université de BORDEAUX	**ANNÉE UNