}{2} + \mathsf{O}\left(\frac{1}{y}\right)$, de sorte que $\lim_{y\to\infty} f_y(u) = e^{-\frac{u^2}{2}}$. Supposons $y \geqslant 1$. Si $u \in]-y, 0]$, on a $\alpha = \frac{u}{y} \in]-1, 0]$, donc $\ln(1+\alpha) \leqslant \alpha - \frac{\alpha^2}{2}$ (petit calcul), donc $y^2 \ln\left(1 + \frac{u}{y}\right) - yu \leqslant -\frac{u^2}{2}$ et $0 < f_y(u) \leqslant e^{-\frac{u^2}{2}}$. Si $u \geqslant 0$, on a [10] $y^2 \ln\left(1 + \frac{u}{y}\right) - yu \leqslant \ln(1+u) - u$, soit $0 < f_y(u) \leqslant (1+u)e^{-u}$. On peut donc appliquer le théorème de convergence dominée : on a [11]

$$\lim_{y\to\infty} I_y = \int_{-\infty}^{\infty} e^{-\frac{u^2}{2}}\, \mathrm{d}u = \sqrt{2\pi}$$

ce qui achève la preuve.
(2) Soit $z \in \mathbf{C}$ tel que $\Re(s) > 0$. On a $\Gamma(z) = \lim_{n\to\infty} \int_0^n t^{z-1}\left(1 - \frac{t}{n}\right)^n \mathrm{d}t$ par convergence dominée (car $0 \leqslant \left(1 - \frac{t}{n}\right)^n \leqslant e^{-\frac{t}{n}}$ pour tout $t \in [0, n]$, et $\lim_{n\to\infty} \left(1 - \frac{t}{n}\right)^n = e^{-\frac{t}{n}}$). En intégrant par parties, on a

$$\begin{aligned}
\int_0^n t^{z-1}\left(1 - \tfrac{t}{n}\right)^n \mathrm{d}t &= \underbrace{\left[\tfrac{t^z}{z}\left(1 - \tfrac{t}{n}\right)^n\right]_0^n}_{=0} + \tfrac{1}{z}\int_0^n t^z \left(1 - \tfrac{t}{n}\right)^{n-1} \mathrm{d}t \\
&= \tfrac{1}{z}\underbrace{\left[\tfrac{t^{z+1}}{z+1}\left(1 - \tfrac{t}{n}\right)^{n-1}\right]_0^n}_{=0} + \tfrac{1}{z(z+1)}\tfrac{n-1}{n}\int_0^n t^{z+1}\left(1 - \tfrac{t}{n}\right)^{n-2} \mathrm{d}t \\
&= \cdots = \tfrac{1}{z(z+1)\cdots(z+n-1)}\tfrac{(n-1)!}{n^{n-1}}\int_0^n t^{z+n-1}\, \mathrm{d}t = \tfrac{1}{z(z+1)\cdots(z+n-1)}\tfrac{(n-1)!}{n^{n-1}}\tfrac{n^{z+n}}{z+n}
\end{aligned}$$

De sorte que

$$\Gamma(z) = \lim_{n\to\infty} \frac{n! n^z}{z(z+1)\cdots(z+n)}$$

(formule d'Euler). En inversant, il vient

$$\begin{aligned}
\frac{1}{\Gamma(z)} &= \lim_{n\to\infty} n^{-z} z \left(1 + \tfrac{z}{1}\right)\left(1 + \tfrac{z}{2}\right)\cdots\left(1 + \tfrac{z}{n}\right) \\
&= \lim_{n\to\infty} z e^{-z\ln(n) + \sum_{k=1}^n \frac{z}{k}} \prod_{k=1}^n \left(1 + \tfrac{z}{k}\right) e^{-\frac{z}{k}} \\
&= z e^{\gamma z} \prod_{k=1}^{\infty} \left(1 + \tfrac{z}{k}\right) e^{-\frac{z}{k}}
\end{aligned}$$

10. Si $g_y(u) = \ln(1+u) + (y-1)u - y^2 \ln\left(1+\frac{u}{y}\right)$, on a $g_y'(u) = \frac{1}{1+u} + y - 1 - \frac{y^2}{y+u}$, donc $g_y''(u) = \frac{y^2}{(y+u)^2} - \frac{1}{(1+u)^2} \geqslant 0$ parce que $y \geqslant 1$ et $u \geqslant 0$. Cela implique que g_y' est croissante sur $\mathbf{R}_{\geqslant 0}$, et comme $g_y'(0) = 0$, on a g_y croissante sur $\mathbf{R}_{\geqslant 0}$: comme $g_y(0) = 0$, on a bien $g_y(u) \geqslant 0$ pour tout $u \geqslant 0$.

11. Soit $J = \int_0^{\infty} e^{-t^2}\, \mathrm{d}t$: on a $\int_{-\infty}^{\infty} e^{-\frac{u^2}{2}}\, \mathrm{d}u = 2\sqrt{2}J$. D'après le théorème de Fubini et en passant en coordonnées polaires, on a $J^2 = \int_{\mathbf{R}^2_{\geqslant 0}} e^{-(x^2+y^2)}\, \mathrm{d}x\, \mathrm{d}y = \int_{\theta=0}^{\frac{\pi}{2}} \int_{r=0}^{\infty} e^{-r^2} r\, \mathrm{d}r\, \mathrm{d}\theta$, de sorte que $J^2 = \frac{\pi}{4}$, soit $J = \frac{\sqrt{\pi}}{2}$.

En prenant la dérivée logarithmique, on en déduit

$$-\frac{\Gamma'(z)}{\Gamma(z)} = \frac{1}{z} + \gamma + \sum_{k=1}^{\infty} \Big(\frac{1}{k+z} - \frac{1}{k}\Big)$$

Évaluée en 1, cette égalité implique $\Gamma'(1) = -\gamma$ (car $\Gamma(1) = 1$). □

5.4. **La fonction Zêta de Riemann.** Rappelons que la fonction zêta de Riemann est la série de Dirichelet définie par

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

elle converge absolument pour $\Re(s) > 1$. Comme $\lim_{x \to 1^+} \zeta(x) = +\infty$, son abscisse de convergence et son abscisse de convergence absolue sont égales à 1. Rappelons en outre que ζ admet le produit eulérien

$$\zeta(s) = \prod_{p \in \mathscr{P}} (1 - p^{-s})^{-1}$$

et que $\zeta(s) \neq 0$ pour tout $s \in \mathbf{C}$ tel que $\Re(s) > 1$.

Lemme 5.4.1. (formule sommatoire d'Abel). Soient $(a_n)_{n \in \mathbf{N}_{>0}} \in \mathbf{C}^{\mathbf{N}_{>0}}$ et $f\colon [1, +\infty[\to \mathbf{C}$ de classe $\mathscr{C}^1$. Pour $x \in [1, +\infty[$, on pose $A(x) = \sum_{1 \leqslant n \leqslant x} a_n$. Alors pour tout $x \in [1, +\infty[$, on a

$$\sum_{1 \leqslant n \leqslant x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)\,\mathrm{d}t$$

Démonstration. On a

$$\begin{aligned}
\sum_{1 \leqslant n \leqslant x} a_n f(n) &= \sum_{1 \leqslant n \leqslant x} (A(n) - A(n-1))f(n) = \sum_{n=1}^{\lfloor x \rfloor} A(n)f(n) - \sum_{n=1}^{\lfloor x \rfloor} A(n-1)f(n) \\
&= A(\lfloor x \rfloor)f(\lfloor x \rfloor) - \sum_{n=1}^{\lfloor x \rfloor - 1} A(n)(f(n+1) - f(n)) \\
&= A(\lfloor x \rfloor)f(\lfloor x \rfloor) - \sum_{n=1}^{\lfloor x \rfloor - 1} \int_n^{n+1} A(t)f'(t)\,\mathrm{d}t \\
&= A(\lfloor x \rfloor)f(\lfloor x \rfloor) - \int_1^{\lfloor x \rfloor} A(t)f'(t)\,\mathrm{d}t = A(x)f(x) - \int_1^x A(t)f'(t)\,\mathrm{d}t
\end{aligned}$$

□

Proposition 5.4.2. La fonction ζ admet un prolongement méromorphe au demi-plan $\{s \in \mathbf{C},\ \Re(s) > 0\}$, avec un unique pôle d'ordre 1 en 1.

Démonstration. Si $t \in \mathbf{R}$, on note $\lfloor t \rfloor \in \mathbf{Z}$ sa partie entière et $\{t\} = t - \lfloor t \rfloor \in [0, 1[$ sa partie fractionnaire. La formule sommatoire d'Abel (avec $a_n = 1$ pour tout $n \in \mathbf{N}_{>0}$ et $f(t) = t^{-s}$) montre que

$$\begin{aligned}
\sum_{n=1}^{N} \frac{1}{n^s} &= \frac{1}{N^{s-1}} + s\int_1^N \frac{\lfloor t \rfloor}{t^{s+1}}\,\mathrm{d}t = \frac{1}{N^{s-1}} + s\int_1^N \frac{\mathrm{d}t}{t^s} - s\int_1^N \frac{\{t\}}{t^{s+1}}\,\mathrm{d}t \\
&= \frac{1}{(1-s)N^{s-1}} + \frac{s}{1-s} - s\int_1^N \frac{\{t\}}{t^{s+1}}\,\mathrm{d}t
\end{aligned}$$

Si $\sigma = \Re(s) > 1$, on a $\lim_{N \to \infty} N^{\sigma - 1} = 0$, ce qui implique

$$\zeta(s) = \frac{s}{s-1} - s\int_1^{\infty} \frac{\{t\}}{t^{s+1}}\,\mathrm{d}t = \frac{1}{s-1} + 1 - s\int_1^{\infty} \frac{\{t\}}{t^{s+1}}\,\mathrm{d}t$$

Comme $\left|\frac{\{t\}}{t^{s+1}}\right| \leqslant \frac{1}{t^{\sigma+1}}$, l'intégrale $\int_1^\infty \frac{\{t\}}{t^{s+1}}\,\mathrm{d}t$ converge absolument si $\sigma > 0$. Il en résulte que l'application

$$s \mapsto \zeta(s) - \frac{1}{s-1} = 1 - s\int_1^\infty \frac{\{t\}}{t^{s+1}}\,\mathrm{d}t$$

est holomorphe sur $\{s \in \mathbf{C},\ \Re(s) > 0\}$, et donc que ζ admet un prolongement méromorphe sur ce demi-plan, avec un unique pôle d'ordre 1 en 1. □

Corollaire 5.4.3. Si $t \in \mathbf{R}_{\geqslant 1}$, on a $\sum\limits_{\substack{p\in\mathscr{P}\\ k\geqslant 2}} p^{-kt} \leqslant 1$ et

$$\sum_{p\in\mathscr{P}} p^{-t} \sim -\ln(t-1)$$

lorsque $t \to 1^+$.

Démonstration. Pour $t \geqslant 1$, on a $\sum\limits_{k\geqslant 2} p^{-kt} = \frac{p^{-2t}}{1-p^{-t}} = \frac{1}{p^t(p^t-1)} \leqslant \frac{1}{p(p-1)}$, de sorte que

$$\sum_{\substack{p\in\mathscr{P}\\ k\geqslant 2}} p^{-kt} \leqslant \sum_{p\in\mathscr{P}} \frac{1}{p(p-1)} \leqslant \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1$$

Comme $\zeta(t) = \prod\limits_{p\in\mathscr{P}} (1-p^{-t})^{-1}$, on a

$$\ln(\zeta(t)) = \sum_{p\in\mathscr{P}} -\ln(1-p^{-t}) = \sum_{p\in\mathscr{P}} \left(\sum_{k=1}^{\infty} \frac{1}{kp^{kt}}\right) = \sum_{p\in\mathscr{P}} p^{-t} + R(t)$$

avec $R(t) = \sum\limits_{p\in\mathscr{P}} \left(\sum\limits_{k=2}^{\infty} \frac{1}{kp^{kt}}\right)$. Comme $0 \leqslant R(t) \leqslant \sum\limits_{p\in\mathscr{P}} \left(\sum\limits_{k=2}^{\infty} \frac{1}{p^{kt}}\right) \in [0,1]$, et comme $\ln(\zeta(t)) \sim -\ln(t-1)$ d'après la proposition 5.4.2, on a bien l'équivalent annoncé. □

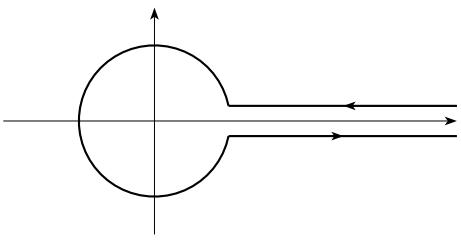
Théorème 5.4.4. (Riemann)
(1) La fonction ζ admet un prolongement méromorphe à $\mathbf{C}$, avec un unique pôle en 1.
(2) Si $I(s) = \frac{\Gamma(\frac{s}{2})\zeta(s)}{\pi^{\frac{s}{2}}}$, on a l'**équation fonctionnelle** :

$$I(s) = I(1-s)$$

Démonstration. (1) Soient $s \in \mathbf{C}$ tel que $\Re(s) > 1$ et $n \in \mathbf{N}_{>0}$. On a $\frac{\Gamma(s)}{n^s} = \int_0^\infty t^{s-1}e^{-nt}\,\mathrm{d}t$ par changement de variables, et donc $\Gamma(s)\zeta(s) = \int_0^\infty \frac{t^{s-1}\,\mathrm{d}t}{e^t-1}$ en sommant sur n. On fixe la détermination principale du logarithme sur $\mathbf{C}\setminus\mathbf{R}_{\geqslant 0}$ telle que $\Im(\ln(z)) \in [0, 2\pi[$ et on pose

$$J(s) = \int_{H_{r,\varepsilon}} \frac{z^{s-1}\,\mathrm{d}z}{e^z-1}$$

où $H_{r,\varepsilon}$ est le contour suivant [12] :



12. Appelé contour de Hankel.

où l'arc de cercle est de rayon $r \in]0, 2\pi[$ et les demi-droites horizontales sont situés à $\Im(z) \in \{\pm\varepsilon\}$. Lorsque r et ε varient, on reste dans une région du plan où la fonction que l'on intègre est holomorphe : l'intégrale $J(s)$ ne dépend ni de r, ni de ε, et est holomorphe en $s \in \mathbf{C}$.
On coupe l'intégrale en trois et on fait tendre ε vers 0 :

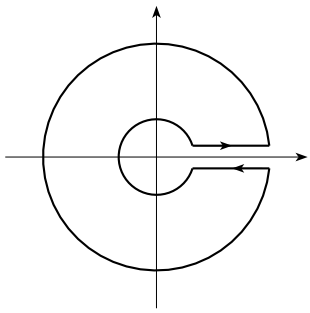
$$J(s) = \int_{|z|=r} \frac{z^{s-1}\,\mathrm{d}z}{e^z - 1} + \big(e^{2i\pi(s-1)} - 1\big) \int_r^\infty \frac{t^{s-1}\,\mathrm{d}t}{e^t - 1}$$

Comme la première intégrale est un $\mathsf{O}\left(r^{\Re(s)-1}\right)$, on en déduit que

$$(*) \qquad J(s) = \big(e^{2i\pi s} - 1\big)\Gamma(s)\zeta(s)$$

pour tout $s \in \mathbf{C}$ tel que $\Re(s) > 1$. Comme la fonction Γ admet un prolongement méromorphe à $\mathbf{C}$ (proposition 5.3.2 (2)), sans zéro, la fonction ζ admet elle aussi un prolongement méromorphe à $\mathbf{C}$, et l'égalité $(*)$ est valable sur $\mathbf{C}$.
Si s est un pôle de ζ avec $\Re(s) \leqslant 0$, on a $\big(e^{2i\pi s} - 1\big)\Gamma(s) = 0$, donc $e^{2i\pi s} = 1$ puisque Γ n'a pas de zéros (*cf* proposition 5.3.2 (4)), de sorte que $s = -n$ avec $n \in \mathbf{N}$. Mais comme Γ a un pôle simple et $s \mapsto e^{2i\pi s} - 1$ un zéro simple en $-n$, on a $\big(e^{2i\pi s} - 1\big)\Gamma(s) \neq 0$ pour $s = -n$, de sorte que ζ n'a pas de pôle sur $\{s \in \mathbf{C},\ \Re(s) \leqslant 0\}$. Joint à la proposition 5.4.2, cela montre que ζ n'a qu'un seul pôle, simple, en $s = 1$.

(2) Par prolongement analytique, il suffit de prouver l'égalité pour $\Re(s) < 0$. Considérons le contour $C_{r,k,\varepsilon}$



où le petit (resp. grand) arc de cercle a pour rayon $r \in]0, 2\pi[$ (resp. $(2k+1)\pi$ avec $k \in \mathbf{N}_{>0}$) et les segments horizontaux ont pour ordonnée $\pm\varepsilon$. La fonction $z \mapsto \frac{z^{s-1}}{e^z-1}$ est méromorphe sur $\mathbf{C}$, de pôles $2in\pi$ avec $n \in \mathbf{Z}$. D'après le théorème des résidus, on a donc

$$\frac{1}{2i\pi} \int_{C_{r,k,\varepsilon}} \frac{z^{s-1}\,\mathrm{d}z}{e^z - 1} = \sum_{1 \leqslant |n| \leqslant k} (2in\pi)^{s-1}$$

Comme $(-1)^{s-1} = e^{i\pi(s-1)}$, on a $\sum\limits_{1 \leqslant |n| \leqslant k} (2in\pi)^{s-1} = (2i\pi)^{s-1}(1 - e^{i\pi s}) \sum\limits_{n=1}^{k} n^{s-1}$. On a donc $\lim\limits_{k\to\infty} \int_{C_{r,k,\varepsilon}} \frac{z^{s-1}\,\mathrm{d}z}{e^z-1} = (2i\pi)^s(1 - e^{i\pi s})\zeta(1-s)$. Notons $\mathcal{C}_{k,\varepsilon}$ le grand arc de cercle. On a alors

$$\int_{C_{r,k,\varepsilon}} \frac{z^{s-1}\,\mathrm{d}z}{e^z - 1} = -J(s) + \mathsf{o}(1) + \int_{\mathcal{C}_{k,\varepsilon}} \frac{z^{s-1}\,\mathrm{d}z}{e^z - 1}$$

où $J(s)$ est l'intégrale considérée en (1) (le signe provenant du fait que le contour est parcouru dans le sens inverse), et le $\mathsf{o}(1)$ la contribution des demi-droites privées des segments horizontaux de $C_{r,k,\varepsilon}$. Comme $|e^z - 1| \geqslant \frac{1}{4}$ pour tout $z \in \mathcal{C}_{k,\varepsilon}$ (lemme 5.4.5), on a $\int_{\mathcal{C}_{k,\varepsilon}} \frac{z^{s-1}\,\mathrm{d}z}{e^z-1} = \mathsf{O}\left(k^{\Re(s)-1}\right) = \mathsf{o}(1)$ (car $\Re(s) < 0$). Il en résulte que $\lim\limits_{k\to\infty} \int_{C_{r,k,\varepsilon}} \frac{z^{s-1}\,\mathrm{d}z}{e^z-1} = -J(s) = -\big(e^{2i\pi s} - 1\big)\Gamma(s)\zeta(s)$ d'après $(*)$, donc $(2i\pi)^s(1 - e^{i\pi s})\zeta(1-s) = -\big(e^{2i\pi s} - 1\big)\Gamma(s)\zeta(s)$, *i.e.* $(2i\pi)^s\zeta(1-s) = \big(1 + e^{i\pi s}\big)\Gamma(s)\zeta(s)$, de sorte que

$$I(1-s) = \frac{\Gamma\big(\frac{1-s}{2}\big)\zeta(1-s)}{\pi^{\frac{1-s}{2}}} = \frac{\Gamma\big(\frac{1-s}{2}\big)\big(1 + e^{i\pi s}\big)\Gamma(s)\zeta(s)}{(2i\pi)^s\pi^{\frac{1-s}{2}}} = \frac{\Gamma\big(\frac{1-s}{2}\big)\big(1 + e^{i\pi s}\big)\Gamma(s)\pi^{\frac{s}{2}}I(s)}{(2i\pi)^s\pi^{\frac{1-s}{2}}\Gamma\big(\frac{s}{2}\big)}$$

Avec la détermination principale du logarithme choisie, on a $i^s = e^{i\frac{\pi}{2}s}$, de sorte que

$$I(1-s) = \frac{\Gamma\left(\frac{1-s}{2}\right)\left(e^{i\frac{\pi}{2}s} + e^{-i\frac{\pi}{2}s}\right)\Gamma(s)I(s)}{2^s\sqrt{\pi}\Gamma\left(\frac{s}{2}\right)} = \frac{\Gamma\left(\frac{1-s}{2}\right)\cos\left(\frac{\pi}{2}s\right)\Gamma\left(\frac{s+1}{2}\right)I(s)}{\pi}$$

(*cf* proposition 5.3.2 (4)). Mais d'après la proposition 5.3.2 (3), on a

$$\Gamma\left(\tfrac{1-s}{2}\right)\Gamma\left(\tfrac{s+1}{2}\right) = \frac{\pi}{\sin\left(\pi\frac{s+1}{2}\right)} = \frac{\pi}{\cos\left(\pi\frac{s}{2}\right)}$$

de sorte que $I(1-s) = I(s)$. □

Lemme 5.4.5. Si $k \in \mathbf{N}_{>0}$, on a $(\forall z \in \mathbf{C})\ |z| = (2k+1)\pi \Rightarrow |e^z - 1| > \frac{1}{4}$.

Démonstration. Raisonnons par l'absurde : soient $r \in \left]0, \frac{1}{4}\right]$ et $z = x+iy \in \mathcal{C}_k$ tels que $|e^z - 1| < r$. Il existe $\theta \in \mathbf{R}$ tel que $e^z - 1 = re^{i\theta}$, *i.e.* $e^x\cos(y) + ie^x\sin(y) - 1 = r\cos(\theta) + ir\sin(\theta)$, soit

$$\begin{cases} e^x\cos(y) = 1 + r\cos(\theta) \\ e^x\sin(y) = r\sin(\theta) \end{cases}$$

On a donc $1-r \leqslant e^x\cos(y) \leqslant 1+r$ et $|e^x\sin(y)| \leqslant r$, d'où $|\tan(y)| \leqslant \frac{r}{1-r} \leqslant 2r$. Comme $\cos(y) \geqslant 0$, on a $y \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] + 2\pi\mathbf{Z}$: il existe $m \in \mathbf{Z}$ tel que $y_0 = y - 2m\pi \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$. Comme en outre $|\tan(y_0)| \leqslant 2r$, on a $|y_0| \leqslant 2r$, de sorte que $|\sin(y)| \leqslant 2r$ et $\sqrt{1-4r^2} \leqslant \cos(y) \leqslant 1$. Comme $1 - r \leqslant e^x\cos(y) \leqslant 1 + r$, on a donc $1 - r \leqslant e^x \leqslant \frac{1+r}{\sqrt{1-4r^2}}$, soit encore $\frac{3}{4} \leqslant e^x \leqslant \frac{5}{2\sqrt{3}}$, et donc $-\pi < \ln\left(\frac{3}{4}\right) \leqslant x \leqslant \ln\left(\frac{5}{2\sqrt{3}}\right) < \pi$. On a donc $x^2 < \pi^2$: comme $x^2 + y^2 = (2k+1)^2\pi^2$, on a donc $\left(2k+\frac{1}{2}\right)^2\pi^2 < ((2k+1)^2 - 1)\pi^2 < y^2 \leqslant (2k+1)^2\pi^2$ (la première inégalité parce que $k \geqslant 1$), soit $2k\pi + \frac{\pi}{2} < y \leqslant (2k+1)\pi$, donc $|y - (2k+1)\pi| < \frac{\pi}{2}$. Mais on a $y = 2m\pi + y_0$ avec $|y_0| < \frac{\pi}{2}$, on a aussi $|y - 2m\pi| < \frac{\pi}{2}$: contradiction. □

Remarque 5.4.6. Au cours de la preuve du théorème 5.4.4, on a montré l'égalité $(2i\pi)^s\zeta(1-s) = \left(1 + e^{i\pi s}\right)\Gamma(s)\zeta(s)$, soit encore

$$\zeta(1-s) = \tfrac{2}{(2\pi)^s}\cos\left(\tfrac{\pi s}{2}\right)\Gamma(s)\zeta(s)$$

qui est une reformulation de l'équation fonctionnelle (moins symétrique que celle du théorème 5.4.4).

Corollaire 5.4.7. Les zéros de $\zeta(s)$ dans $\{s \in \mathbf{C},\ \Re(s) < 0\}$ sont $-2\,\mathbf{N}_{>0} = \{-2, -4, \ldots\}$ (on les appelle les **zéros triviaux**). Les autres appartiennent à $\{s \in \mathbf{C},\ 0 \leqslant \Re(s) \leqslant 1\}$.

Démonstration. La fonction $\Gamma\left(\frac{s}{2}\right)$ n'a ni zéro ni pôle sur $\{s \in \mathbf{C}, \Re(s) > 1\}$ (proposition 5.3.2). Il en est de même de $\zeta(s)$ (cela se voit sur le produit eulérien, absolument convergent sur $\{s \in \mathbf{C}, \Re(s) > 1\}$), donc de $I(s)$. Comme $I(s) = I(1-s)$, la fonction $I(s)$ n'a ni zéro ni pôle sur $\{s \in \mathbf{C}, \Re(s) < 0\}$. Sur ce domaine, la fonction $\Gamma\left(\frac{s}{2}\right)$ a pour pôles $-2\,\mathbf{N}_{>0}$, tous simples : ce sont donc les zéros de la fonction $\zeta(s)$ sur $\{s \in \mathbf{C}, \Re(s) < 0\}$, et ils sont tous simples. □

Définition 5.4.8. D'après ce qui précède, la fonction $I(s)$ a 0 et 1 pour deux seuls pôles, qui sont simples. Si

$$\xi(s) = \frac{s(s-1)}{2}I(s)$$

alors $\xi(s)$ est holomorphe sur $\mathbf{C}$, vérifie $\xi(1-s) = \xi(s)$, et ses zéros sont précisément les zéros non triviaux de la fonction $\zeta(s)$ (ils appartiennent donc à la bande $\{s \in \mathbf{C},\ 0 \leqslant \Re(s) \leqslant 1\}$ privée de 0 et 1). On pose aussi

$$\Xi(s) = \xi\left(\tfrac{1}{2} + is\right)$$

C'est une fonction holomorphe telle que $\Xi(-s) = \Xi(s)$.

Remarque 5.4.9. (Hypothèse de Riemann) Les zéros non triviaux de $\zeta(s)$ (*i.e.* les zéros de $\xi(s)$) sont situés sur la droite $\Re(s) = \frac{1}{2}$ (ce qui équivaut à dire que les zéros de Ξ sont tous réels). La localisation des zéros de la fonction $\zeta(s)$ a de nombreuses conséquences, notamment sur la répartition des nombres premiers (voir plus bas).

La fonction $\frac{z}{e^z-1}$ est développable en série entière au voisinage de 0 : il existe donc des nombres $(B_n)_{n\in\mathbf{N}}$ tels que

$$\frac{z}{e^z-1}=\sum_{n=0}^{\infty}\frac{B_n z^n}{n!}$$

Définition 5.4.10. Le nombre B_n s'appelle le n-ième **nombre de Bernoulli**.

Corollaire 5.4.11. (1) On a $B_n\in\mathbf{Q}$ pour tout $n\in\mathbf{N}$ et $B_{2n+1}=0$ pour tout $n\in\mathbf{N}_{>0}$.
(2) Pour $n\in\mathbf{N}$, on a [a] $\zeta(-n)=\frac{(-1)^n B_{n+1}}{n+1}$.
(3) On a $\zeta(2n)=-\frac{(2i\pi)^{2n}}{2(2n)!}B_{2n}\in\pi^{2n}\,\mathbf{Q}^\times$ pour tout $n\in\mathbf{N}_{>0}$.

a. On retrouve le fait que $\zeta(-2k)=0$ pour tout $k\in\mathbf{N}_{>0}$.

Démonstration. (1) La fonction $z\mapsto\frac{z}{e^z-1}$ est méromorphe sur $\mathbf{C}$, de pôles $2i\pi n$ pour $n\in\mathbf{Z}\backslash\{0\}$: elle admet bien un développement en série entière au voisinage de 0 : soit R son rayon de convergence. On a $\frac{e^z-1}{z}=\sum_{k=0}^{+\infty}\frac{z^k}{(k+1)!}$, donc

$$\sum_{k=0}^{n}\frac{B_k}{k!(n-k+1)!}=\begin{cases}1 & \text{si } n=0\\ 0 & \text{si } n>0\end{cases}$$

ce qui implique $B_0=1$ et $(n+1)B_n=-\sum_{k=0}^{n-1}\binom{n+1}{k}B_k$ pour $n>0$. Une récurrence immédiate implique que $B_n\in\mathbf{Q}$ pour tout $n\in\mathbf{N}$, et la formule précédente permet de calculer les B_n de proche en proche :

n	0	1	2	3	4	5	6	7	8	9	10
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$

Pour $x\in]-R,R[$, on a $\frac{x}{e^x-1}+\frac{x}{2}=\frac{x}{2}\frac{e^x+1}{e^x-1}=\frac{x}{2}\frac{e^{x/2}+e^{-x/2}}{e^{x/2}-e^{-x/2}}=\frac{x}{2}\frac{\cosh(x/2)}{\sinh(x/2)}$, ce qui implique que la fonction $x\mapsto\frac{x}{e^x-1}+\frac{x}{2}=1+\sum_{k=2}^{\infty}\frac{B_k}{k!}x^k$ est paire : on a $B_{2n+1}=0$ dès que $n\in\mathbf{N}_{>0}$.
(2) On reprend les notations de la preuve du théorème 5.4.4 (1). On a $s\Gamma(s)=\Gamma(s+1)$, donc $\Gamma(s)=\frac{\Gamma(s+n+1)}{s(s+1)\cdots(s+n)}$. Comme $\lim_{s\to-n}\frac{e^{2i\pi s}-1}{s+n}=2i\pi$ (c'est la dérivée de $s\mapsto e^{2i\pi s}$ en $-n$), on a $\lim_{s\to-n}(e^{2i\pi s}-1)\Gamma(s)=2i\pi\frac{\Gamma(1)}{(-1)^n n!}=\frac{2i\pi}{(-1)^n n!}$. Par ailleurs, on a $f_n(z):=\frac{z^{-n-1}}{e^z-1}=\sum_{k=0}^{+\infty}\frac{z^{k-n-2}B_k}{k!}$ au voisinage de 0 : le résidu de f_n en 0 est $\frac{B_{n+1}}{(n+1)!}$. Comme 0 est le seul pôle de f_n dans le domaine délimité par $H_{r,\varepsilon}$, le théorème des résidus implique que $J(-n)=\int_{H_{r,\varepsilon}}\frac{z^{-n-1}}{e^s-1}\,\mathrm{d}z=2i\pi\frac{B_{n+1}}{(n+1)!}$. Avec ce qui précède, on a donc

$$\tfrac{2i\pi}{(-1)^n n!}\zeta(-n)=\lim_{s\to-n}\big(e^{2i\pi s}-1\big)\Gamma(s)\zeta(s)=2i\pi\tfrac{B_{n+1}}{(n+1)!}$$

i.e. $\zeta(-n)=(-1)^n\frac{B_{n+1}}{n+1}$ (en particulier, $\zeta(-n)=0$ pour $n>0$ pair).
(3) L'équation fonctionnelle $I(s)=I(1-s)$ appliquée en $s=2n>0$ donne $\pi^{-n}\Gamma(n)\zeta(2n)=\pi^{n-\frac12}\Gamma\big(\frac12-n\big)\zeta(1-2n)$. On a $\Gamma(n)=(n-1)!$ et $\zeta(1-2n)=-\frac{B_{2n}}{2n}$ en vertu de ce qui précède. Par ailleurs, on a $\Gamma\big(\frac12-n\big)=\frac{\Gamma\big(\frac12\big)}{\big(\frac12-n\big)\big(\frac12-n+1\big)\cdots\big(-\frac12\big)}=\frac{2^n\sqrt{\pi}}{(-1)^n 1.3.5.\cdots.(2n-1)}=\frac{(-1)^n 4^n n!\sqrt{\pi}}{(2n)!}=\frac{(2i)^{2n}n!\sqrt{\pi}}{(2n)!}$ (*cf* proposition 5.3.2 (4)). On a donc $\pi^{-n}(n-1)!\zeta(2n)=-\pi^{n-\frac12}\frac{(2i)^{2n}n!\sqrt{\pi}}{(2n)!}\frac{B_{2n}}{2n}$ soit $\zeta(2n)=-\frac{(2i\pi)^{2n}}{2(2n)!}B_{2n}$. □

Corollaire 5.4.12. Au voisinage de 1, on a $\zeta(s)=\frac{1}{s-1}+\gamma+\mathsf{O}(|s-1|)$, et $\frac{\zeta'(s)}{\zeta(s)}=-\frac{1}{s-1}-\gamma+\mathsf{O}(|s-1|)$. On a en outre $\frac{\zeta'(0)}{\zeta(0)}=\ln(2\pi)$ et $\zeta'(0)=-\frac{\ln(2\pi)}{2}$.

Démonstration. Rappelons que $\zeta(s) = \frac{1}{s-1} + 1 - s\int_0^\infty \frac{\{t\}\,\mathrm{d}t}{t^{s+1}}$ (*cf* preuve de la proposition 5.4.2). On a donc

$$\lim_{s\to 1}\big(\zeta(s) - \tfrac{1}{s-1}\big) = 1 - \int_0^\infty \frac{\{t\}\,\mathrm{d}t}{t^2} = 1 - \lim_{n\to\infty}\int_0^n \frac{\{t\}\,\mathrm{d}t}{t^2}$$
$$= 1 - \lim_{n\to\infty}\sum_{k=0}^{n-1}\frac{t-k}{t^2}\,\mathrm{d}t = 1 - \lim_{n\to\infty}\Big(\ln(n) - \sum_{k=1}^{n}\tfrac{1}{k}\Big) = \gamma$$

Il en résulte que $\zeta(s) = \frac{1}{s-1} + \gamma + \sum_{n=1}^{\infty} a_n(s-1)^n = \frac{1}{s-1}\big(1 + \gamma(s-1) + \mathsf{O}(|s-1|^2)\big)$. En dérivant, il vient $\zeta'(s) = -\frac{1}{(s-1)^2} + \sum_{n=1}^{\infty} a_n(s-1)^{n-1} = -\frac{1}{(s-1)^2} + \mathsf{O}(1)$. Il en résulte que

$$\frac{\zeta'(s)}{\zeta(s)} = \Big(-\frac{1}{(s-1)^2} + \mathsf{O}(1)\Big)(s-1)\big(1 - \gamma(s-1) + \mathsf{O}(|s-1|^2)\big) = -\frac{1}{s-1} - \gamma + \mathsf{O}(|s-1|)$$

On prend la dérivée logarithmique de l'équation fonctionnelle de la remarque 5.4.6 : on a

$$-\frac{\zeta'(1-s)}{\zeta(1-s)} = -\ln(2\pi) - \frac{\pi}{2}\tan\Big(\frac{\pi s}{2}\Big) + \frac{\Gamma'(s)}{\Gamma(s)} + \frac{\zeta'(s)}{\zeta(s)}$$

Comme $\frac{\pi}{2}\tan\big(\frac{\pi s}{2}\big) = -\frac{\pi}{2}\frac{\cos\left(\frac{\pi(s-1)}{2}\right)}{\sin\left(\frac{\pi(s-1)}{2}\right)} = -\frac{1}{s-1} + \mathsf{O}(|s-1|)$, on en déduit que

$$-\frac{\zeta'(1-s)}{\zeta(1-s)} = -\ln(2\pi) + \gamma + \frac{\Gamma'(s)}{\Gamma(s)} + \mathsf{O}(|s-1|)$$

Mais $\frac{\Gamma'(1)}{\Gamma(1)} = -\gamma$ (*cf* proposition 5.3.5 (2)), il vient donc $\frac{\zeta'(0)}{\zeta(0)} = \ln(2\pi)$ en faisant tendre s vers 1. Comme $\zeta(0) = -\frac{1}{2}$, on a bien $\zeta'(0) = -\frac{\ln(2\pi)}{2}$. □

Lemme 5.4.13. Les fonctions $\xi(s)$ et $\Xi(s)$ sont d'ordre 1. En outre, il y a une infinité de zéros non triviaux.

Démonstration. Si $\sigma := \Re(s) > 0$, on a $\zeta(s) = \frac{1}{s-1} + 1 - s\int_1^\infty \frac{\{t\}}{t^{s+1}}\,\mathrm{d}t$: si $\sigma \geqslant \frac{1}{2}$, on a donc $|\zeta(s)| = \mathsf{O}(1) + \mathsf{O}\Big(|s|\int_1^\infty \frac{\mathrm{d}t}{t^{3/2}}\Big) = \mathsf{O}(|s|)$ (*cf* preuve de la proposition 5.4.2). Par ailleurs, on a $\big|\Gamma\big(\frac{s}{2}\big)\big| = \big|\int_0^\infty e^{-t}t^{\frac{s}{2}-1}\,\mathrm{d}t\big| \leqslant \Gamma\big(\frac{\sigma}{2}\big)$. D'après la formule de Stirling (*cf* proposition 5.3.5), on a $\Gamma\big(\frac{\sigma}{2}\big) = \mathsf{O}\big(\exp\big(\frac{\sigma}{2}\ln\big(\frac{\sigma}{2e}\big)\big)\sqrt{\pi\sigma}\big) = \mathsf{O}\big(\exp\big(\frac{\sigma\ln(\sigma)}{2}\big)\big)$, ce qui implique que

$$|\xi(s)| = \left|\frac{s(s-1)}{2}\frac{\Gamma\big(\frac{s}{2}\big)\zeta(s)}{\pi^{\frac{s}{2}}}\right| = \mathsf{O}\big(\exp\big(\tfrac{\sigma}{2}\ln(\sigma)\big)\,|s|^3\big)$$
$$= \mathsf{O}\big(\exp\big(\tfrac{|s|}{2}\ln(|s|)\big)\,|s|^3\big) = \mathsf{O}\big(\exp\big(|s|\ln(|s|)\big)\big)$$

(parce que $\big|\pi^{-\frac{s}{2}}\big| = \exp\big(-\Re(s)\frac{\ln(\pi)}{2}\big) \leqslant e^{-\frac{\ln(\pi)}{4}} = \mathsf{O}(1)$ vu que $\sigma \geqslant \frac{1}{2}$, et $\sigma \leqslant |s|$). Il en résulte que $\ln(|\xi(s)|) \leqslant |s|\ln(|s|) + \mathsf{O}(1)$, et $\ln(\ln(|\xi(s)|)) \leqslant \ln(|s|) + \ln(\ln(|s|)) + \mathsf{O}(1)$, de sorte que $\frac{\ln(\ln(|\xi(s)|))}{\ln(|s|)} \leqslant 1 + \mathsf{o}(1)$, ce qui implique $\rho_\xi \leqslant 1$. Il y a égalité parce que $\lim_{x\to\infty}\zeta(x) = 1$, de sorte que $\xi(x) \sim \frac{x^2}{2\pi^{\frac{x}{2}}}\Gamma\big(\frac{x}{2}\big)$, *i.e.* $\xi(x) \sim \frac{x^2}{2}\big(\frac{x}{2e\pi}\big)^{\frac{x}{2}}\sqrt{\pi x}$, donc $\ln(\xi(x)) \sim \frac{5}{2}\ln(x) + \frac{x}{2}\ln\big(\frac{x}{2e\pi}\big) + \frac{\ln(\pi)}{2} - \ln(2)$ *i.e.* $\ln(\xi(x)) \sim \frac{x}{2}\ln(x)$, si bien que $\ln(\ln(\xi(x))) \sim \ln(x)$.

Le fait que $\Xi(s)$ est d'ordre 1 en résulte. Par ailleurs, la fonction $\Xi(s)$ étant paire, il existe f holomorphe sur $\mathbf{C}$ telle que $\Xi(s) = f(s^2)$. On a alors $\rho_f = \frac{1}{2}$, ce qui implique que $f(s)$ a une infinité de zéros (corollaire 5.2.3) : il en est donc de même de $\Xi(s)$ et de $\xi(s)$. Comme les zéros de $\xi(s)$ sont précisément les zéros non triviaux de la fonction $\zeta(s)$, il y en a une infinité. □

Dans tout ce qui suit, on note Z l'ensemble des zéros non triviaux de $\zeta(s)$. On vient de voir que Z est infini.

Proposition 5.4.14. (Produit de Hadamard de $\zeta(s)$). On a

$$\zeta(s) = \frac{e^{bs}}{2(s-1)\Gamma\left(\frac{s}{2}+1\right)} \prod_{\rho\in Z} \left(1-\frac{s}{\rho}\right)e^{\frac{s}{\rho}} = \frac{e^{(b+\frac{\gamma}{2})s}}{2(s-1)} \prod_{\rho\in -2\,\mathbf{N}_{>0}\cup Z} \left(1-\frac{s}{\rho}\right)e^{\frac{s}{\rho}}$$

avec $b = \ln(2\pi) - 1 - \frac{\gamma}{2}$.

Démonstration. Comme $\xi(s)$ est holomorphe d'ordre 1 (*cf* lemme 5.4.13) et $\xi(0) = \frac{1}{2}$, le théorème 5.2.1 implique qu'il existe $b_0 \in \mathbf{C}$ tel que

$$\xi(s) = \frac{e^{b_0 s}}{2} \prod_{\rho\in Z} \left(1-\frac{s}{\rho}\right)e^{\frac{s}{\rho}}$$

Comme $\xi(s) = \frac{s(s-1)}{2\pi^{\frac{s}{2}}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \frac{s-1}{\pi^{\frac{s}{2}}}\Gamma\left(\frac{s}{2}+1\right)\zeta(s)$, on a donc (*cf* proposition 5.3.5 (2))

$$\begin{aligned}\zeta(s) &= \frac{2\pi^{\frac{s}{2}}}{s(s-1)\Gamma\left(\frac{s}{2}\right)}\xi(s) = \frac{e^{(b_0+\frac{\ln(\pi)+\gamma}{2})s}}{2(s-1)} \left(\prod_{n=1}^{\infty}\left(1+\frac{s}{2n}\right)e^{-\frac{s}{2n}}\right)\left(\prod_{\rho\in Z}\left(1-\frac{s}{\rho}\right)e^{\frac{s}{\rho}}\right)\\ &= \frac{\pi^{\frac{s}{2}}}{(s-1)\Gamma\left(\frac{s}{2}+1\right)}\xi(s) = \frac{e^{bs}}{2(s-1)\Gamma\left(\frac{s}{2}+1\right)} \prod_{\rho\in Z}\left(1-\frac{s}{\rho}\right)e^{\frac{s}{\rho}}\end{aligned}$$

avec $b = b_0 + \frac{\ln(\pi)}{2}$. En prenant la dérivée logarithmique, on a

$$\frac{\zeta'(s)}{\zeta(s)} = b - \frac{1}{s-1} - \frac{\Gamma'\left(\frac{s}{2}+1\right)}{2\Gamma\left(\frac{s}{2}+1\right)} + \sum_{\rho\in Z}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right)$$

En $s=0$, on tire $\frac{\zeta'(0)}{\zeta(0)} = b + 1 - \frac{\Gamma'(1)}{2\Gamma(1)}$, *i.e.* $b = \ln(2\pi) - 1 - \frac{\gamma}{2}$ (*cf* corollaire 5.4.12 et proposition 5.3.5 (2)). □

Remarque 5.4.15. Outre l'hypothèse de Riemann, de nombreuses questions restent ouvertes concernant la fonction $\zeta(s)$. Par exemple, on conjecture que $\{\zeta(2n+1)\}_{n\in\mathbf{N}_{>0}}$ est algébriquement indépendante sur $\mathbf{Q}(\pi)$. Actuellement, on sait seulement que $\zeta(3)$ est irrationnel (Apéry, 1978), qu'il existe une infinité de $\zeta(2n+1)$ irrationnels (Rivoal, 2000), et que l'un parmi $\zeta(5)$, $\zeta(7)$, $\zeta(9)$ et $\zeta(11)$ est irrationnel (Zudilin, 2001).

5.4.16. *Le théorème des nombres premiers.*

Définition 5.4.17. (1) La **fonction de comptage des nombres premiers** est

$$\begin{aligned}\pi\colon [2,+\infty[&\to \mathbf{N}\\ x &\mapsto \#\{p\in\mathscr{P},\, p\leqslant x\}\end{aligned}$$

(2) La fonction **d'écart logarithmique intégrale** est

$$\begin{aligned}\mathrm{Li}\colon [2,+\infty[&\to \mathbf{R}\\ x &\mapsto \int_2^x \frac{\mathrm{d}t}{\ln(t)}\end{aligned}$$

(3) La **fonction de Tchebychev** est

$$\begin{aligned}\psi\colon [2,+\infty[&\to \mathbf{R}\\ x &\mapsto \sum_{\substack{p\in\mathscr{P}\\ m\in\mathbf{N}_{>0}\\ p^m\leqslant x}} \ln(p)\end{aligned}$$

Théorème 5.4.18. (des nombres premiers). On a $\pi(s) \sim \frac{x}{\ln(x)}$ quand $x \to +\infty$, *i.e.* $\lim\limits_{x\to\infty} \frac{\pi(x)\ln(x)}{x} = 1$.

Remarque 5.4.19. Ce théorème a été conjecturé par Gauss et Legendre vers 1790, et démontré indépendamment par Hadamard [13] et de la Vallée-Poussin en 1896 sous la forme plus précise suivante : il existe une constante $c > 0$ telle que

$$\pi(x) = \mathrm{Li}(x) + \mathsf{O}\left(x \exp\left(-\sqrt{\tfrac{\ln(x)}{2c}}\right)\right)$$

L'hypothèse de Riemann implique l'approximation optimale suivante :

$$\pi(x) = \mathrm{Li}(x) + \mathsf{O}(\sqrt{x}\ln(x))$$

Lemme 5.4.20. Soient $\sigma \in \mathbf{R}_{>0}$ et $u \in \mathbf{R}$. On a

$$\frac{1}{2i\pi}\int_{\Re(s)=\sigma} \frac{e^{us}}{s}\,\mathrm{d}s = \begin{cases} 1 & \text{si } u > 0 \\ \frac{1}{2} & \text{si } u = 0 \\ 0 & \text{si } u < 0 \end{cases}$$

Démonstration. Supposons $u > 0$: pour $a, h \in \mathbf{R}_{>0}$, soit $R_{a,h}$ le contour rectangulaire de sommets $-a \pm ih$ et $\sigma \pm ih$ (parcouru dans le sens trigonométrique). D'après le théorème des résidus, on a $\frac{1}{2i\pi}\int_{R_{a,h}} \frac{e^{us}}{s}\,\mathrm{d}s = 1$, donc

$$\begin{aligned}\left|\frac{1}{2i\pi}\int_{\sigma-ih}^{\sigma+ih} \frac{e^{us}}{s}\,\mathrm{d}s - 1\right| &\leqslant \int_{-h}^{h}\left|\frac{e^{u(-a+it)}}{2\pi(-a+it)}\right|\mathrm{d}t + \int_{-a}^{\sigma}\left|\frac{e^{u(t+ih)}}{2\pi(t+ih)}\right|\mathrm{d}t + \int_{-a}^{\sigma}\left|\frac{e^{u(t-ih)}}{2\pi(t-ih)}\right|\mathrm{d}t \\ &\leqslant \int_{-h}^{h}\frac{e^{-au}}{2a\pi}\,\mathrm{d}t + 2\int_{-a}^{\sigma}\frac{e^{ut}}{2h\pi}\,\mathrm{d}t = \frac{he^{-au}}{a\pi} + \frac{e^{u\sigma}-e^{-au}}{uh\pi}\end{aligned}$$

de sorte que $\left|\frac{1}{2i\pi}\int_{\sigma-ih}^{\sigma+ih}\frac{e^{us}}{s}\,\mathrm{d}s - 1\right| \leqslant \frac{e^{u\sigma}}{uh\pi}$ en faisant tendre a vers $+\infty$. On obtient la première égalité en faisant tendre h vers $+\infty$.
Supposons $u < 0$: pour $a, h \in \mathbf{R}_{>0}$ avec $a > \sigma$, soit $R'_{a,h}$ le contour rectangulaire de sommets $a \pm ih$ et $\sigma \pm ih$. D'après le théorème des résidus, on a $\frac{1}{2i\pi}\int_{R_{a,h}} \frac{e^{us}}{s}\,\mathrm{d}s = 0$, donc

$$\begin{aligned}\left|\frac{1}{2i\pi}\int_{\sigma-ih}^{\sigma+ih} \frac{e^{us}}{s}\,\mathrm{d}s\right| &\leqslant \int_{-h}^{h}\left|\frac{e^{u(a+it)}}{2\pi(a+it)}\right|\mathrm{d}t + \int_{\sigma}^{a}\left|\frac{e^{u(t+ih)}}{2\pi(t+ih)}\right|\mathrm{d}t + \int_{\sigma}^{a}\left|\frac{e^{u(t-ih)}}{2\pi(t-ih)}\right|\mathrm{d}t \\ &\leqslant \int_{-h}^{h}\frac{e^{au}}{2a\pi}\,\mathrm{d}t + 2\int_{\sigma}^{a}\frac{e^{ut}}{2h\pi}\,\mathrm{d}t = \frac{he^{au}}{a\pi} + \frac{e^{au}-e^{-\sigma u}}{uh\pi}\end{aligned}$$

de sorte que $\left|\frac{1}{2i\pi}\int_{\sigma-ih}^{\sigma+ih}\frac{e^{us}}{s}\,\mathrm{d}s\right| \leqslant \frac{e^{\sigma u}}{uh\pi}$ en faisant tendre a vers $+\infty$. On obtient la troisième égalité en faisant tendre h vers $+\infty$.
Dans le cas $u = 0$, on a

$$\frac{1}{2i\pi}\int_{\Re(s)=\sigma}\frac{\mathrm{d}s}{s} = \frac{1}{2i\pi}\int_{-\infty}^{\infty}\frac{i\,\mathrm{d}t}{\sigma+it} = \frac{1}{2\pi}\int_{-\infty}^{\infty}\frac{(\sigma-it)\,\mathrm{d}t}{\sigma^2+t^2} = \frac{1}{2}$$

□

Lemme 5.4.21. Le théorème des nombres premiers équivaut à $\psi(s) \sim x$ quand $x \to +\infty$.

Démonstration. On a $\psi(x) = \sum_{\substack{p\in\mathscr{P}\\ p\leqslant x}} \ln(p)\left\lfloor\frac{\ln(x)}{\ln(p)}\right\rfloor \leqslant \sum_{\substack{p\in\mathscr{P}\\ p\leqslant x}} \ln(x) = \pi(x)\ln(x)$. Par ailleurs, si $\varepsilon \in]0,1[$, on a $\psi(x) \geqslant \sum_{\substack{p\in\mathscr{P}\\ x^{1-\varepsilon}\leqslant p\leqslant x}} \ln(p) \geqslant \sum_{\substack{p\in\mathscr{P}\\ x^{1-\varepsilon}\leqslant p\leqslant x}} (1-\varepsilon)\ln(x) = (1-\varepsilon)\ln(x)\big(\pi(x) + \mathsf{O}(x^{1-\varepsilon})\big)$.
On a donc $(1-\varepsilon)\big(\frac{\pi(x)\ln(x)}{x} + \mathsf{O}\left(\frac{\ln(x)}{x^\varepsilon}\right)\big) \leqslant \frac{\psi(x)}{x} \leqslant \frac{\pi(x)\ln(x)}{x}$ pour tout $\varepsilon \in]0,1[$: si $\pi(x) \sim \frac{x}{\ln(x)}$ quand $x \to +\infty$, on a $\lim_{x\to\infty}\frac{\psi(x)}{x} = 1$.
Réciproquement, on a $\frac{\psi(x)}{x} \leqslant \frac{\pi(x)\ln(x)}{x} \leqslant (1-\varepsilon)\frac{\psi(x)}{x} + \mathsf{O}\left(\frac{\ln(x)}{x^\varepsilon}\right)$: si $\psi(s) \sim x$ quand $x \to +\infty$, on a $\lim_{x\to\infty}\frac{\pi(x)\ln(x)}{x} = 1$. □

13. À Bordeaux !

Remarque 5.4.22. L'intérêt du lemme qui précède vient du fait qu'il est plus commode de travailler avec la fonction ψ, car c'est elle qui apparaît naturellement lorsqu'on étudie la fonction zêta.

Théorème 5.4.23. (formule explicite de Riemann) Pour $x \in \mathbf{R}_{>1}$ non puissance d'un nombre premier, on a

$$\psi(x) = x - \sum_{\rho \in Z} \frac{x^\rho}{\rho} - \ln(2\pi) - \frac{1}{2}\ln\left(1 - \frac{1}{x^2}\right)$$

Démonstration. On part de la dérivée logarithmique du produit de Hadamard de $\zeta(s)$ (*cf* proposition 5.4.14) :

$$\frac{\zeta'(s)}{\zeta(s)} = \underbrace{b + \frac{\gamma}{2}}_{=\ln(2\pi)-1} - \frac{1}{s-1} + \sum_{\rho \in -2\mathbf{N}_{>0} \cup Z} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) = \ln(2\pi) - \frac{s}{s-1} + \sum_{\rho \in -2\mathbf{N}_{>0} \cup Z} \frac{s}{(s-\rho)\rho}$$

Soit $\sigma \in \mathbf{R}_{>2}$. D'après le lemme 5.4.20, on a :

$$\frac{1}{2i\pi}\int_{\Re(s)=\sigma} \ln(2\pi)\frac{x^s}{s}\,\mathrm{d}s = \frac{1}{2i\pi}\int_{\Re(s)=\sigma} \ln(2\pi)\frac{e^{s\ln(x)}}{s}\,\mathrm{d}s = \ln(2\pi)$$

$$\frac{1}{2i\pi}\int_{\Re(s)=\sigma} -\frac{s}{s-1}\frac{x^s}{s}\,\mathrm{d}s = \frac{1}{2i\pi}\int_{\Re(s-1)=\sigma-1} -\frac{xe^{(s-1)\ln(x)}}{s-1}\,\mathrm{d}s = -x$$

$$\frac{1}{2i\pi}\int_{\Re(s)=\sigma} \frac{s}{(s-\rho)\rho}\frac{x^s}{s}\,\mathrm{d}s = \frac{1}{2i\pi}\int_{\Re(s-\rho)=\sigma-\Re(\rho)} \frac{x^\rho e^{(s-\rho)\ln(x)}}{s-\rho}\,\mathrm{d}s = \frac{x^\rho}{\rho}$$

(car $\sigma - \Re(\rho), \sigma - 1 > 0$ pour tout zéro ρ de $\zeta(s)$). Par convergence uniforme sur les compacts [14] de $\{s \in \mathbf{C},\ \Re(s) > 1\}$, on a

$$(*) \qquad \frac{1}{2i\pi}\int_{\Re(s)=\sigma} \frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}\,\mathrm{d}s = \ln(2\pi) - x + \sum_{\rho \in Z}\frac{x^\rho}{\rho} + \underbrace{\sum_{n \in \mathbf{N}_{>0}} \frac{x^{-2n}}{-2n}}_{=\frac{1}{2}\ln\left(1-x^{-2}\right)}$$

Évaluons maintenant cette intégrale en utilisant la dérivée logarithmique du produit eulérien :

$$\frac{\zeta'(s)}{\zeta(s)} = \sum_{p \in \mathscr{P}} \frac{-p^{-s}\ln(p)}{1-p^{-s}} = -\sum_{\substack{p \in \mathscr{P} \\ n \in \mathbf{N}_{>0}}} p^{-ns}\ln(p)$$

(série absolument convergente sur les compacts de $\{s \in \mathbf{C},\ \Re(s) > 1\}$). On a donc

$$\frac{1}{2i\pi}\int_{\Re(s)=\sigma} \frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}\,\mathrm{d}s = -\sum_{\substack{p \in \mathscr{P} \\ n \in \mathbf{N}_{>0}}} \frac{1}{2i\pi}\int_{\Re(s)=\sigma} \ln(p)\frac{e^{s(\ln(x)-n\ln(p))}}{s}\,\mathrm{d}s$$

D'après le lemme 5.4.20, on a $\frac{1}{2i\pi}\int_{\Re(s)=\sigma} \frac{e^{s(\ln(x)-n\ln(p))}}{s}\,\mathrm{d}s = \begin{cases} 1 & \text{si } p^n < x \\ 0 & \text{si } p^n > x \end{cases}$ (rappelons que x n'est pas une puissance d'un nombre premier), on a donc

$$\frac{1}{2i\pi}\int_{\Re(s)=\sigma} \frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}\,\mathrm{d}s = -\sum_{\substack{p \in \mathscr{P} \\ n \in \mathbf{N}_{>0} \\ p^n < x}} \ln(p) = -\psi(x)$$

Joint à l'égalité $(*)$, cela prouve le théorème. □

Remarque 5.4.24. Il existe une autre expression de la formule explicite : pour $x \in \mathbf{R}_{>1}$, on a

$$\sum_{n=1}^{\infty} \frac{1}{n}\pi\left(x^{\frac{1}{n}}\right) = \mathrm{Li}(x) - \sum_{\rho \in Z} \mathrm{Li}(x^\rho) + \int_x^\infty \frac{\mathrm{d}t}{t(t^2-1)\ln(t)} - \ln(2)$$

(où la somme est prise en associant ρ et $1-\rho$).

14. Il est sans doute nécessaire d'apparier d'abord les termes correspondant aux zéros ρ et $1-\rho$.

Théorème 5.4.25. (Hadamard, de La Vallée Poussin) On a $\Re(s) \geqslant 1 \Rightarrow \zeta(s) \neq 0$.

Démonstration. On sait déjà que $\zeta(s) \neq 0$ pour $\Re(s) > 1$ (cela résulte du produit eulérien de $\zeta(s)$). Soient $\sigma, t \in \mathbf{R}$ avec $\sigma > 1$. On a

$$|\zeta(\sigma+it)| = \prod_{p\in\mathscr{P}} \left|1-p^{-\sigma-it}\right|^{-1} = \prod_{p\in\mathscr{P}} \left((1-p^{-\sigma-it})(1-p^{-\sigma+it})\right)^{-\frac{1}{2}}$$

donc

$$\begin{aligned}\ln\big(|\zeta(\sigma+it)|\big) &= -\frac{1}{2}\sum_{p\in\mathscr{P}} \big(\ln(1-p^{-\sigma-it}) + \ln(1-p^{-\sigma+it})\big)\\ &= \frac{1}{2}\sum_{p\in\mathscr{P}}\sum_{n=1}^{\infty} \frac{p^{(-\sigma-it)n}+p^{(-\sigma+it)n}}{n}\\ &= \sum_{p\in\mathscr{P}}\sum_{n=1}^{\infty} \frac{\cos(nt\ln(p))}{np^{n\sigma}}\end{aligned}$$

Il en résulte que

$$\begin{aligned}\ln\big(\big|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)\big|\big) &= \sum_{p\in\mathscr{P}}\sum_{n=1}^{\infty} \frac{3+4\cos(nt\ln(p))+\cos(2nt\ln(p))}{np^{n\sigma}}\\ &= 2\sum_{p\in\mathscr{P}}\sum_{n=1}^{\infty} \frac{\big(1+\cos(nt\ln(p))\big)^2}{np^{n\sigma}} \geqslant 0\end{aligned}$$

ce qui implique que

$$\big|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)\big| \geqslant 1$$

Supposons maintenant que $\zeta(1+it) = 0$: on a $\zeta(\sigma+it) = \mathsf{O}(\sigma-1)$. Comme $\zeta(\sigma)^3 \sim \frac{1}{(\sigma-1)^3}$ et $\zeta(\sigma+2it) = \mathsf{O}(1)$ quant $\sigma \to 1$, on a $\lim_{\sigma\to 1^+} \zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it) = 0$, ce qui contredit l'inégalité qui précède. □

Proposition 5.4.26. Pour tout $\varepsilon \in \mathbf{R}_{>0}$, on a $\sum_{\rho\in Z} \frac{1}{\left|\rho-\frac{1}{2}\right|^{1+\varepsilon}} < +\infty$.

Démonstration. Montrons que les zéros de $\xi(s)$ (*i.e.* les éléments de Z) croissent suffisament vite. Si $R \in \mathbf{R}_{>0}$, soit $n(R)$ le nombre de zéros de $\xi(s)$ dans le disque $\{s \in \mathbf{C},\ \left|s-\frac{1}{2}\right| \leqslant R\}$. On applique le théorème de Jensen [15] à la fonction entière $\xi(s)$ sur le disque $\{s \in \mathbf{C},\ \left|s-\frac{1}{2}\right| \leqslant 2R\}$ (si $\xi(s)$ s'annule sur le cercle $\{s \in \mathbf{C},\ \left|s-\frac{1}{2}\right| = 2R\}$, on applique ce qui suit à $R+\eta$ à la place de R avec $\eta \in \mathbf{R}_{>0}$ suffisament petit). On a donc

$$\ln\left|\xi\left(\tfrac{1}{2}\right)\right| + \sum_{\substack{\rho\in Z\\ \left|\rho-\frac{1}{2}\right|\leqslant 2R}} \ln\left(\frac{2R}{\left|\rho-\frac{1}{2}\right|}\right) \leqslant C(2R)\ln 2R$$

(où $C \in \mathbf{R}_{>0}$ est une constante [16], *cf* lemme 5.4.13). Les nombres dans la somme sont positifs, et $\geqslant \ln(2)$ lorque $\left|\rho-\frac{1}{2}\right| \leqslant R$: on a $n(R)\ln(2) \leqslant 2CR\ln(2R) - \ln\left|\xi\left(\frac{1}{2}\right)\right|$ d'où

$$n(R) \leqslant \frac{2C}{\ln(2)} R\ln(R) + 2CR - \frac{\ln\left|\xi\left(\frac{1}{2}\right)\right|}{\ln(2)} \leqslant 3CR\ln(R)$$

pour R assez grand.
Montrons maintenant la proposition : on écrit $Z = \{\rho_n\}_{n\in\mathbf{N}_{>0}}$ de sorte que la suite $\left\{\left|\rho_n-\frac{1}{2}\right|\right\}_{n\in\mathbf{N}_{>0}}$ soit croissante. Soit $\{R_n\}_{n\in\mathbf{N}_{>0}}$ la suite de réels défine par $(3C+1)R_n\ln(R_n) = n$. D'après ce qu'on vient de voir, pour n assez grand, il y a au plus $\frac{3C}{3C+1}n$ racines $\rho \in Z$ dans le disque

15. Si f est une fonction holomorphe sur $U \supset \overline{\mathrm{D}(0,r)}$ et $\alpha_1, \ldots, \alpha_N$ les zéros de f dans $\overline{\mathrm{D}(0,r)}$ (comptés avec multiplicités), on a $\ln|f(0)| = -\sum_{k=1}^{N} \ln\left(\frac{r}{|\alpha_k|}\right) + \frac{1}{2\pi}\int_0^{2\pi} \ln\left|f(re^{i\theta})\right| \mathrm{d}\theta$, *cf* [6, Théorème 15.18].

16. On peut prendre $C = 1$.

$\{s \in \mathbf{C},\ \left|s-\frac{1}{2}\right| \leqslant R_n\}$. Il en résulte qu'il existe $n_0 \in \mathbf{N}$ tel que pour tout $n \geqslant n_0$, la n-ième racine ρ_n n'appartient pas à ce disque : on a $\left|\rho_n - \frac{1}{2}\right| > R_n$. On a donc

$$\sum_{n=n_0}^{\infty} \frac{1}{\left|\rho_n-\frac{1}{2}\right|^{1+\varepsilon}} \leqslant \sum_{n=n_0}^{\infty} \frac{1}{R_n^{1+\varepsilon}} = \sum_{n=n_0}^{\infty} \left(\frac{(3C+1)\ln(R_n)}{n}\right)^{1+\varepsilon} = (3C+1)^{1+\varepsilon} \sum_{n=n_0}^{\infty} \frac{1}{n^{1+\frac{\varepsilon}{2}}} \frac{\ln(R_n)^{1+\varepsilon}}{n^{\frac{\varepsilon}{2}}}$$

Par définition de R_n, on a $\ln(n) = \ln(R_n) + \ln(\ln(R_n)) + \ln(3C+1)$: quitte à augmenter n_0, on peut supposer que $\ln(n) \geqslant \ln(R_n)$ pour $n \geqslant n_0$. On a alors $\frac{\ln(R_n)^{1+\varepsilon}}{n^{\frac{\varepsilon}{2}}} \leqslant \frac{\ln(n)^{1+\varepsilon}}{n^{\frac{\varepsilon}{2}}} \xrightarrow[n\to\infty]{} 0$: quitte à augmenter n_0, on peut supposer que $\frac{\ln(R_n)^{1+\varepsilon}}{n^{\frac{\varepsilon}{2}}} \leqslant 1$ pour tout $n \geqslant n_0$. On a alors $\sum\limits_{n=n_0}^{\infty} \frac{1}{\left|\rho_n-\frac{1}{2}\right|^{1+\varepsilon}} \leqslant \sum\limits_{n=n_0}^{\infty} \frac{1}{n^{1+\frac{\varepsilon}{2}}} < +\infty$, ce qui permet de conclure. □

Démonstration du théorème 5.4.18. En procédant comme dans la preuve du théorème 5.4.23, on montre que

$$\int_0^x \psi(t)\,\mathrm{d}t = \frac{x^2}{2} - \ln(2\pi)x - \sum_{\rho\in Z} \frac{x^{\rho+1}}{\rho(\rho+1)} - \sum_{n=1}^{\infty} \frac{x^{1-2n}}{2n(2n-1)} + \frac{\zeta'(-1)}{\zeta(-1)}$$

Soit $\frac{1}{2} - \frac{1}{x^2}\int_0^x \psi(t)\,\mathrm{d}t = \frac{\ln(2\pi)}{x} + \sum\limits_{\rho\in Z} \frac{x^{\rho-1}}{\rho(\rho+1)} + \sum\limits_{n=1}^{\infty} \frac{x^{-(2n+1)}}{2n(2n-1)} - \frac{\zeta'(-1)}{\zeta(-1)x^2}$. Les séries $\sum\limits_{n=1}^{\infty} \frac{1}{2n(2n-1)}$ et $\sum\limits_{\rho\in Z} \frac{1}{|\rho(\rho+1)|}$ sont convergentes (la deuxième grâce à la proposition 5.4.26). Les séries $\sum\limits_{n=1}^{\infty} \frac{x^{-(2n+1)}}{2n(2n-1)}$ et $\sum\limits_{\rho\in Z} \frac{x^{\rho-1}}{\rho(\rho+1)}$ convergent donc uniformément sur $[2,+\infty[$ (on a $\left|x^{\rho-1}\right| \leqslant 1$). Leur limite en $+\infty$ est la somme des limites de ses termes. On a donc $\lim\limits_{x\to\infty} \sum\limits_{n=1}^{\infty} \frac{x^{-(2n+1)}}{2n(2n-1)} = 0$ et $\lim\limits_{x\to\infty} \sum\limits_{\rho\in Z} \frac{x^{\rho-1}}{\rho(\rho+1)} = 0$ (car $\Re(\rho) < 1$ pour tout $\rho \in Z$ en vertu du théorème 5.4.25), et donc $\frac{1}{2} - \frac{1}{x^2}\int_0^x \psi(t)\,\mathrm{d}t = \mathsf{o}(1)$, *i.e.* $\int_0^x \psi(t)\,\mathrm{d}t = \frac{x^2}{2} + \mathsf{o}(x^2)$. Si $\varepsilon \in]0,1[$, on a donc

$$\int_{(1-\varepsilon)x}^{x} \psi(t)\,\mathrm{d}t = \frac{x^2}{2}\big(1-(1-\varepsilon)^2\big) + \mathsf{o}(x^2) = \varepsilon x^2 - \frac{\varepsilon^2 x^2}{2} + \mathsf{o}(x^2)$$

Comme ψ est croissante, on a $\varepsilon x\psi((1-\varepsilon)x) \leqslant \int_{(1-\varepsilon)x}^{x} \psi(t)\,\mathrm{d}t \leqslant \varepsilon x\psi(x)$, *i.e.* $\psi((1-\varepsilon)x) \leqslant x - \frac{\varepsilon x}{2} + \mathsf{o}(x) \leqslant \psi(x)$ soit encore

$$\Big(1-\frac{\varepsilon}{2}\Big)x + \mathsf{o}(x) \leqslant \psi(x) \leqslant \frac{1}{1-\varepsilon}\Big(1-\frac{\varepsilon}{2}\Big)x + \mathsf{o}(x)$$

Comme c'est vrai pour tout $\varepsilon \in]0,1[$, on a $\psi(x) \sim x$, ce qui permet de conclure en utilisant le lemme 5.4.21. □

5.5. Fonctions L de Dirichlet et théorème de la progression arithmétique.

5.5.1. *Caractères des groupes abéliens finis.* Soit G un groupe fini.

Définition 5.5.2. Un **caractère** de G est un morphisme de groupes $G \to \mathbf{C}^\times$. On note $\widehat{G}$ l'ensemble des caractères de G.

Proposition 5.5.3. Supposons G abélien.
(1) Muni de la multiplication naturelle, $\widehat{G}$ est un groupe abélien, isomorphe à G (non canoniquement.
(2) Le morphisme d'évaluation
$$G \to \widehat{\widehat{G}}$$
$$g \mapsto (\chi \mapsto \chi(g))$$
est un isomorphisme.
(3) (Relations d'orthogonalité) Si $g \in G$, on a $\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} \#G & \text{si } g = 1 \\ 0 & \text{sinon} \end{cases}$.
(4) Si $\chi \in \widehat{G}$, on a $\sum_{g \in G} \chi(g) = \begin{cases} \#G & \text{si } \chi = 1 \\ 0 & \text{sinon} \end{cases}$.

Démonstration. (1) Comme G est abélien, il est isomorphe (non canoniquement) à un produit de groupes cycliques : il suffit de traiter le cas où $G = \mathbf{Z}/n\,\mathbf{Z}$. On a alors
$$\widehat{G} = \mathbb{\mu}_n(\mathbf{C}) \simeq \mathbf{Z}/n\,\mathbf{Z}$$
$$\chi \mapsto \chi(1)$$
(2) Comme $\#\widehat{\widehat{G}} = \#\widehat{G} = \#G$ d'après (1), il suffit de voir que le morphisme est injectif. Là encore, on peut supposer G cyclique, cas dans lequel c'est évident.
(3) C'est évident si $g = 1$. Si $g \neq 1$, il existe $\chi_1 \in \widehat{G}$ tel que $\chi_1(g) \neq 1$ (d'après (2)). On a alors $\chi_1(g) \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \chi(g)$, donc $\sum_{\chi \in \widehat{G}} \chi(g) = 0$.
(4) n'est autre que (3) appliqué à $\widehat{G}$ à la place de G. □

Définition 5.5.4. Soit $m \in \mathbf{N}_{>0}$. Un **caractère de Dirichelet** modulo m est un caractère du groupe $(\mathbf{Z}/m\,\mathbf{Z})^\times$. On note χ_0 le caractère trivial [a].

a. *I.e.* constant égal à 1.

Dans ce qui suit, on note $\overline{x}$ l'image d'un entier x dans $\mathbf{Z}/m\,\mathbf{Z}$. Si χ est un caractère de Dirichelet modulo m, et $x \in \mathbf{Z}$, on pose
$$\chi(x) = \begin{cases} \chi(\overline{x}) & \text{si } \mathsf{pgcd}(x, m) = 1 \\ 0 & \text{sinon} \end{cases}$$
Remarquons que $(\forall x, y \in \mathbf{Z})\ \chi(xy) = \chi(x)\chi(y)$.

5.5.5. *Fonctions L de Dirichlet.* Soient $m \in \mathbf{N}_{>0}$ et χ un caractère de Dirichelet modulo m.

Définition 5.5.6. La **fonction L de Dirichelet** associée à χ est la série de Dirichelet
$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

Remarque 5.5.7. Lorsque $m = 1$, on a nécessairement $\chi = \chi_0$, et on obtient la fonction zéta de Riemann.

Lemme 5.5.8. Soit $(z_n)_{n \in \mathbf{N}_{>0}}$ est une suite de nombres complexes. Pour $x \in [1, +\infty[$, on pose $A(x) = \sum_{n \leqslant x} z_n$. Supposons que $A(x) = \mathsf{O}(x^r)$ quand $x \to +\infty$. Alors la série de Dirichelet $\sum_{n=1}^{\infty} \frac{z_n}{n^s}$ a pour abscisse de convergence $< r$, et définit donc une fonction holomorphe sur $\{s \in \mathbf{C},\ \Re(s) > r\}$.

Démonstration. Soit $c \in \mathbf{R}_{>0}$ tel que $(\forall x \in \mathbf{R}_{>0})\ |A(x)| \leqslant cx^r$. On vérifie le critère de Cauchy. D'après la formule sommatoire d'Abel (*cf* lemme 5.4.1), on a
$$\left| \sum_{n=m}^{p} \frac{z_n}{n^s} \right| = \left| \frac{A(k)}{k^s} - \frac{A(m)}{m^s} + s \int_m^k \frac{A(t)}{t^{s+1}}\, \mathrm{d}t \right| \leqslant \frac{2c + c\,|s|\,/\delta}{m^\delta}$$

où $\delta = \Re(s) - r$. □

Proposition 5.5.9. Soit χ un caractère modulo m.
(1) Pour $\Re(s) > 1$, on a $L(s,\chi) = \prod_{p\in\mathscr{P}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$. En particulier, on a $L(s,\chi) \neq 0$ pour $\Re(s) > 1$.
(2) Si $\chi = \chi_0$, on a $L(s,\chi_0) = \zeta(s) \prod_{\substack{p\in\mathscr{P}\\ p|m}} \left(1 - \frac{1}{p^s}\right)$ pour $\Re(s) > 1$. Elle se prolonge en une fonction méromorphe sur $\mathbf{C}$, avec un unique pôle en $s = 1$, simple, de résidu $\frac{\varphi(m)}{m}$.
(3) Si $\chi \neq \chi_0$, la série définissant $L(s,\chi)$ converge uniformément sur les compacts de $\{s \in \mathbf{C}, \Re(s) > 0\}$: elle est donc holomorphe sur $\{s \in \mathbf{C}, \Re(s) > 0\}$.

Démonstration. Commençons par observer que $\sum_{1\leqslant n\leqslant x} \chi(n) = \begin{cases} \mathsf{O}(n) & \text{si } \chi = \chi_0 \\ \mathsf{O}(1) & \text{sinon} \end{cases}$, ce qui implique que la série de Dirichelet a une abscisse de convergence $\leqslant 1$ si $\chi = \chi_0$ et $\leqslant 0$ si $\chi \neq \chi_0$. Cela prouve (3).
(1) n'est autre que le produit eulérien de la série de Dirichelet (*cf* corollaire 5.1.15), car χ est totalement multiplicative.
(2) résulte de (1), car $\chi_0(p) = \begin{cases} 0 & \text{si } p \mid m \\ 1 & \text{sinon} \end{cases}$, et du fait que $\lim_{s\to 1}(s-1)\zeta(s) = 1$. □

Lemme 5.5.10. Si $a \in (\mathbf{Z}/m\,\mathbf{Z})^\times =: G$ est d'ordre d, on a

$$\prod_{\chi\in\widehat{G}} \big(1 - \chi(a)T\big) = (1 - T^d)^{\frac{\varphi(m)}{d}} \in \mathbf{C}[T]$$

Démonstration. Soit $a^* \in \widehat{\widehat{G}}$ le caractère défini par $a^*(\chi) = \chi(a)$ (*cf* proposition 5.5.3). Il est d'ordre d, ce qui implique que a^* est une surjection $\widehat{G} \to \mathbb{\mu}_d(\mathbf{C})$. On a donc

$$\prod_{\chi\in\widehat{G}} \big(1 - \chi(a)T\big) = \prod_{w\in\mathbb{\mu}_d(\mathbf{C})} \prod_{\substack{\chi\in\widehat{G}\\ a^*(\chi)=w}} (1 - wT) = \prod_{w\in\mathbb{\mu}_d(\mathbf{C})} (1 - wT)^{\frac{\varphi(m)}{d}}$$

On conclut en observant que $\prod_{w\in\mathbb{\mu}_d(\mathbf{C})} (1 - wT) = 1 - T^d$. □

Lemme 5.5.11. Soit $(a_n)_{n\in\mathbf{N}_{>0}}$ une suite de réels positifs ou nuls. On suppose que la série de Dirichelet $g(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ a une abscisse de convergence $\leqslant 1$, et se prolonge en une fonction holomorphe sur $\{s \in \mathbf{C}, \Re(s) > 0\}$ (encore notée $g(s)$). Alors $\sum_{n=1}^{\infty} \frac{a_n}{n^t} = g(t)$ pour tout $t \in]0,1]$.

Démonstration. Pour $k \in \mathbf{N}$, posons $b_k = (-1)^k \frac{g^{(k)}(2)}{k!}$. On a $g(s) = \sum_{k=1}^{\infty} b_k(2-s)^k$ dans un voisinage ouvert de 2. Mais comme g est holomorphe sur $\{s \in \mathbf{C}, \Re(s) > 0\}$, elle est développable en série entière sur $\mathrm{D}(2,2)$: l'égalité qui précède est valide pour tout $s \in \mathrm{D}(2,2)$. Si $t \in]0,2]$, on a donc

$$g(t) = \sum_{k=0}^{\infty} b_k(2-t)^k = \sum_{k=0}^{\infty} \left(\sum_{n=1}^{\infty} \frac{\ln^k(n)}{k!} \frac{a_n}{n^2} \right) (2-t)^k = \sum_{n=1}^{\infty} \left(\sum_{k=0}^{\infty} \frac{\ln^k(n)}{k!} (2-t)^k \right) \frac{a_n}{n^2} = \sum_{n=1}^{\infty} \frac{a_n}{n^t}$$

(l'intersection des signes somme étant licite parce qu'il s'agit d'une série à termes positifs sommable). □

Théorème 5.5.12. Si χ est un caractère modulo m, on a $L(1,\chi) \neq 0$.

Démonstration. Posons $\zeta_m(s) = \prod_{\chi} L(s,\chi)$ (le produit étant pris sur tous les caractères modulo m). C'est une fonction holomorphe sur $\{s \in \mathbf{C}, \Re(s) > 0\}\backslash\{1\}$. Comme $L(s,\chi_0)$ a un pôle simple en 1, il s'agit de voir que $\zeta_m(s)$ a un pôle en 1. Raisonnons par l'absurde : supposons $\zeta_m(s)$

holomorphe sur $\{s \in \mathbf{C},\ \Re(s) > 0\}$. Pour $p \in \mathscr{P}$ tel que $p \nmid m$, on note $d(m)$ l'ordre de p dans $(\mathbf{Z}/m\,\mathbf{Z})^\times$. Pour $\Re(s) > 1$, on a

$$\zeta_m(s) = \prod_{\chi} \prod_{p \nmid m} \Big(1 - \frac{\chi(p)}{p^s}\Big)^{-1} = \prod_{p \nmid m} \Big(1 - \frac{1}{p^{d(p)s}}\Big)^{-\frac{\varphi(m)}{d(p)}}$$

(*cf* lemme 5.5.10). C'est une série de Dirichelet de la forme $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ avec $a_n \in \mathbf{R}_{\geqslant 0}$. D'après le lemme 5.5.11, cette série converge sur $\mathbf{R}_{>0}$, et

$$\sum_{n=1}^{\infty} \frac{a_n}{n^t} = \prod_{p \nmid m} \Big(1 - \frac{1}{p^{d(p)t}}\Big)^{-\frac{\varphi(m)}{d(p)}}$$

Pour $t \in \big]\frac{1}{\varphi(m)}, 1\big]$, on a

$$\Big(1 - \frac{1}{p^{d(p)t}}\Big)^{-\frac{\varphi(m)}{d(p)}} = \Big(\sum_{k=0}^{\infty} \frac{1}{p^{d(p)k}}\Big)^{\frac{\varphi(m)}{d(p)}} \geqslant \sum_{k=0}^{\infty} \frac{1}{p^{\varphi(m)k}}$$

de sorte que

$$\zeta_m(t) \geqslant \sum_{\substack{n \in \mathbf{N}_{>0} \\ \mathsf{pgcd}(n,m)=1}} \frac{1}{n^{\varphi(m)t}} = L(\varphi(m)t, \chi_0)$$

Mais le membre de droite tend vers $+\infty$ quand $t \to \frac{1}{\varphi(m)}$: contradiction. □

5.5.13. *Le théorème de la progression arithmétique.*

Théorème 5.5.14. (de la progression arithmétique) Si $a, m \in \mathbf{N}_{>0}$ sont tels que $\mathsf{pgcd}(a, m) = 1$, l'ensemble des nombre premiers p tels que $p \equiv a \mod m\,\mathbf{Z}$ est infini.

Remarque 5.5.15. On peut montrer (Siegel-Walfisz) que les nombres premiers sont répartis de façon uniforme suivant les classes modulo m :

$$\lim_{x \to \infty} \frac{\#\{p \in \mathscr{P},\ p \equiv a \mod m\,\mathbf{Z},\ p \leqslant x\}}{\pi(x)} = \frac{1}{\varphi(m)}$$

Lemme 5.5.16. Soient χ un caractère modulo m et

$$f_\chi \colon \{s \in \mathbf{C},\ \Re(s) > 1\} \to \mathbf{C}$$
$$s \mapsto \sum_{p \in \mathscr{P}} \frac{\chi(p)}{p^s}$$

(1) On a $f_{\chi_0}(t) \sim -\ln(t-1)$ quand $t \to 1^+$.
(2) Si $\chi \neq \chi_0$, la fonction f_χ est bornée sur $]1, +\infty[$.

Démonstration. (1) On a $f_{\chi_0}(t) = \sum_{p \in \mathscr{P}} \frac{1}{p^t} - \sum_{\substack{p \in \mathscr{P} \\ p \mid m}} \frac{1}{p^t}$, l'équivalence résulte alors du corollaire 5.4.3.

(2) On applique la détermination principale du logarithme au produit eulérien de la fonction $L(s, \chi)$: on a

$$\ln(L(s,\chi)) = -\sum_{p \in \mathscr{P}} \ln\Big(1 - \frac{\chi(p)}{p^s}\Big) = \sum_{p \in \mathscr{P}} \sum_{k=1}^{\infty} \frac{\chi(p)^k}{k p^{ks}} = f_\chi(s) + F_\chi(s)$$

avec

$$|F_\chi(s)| = \Big|\sum_{p \in \mathscr{P}} \sum_{k=2}^{\infty} \frac{\chi(p)^k}{k p^{ks}}\Big| \leqslant \sum_{\substack{p \in \mathscr{P} \\ k \geqslant 2}} \frac{1}{p^{kt}} \leqslant 1$$

(*cf* corollaire 5.4.3), où $t = \Re(s)$. Comme $L(t, \chi)$ converge vers $L(1, \chi) \neq 0$ quand $t \to 1^+$ (*cf* théorème 5.5.12), on voit que f_χ reste bornée au voisinage de 1. □

Démonstration du théorème 5.5.14. Soient $A = \{p \in \mathscr{P},\ p \equiv a \mod m\,\mathbf{Z}\}$ et $g(s) = \sum_{p\in A} \frac{1}{p^s}$ (pour $\Re(s) > 1$). On a

$$\sum_\chi \chi(a)^{-1} f_\chi(s) = \sum_\chi \chi(a)^{-1} \sum_{p\in\mathscr{P}} \frac{\chi(p)}{p^s} = \sum_{p\in\mathscr{P}} \left(\sum_\chi \chi(a)^{-1}\chi(p)\right)\frac{1}{p^s}$$

Comme $\sum_\chi \chi(a)^{-1}\chi(p) = \begin{cases}\varphi(m) & \text{si } p \equiv a \mod m\,\mathbf{Z}\\ 0 & \text{sinon}\end{cases}$ (*cf* proposition 5.5.3), on a

$$\varphi(m) g(s) = \sum_\chi \chi(a)^{-1} f_\chi(s) = f_{\chi_0}(s) + \sum_{\chi\neq\chi_0} \chi(a)^{-1} f_\chi(s)$$

D'après le lemme 5.5.16, on a $\lim_{t\to 1^+} g(t) = +\infty$, ce qui implique que A est infini. □

5.5.17. *Prolongement analytique et équation fonctionnelle.* Soit χ un caractère de Dirichelet modulo m.

Définition 5.5.18. On dit que χ est **primitif** s'il ne peut se factoriser en $(\mathbf{Z}/m\,\mathbf{Z})^\times \to (\mathbf{Z}/d\,\mathbf{Z})^\times \to \mathbf{C}^\times$ avec d un diviseur *strict* de m. On dit alors que m est le **conducteur** de χ.

Remarque 5.5.19. Si χ est injectif, il est primitif, mais la réciproque est fausse : on a $(\mathbf{Z}/12\,\mathbf{Z})^\times = \{\pm 1, \pm 5\}$ et le caractère χ défini par $\chi(-1) = 1$ et $\chi(5) = -1$ n'est pas injectif, mais ne se factorise pas à travers $(\mathbf{Z}/12\,\mathbf{Z})^\times \to (\mathbf{Z}/d\,\mathbf{Z})^\times$ pour $d \in \{2, 3, 4, 6\}$ (car $(\mathbf{Z}/d\,\mathbf{Z})^\times = \{\pm 1\}$: cela forcerait χ à être trivial).

Définition 5.5.20. Supposons χ primitif modulo m. La **somme de Gauss** de χ est

$$\tau(\chi) = \sum_{k\in\mathbf{Z}/m\,\mathbf{Z}} \chi(k) e^{\frac{2ik\pi}{m}} \in \mathbf{C}$$

Proposition 5.5.21. On a $|\tau(\chi)| = \sqrt{m}$.

Démonstration. Si $n \in \mathbf{Z}$ est tel que $\mathsf{pgcd}(m, n) = 1$, on a

$$\sum_{k\in\mathbf{Z}/m\,\mathbf{Z}} \chi(k) e^{\frac{2ikn\pi}{m}} = \chi(n)^{-1} \sum_{k\in\mathbf{Z}/m\,\mathbf{Z}} \chi(kn) e^{\frac{2ikn\pi}{m}} = \overline{\chi}(n)\tau(\chi)$$

Si $\mathsf{pgcd}(m, n) = d > 1$, écrivons $n = dn'$ et $m = dm'$. Supposons $(\forall c \in (\mathbf{Z}/m\,\mathbf{Z})^\times)\ c \equiv 1 \mod m'\,\mathbf{Z} \Rightarrow \chi(c) = 1$. Pour tout $k_1, k_2 \in (\mathbf{Z}/m\,\mathbf{Z})^\times$, on a $k_1 \equiv k_2 \mod m'\,\mathbf{Z} \Rightarrow \chi(k_1) = \chi(k_2)$, de sorte que χ se factorise à travers $(\mathbf{Z}/m\,\mathbf{Z})^\times \to (\mathbf{Z}/m'\,\mathbf{Z})^\times$, ce qui contredit le fait que χ est primitif. Il existe donc $c \in (\mathbf{Z}/m\,\mathbf{Z})^\times$ tel que $c \equiv 1 \mod m'\,\mathbf{Z}$ et $\chi(c) \neq 1$. On a

$$\sum_{k\in\mathbf{Z}/m\,\mathbf{Z}} \chi(k) e^{\frac{2ikn\pi}{m}} = \sum_{k\in\mathbf{Z}/m\,\mathbf{Z}} \chi(k) e^{\frac{2ikn'\pi}{m'}} = \sum_{r\in\mathbf{Z}/m'\,\mathbf{Z}} \left(\sum_{\substack{k\in\mathbf{Z}/m\,\mathbf{Z}\\ k\equiv r \mod m'}} \chi(k)\right) e^{\frac{2irn'\pi}{m'}}$$

La multiplication par c permute $\{k \in \mathbf{Z}/m\,\mathbf{Z},\ k \equiv r \mod m'\}$, ce qui implique que

$$\sum_{\substack{k\in\mathbf{Z}/m\,\mathbf{Z}\\ k\equiv r \mod m'}} \chi(k) = \chi(c) \sum_{\substack{k\in\mathbf{Z}/m\,\mathbf{Z}\\ k\equiv r \mod m'}} \chi(k)$$

et donc $\sum_{\substack{k\in\mathbf{Z}/m\,\mathbf{Z}\\ k\equiv r \bmod m'}} \chi(k) = 0$, d'où $\sum_{k\in\mathbf{Z}/m\,\mathbf{Z}} \chi(k) e^{\frac{2ikn\pi}{m}} = 0 = \underbrace{\overline{\chi}(m)}_{=0}\tau(\chi)$. Ainsi

$$\sum_{k_1,k_2\in(\mathbf{Z}/m\,\mathbf{Z})^\times} \chi(k_1)\overline{\chi(k_2)} e^{\frac{2i(k_1-k_2)n\pi}{m}} = \left|\sum_{k\in\mathbf{Z}/m\,\mathbf{Z}} \chi(k) e^{\frac{2ikn\pi}{m}}\right|^2 = \begin{cases}|\tau(\chi)|^2 & \text{si } \mathsf{pgcd}(m, n) = 1\\ 0 & \text{sinon}\end{cases}$$

en sommant pour $n \in \mathbf{Z}/m\,\mathbf{Z}$, on a donc

$$\varphi(m)\,|\tau(\chi)|^2 = \sum_{n\in\mathbf{Z}/m\,\mathbf{Z}} \sum_{k_1,k_2\in(\mathbf{Z}/m\,\mathbf{Z})^\times} \chi(k_1)\overline{\chi(k_2)} e^{\frac{2i(k_1-k_2)n\pi}{m}}$$

Comme $\sum_{n\in\mathbf{Z}/m\,\mathbf{Z}} e^{\frac{2ikn\pi}{m}} = \begin{cases} m & \text{si } m \mid k \\ 0 & \text{sinon} \end{cases}$, on a

$$\varphi(m)\,|\tau(\chi)|^2 = \sum_{k\in(\mathbf{Z}/m\,\mathbf{Z})^\times} |\chi(k)|^2\, m = \varphi(m)m$$

ce qui permet de conclure. □

On a $\chi(-1)^2 = \chi(1) = 1$: il existe $\varepsilon \in \{0,1\}$ tel que $\chi(-1) = (-1)^\varepsilon$. On pose alors

$$\Lambda(s,\chi) = \frac{\Gamma\left(\frac{s+\varepsilon}{2}\right)L(s,\chi)}{\pi^{\frac{s+\varepsilon}{2}}}$$

(c'est la généralisation de la fonction I du théorème 5.4.4).

Théorème 5.5.22. Supposons χ primitif modulo m.
(1) La fonction $\Lambda(s,\chi)$ admet un prolongement méromorphe au plan complexe. Si $\chi \neq \chi_0$, le prolongement est holomorphe sur $\mathbf{C}$, si $\chi = \chi_0$, le prolongement admet des pôles simples en $s = 0$ et $s = 1$.
(2) On a l'équation fonctionnelle

$$\Lambda(1-s,\overline{\chi}) = \frac{i^\varepsilon m^s}{\tau(\chi)}\Lambda(s,\chi)$$

Démonstration. Voir [2, Theorem 1.1.1]. □

Remarque 5.5.23. Hypothèse de Riemann généralisée : les zéros de $L(s,\chi)$ tels que $0 \leqslant \Re(s) \leqslant 1$ vérifient $\Re(s) = \frac{1}{2}$.

5.6. **Fonction zêta de Dedekind, énoncé de la formule analytique du nombre de classes.** Soit K un corps de nombres.

Définition 5.6.1. La **fonction zêta de Dedekind** est la fonction de la variable complexe :

$$\zeta_K(s) = \sum_{I\subset\mathcal{O}_K} \frac{1}{\mathsf{N}(I)^s}$$

la somme étant étendue à tous les idéaux de $\mathcal{O}_K$ (rappelons que $\mathsf{N}(I) = \#(\mathcal{O}_K/I)$).

Remarque 5.6.2. (1) Pour $K = \mathbf{Q}$, on retrouve la fonction zêta de Riemann.
(2) Pour $n \in \mathbf{N}_{>0}$, posons $a_K(n) = \#\{I \subset \mathcal{O}_K,\ I \text{ idéal},\ \mathsf{N}(I) = n\}$. On a alors

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_K(n)}{n^s}$$

de sorte que $\zeta_K(s)$ est une série de Dirichelet.

Proposition 5.6.3. (1) La série définissant $\zeta_K(s)$ converge uniformément sur tout compact de $\{s \in \mathbf{C},\ \Re(s) > 1\}$, et définit donc une fonction holomorphe sur $\{s \in \mathbf{C},\ \Re(s) > 1\}$.
(2) Pour $\Re(s) > 1$, on a le produit eulérien $\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathsf{N}(\mathfrak{p})^s}\right)^{-1}$, où $\mathfrak{p}$ parcourt les idéaux maximaux de $\mathcal{O}_K$. En particulier $\zeta_K(s) \neq 0$.

Démonstration. (1) Si $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_K$ et $\mathfrak{p}\cap\mathbf{Z} = p\,\mathbf{Z}$, on a $\mathsf{N}(\mathfrak{p}) = p^{f_\mathfrak{p}}$. Si $t \in]1,+\infty[$, on a

$$\prod_{\mathsf{N}(\mathfrak{p})\leqslant N} \left(1 - \tfrac{1}{\mathsf{N}(\mathfrak{p})^t}\right)^{-1} \leqslant \prod_{\substack{p\in\mathscr{P}\\ p\leqslant N}} \prod_{\mathfrak{p}\mid p} \left(1 - \tfrac{1}{p^{tf_\mathfrak{p}}}\right)^{-1} \leqslant \prod_{\substack{p\in\mathscr{P}\\ p\leqslant N}} \prod_{\mathfrak{p}\mid p} \left(1 - \tfrac{1}{p^t}\right)^{-1}$$

Comme il existe au plus $d = [K : \mathbf{Q}]$ idéaux premiers au-dessus de $p\,\mathbf{Z}$, le terme de droite est majoré par

$$\prod_{\substack{p\in\mathscr{P}\\ p\leqslant N}} \left(1 - \tfrac{1}{p^t}\right)^{-d} \leqslant \zeta(t)^d$$

Cela implique que le produit infini $\prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathsf{N}(\mathfrak{p})^t}\right)^{-1}$ converge.

Un idéal $I \subset \mathcal{O}_K$ se décompose de façon unique $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$ avec $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ des idéaux maximaux et $\alpha_1, \ldots, \alpha_r \in \mathbf{N}$. Si $t \in]1, +\infty[$, on a donc

$$\sum_{\substack{I \subset \mathcal{O}_K \\ \mathsf{N}(I) \leqslant N}} \frac{1}{\mathsf{N}(I)^t} \leqslant \prod_{\mathsf{N}(\mathfrak{p}) \leqslant N} \left(\sum_{n=0}^{\infty} \frac{1}{\mathsf{N}(\mathfrak{p})^{nt}} \right) = \prod_{\mathsf{N}(\mathfrak{p}) \leqslant N} \left(1 - \frac{1}{\mathsf{N}(\mathfrak{p})^t}\right)^{-1} \leqslant \zeta(t)^d$$

d'après ce qui précède. La série à termes positifs $\sum_{I \subset \mathcal{O}_K} \frac{1}{\mathsf{N}(I)^t}$ converge donc. Si $\Re(s) \geqslant 1 + \delta$ avec $\delta \in \mathbf{R}_{>0}$, on a donc

$$\sum_{\substack{I \subset \mathcal{O}_K \\ \mathsf{N}(I) > N}} \left| \frac{1}{\mathsf{N}(I)^s} \right| \leqslant \sum_{\substack{I \subset \mathcal{O}_K \\ \mathsf{N}(I) > N}} \frac{1}{\mathsf{N}(I)^t}$$

ce qui implique la convergence uniforme sur $\{s \in \mathbf{C},\ \Re(s) \geqslant 1 + \delta\}$, et donc (1).
La preuve de (2) est identique à celle de la proposition 5.1.14. □

Théorème 5.6.4. (1) La fonction $\zeta_K(s)$ admet un prolongement méromorphe à $\mathbf{C}$, avec un unique pôle simple en $s = 1$.
(2) On a $\operatorname{Res}_1 \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}}{\#\mathbb{\mu}(K)\sqrt{|d_K|}} h_K R_K$ (où h_K est le nombre de classes et R_K le régulateur).
(3) On a $\lim_{s \to 0} \frac{\zeta_K(s)}{s^{r_1 - r_2 - 1}} = -\frac{h_K R_K}{\#\mathbb{\mu}(K)}$.

Démonstration. Voir [5, Corollary VII.5.12]. Observons tout de même que pour $\Re(s) > 1$, on a $\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_K(n)}{n^s}$. Comme $\sum_{i=0}^{n} a_K(i) = N_K(n) = \frac{2^{r_1}(2\pi)^{r_2}}{\#\mathbb{\mu}(K)\sqrt{|d_K|}} h_K R_K n + \mathsf{O}\left(n^{1 - \frac{1}{[K:\mathbf{Q}]}}\right)$ (*cf* théorème 4.4.5), on a $\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}}{\#\mathbb{\mu}(K)\sqrt{|d_K|}} h_K R_K \zeta(s) + f(s)$ avec $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, où $\sum_{i=1}^{n} a_i = \mathsf{O}\left(n^{1 - \frac{1}{[K:\mathbf{Q}]}}\right)$. D'après le lemme 5.5.8 (2), la fonction f est holomorphe sur $\left\{s \in \mathbf{C},\ \Re(s) > 1 - \frac{1}{[K:\mathbf{Q}]}\right\}$. La fonction $\zeta_K(s)$ se prolonge donc en une fonction méromorphe sur ce domaine, avec un seul pôle en $s = 1$, simple, de résidu égal à $\frac{2^{r_1}(2\pi)^{r_2}}{\#\mathbb{\mu}(K)\sqrt{|d_K|}} h_K R_K$. □

Références

[1] L. Ahlfors – *Complex analysis. An introduction to the theory of analytic functions of one complex variable*, McGraw-Hill Book Company, 1953.

[2] D. Bump – *Automorphic forms and representations*, Cambridge studies in advanced mathematics, vol. 55, Cambridge University Press, 1998.

[3] K. Kato, N. Kurokawa & T. Saito – *Number theory 2*, Translations of Mathematical Monographs, vol. 240, American Mathematical Society, 2011.

[4] H. Matsumura – *Commutative ring theory*, second éd., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, 1989.

[5] J. Neukirch – *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999.

[6] W. Rudin – *Analyse réelle et complexe*, Dunod, 1998.

[7] G. Tenenbaum – *Introduction to analytic ans probabilistic number theory*, Cambridge studies in advanced mathematics, vol. 46, Cambridge University Press, 1995.

Institut de Mathématiques de Bordeaux, Université Bordeaux 1, 351, cours de la Libération, 33405 Talence, France

E-mail address: olivier.brinon@math.u-bordeaux1.fr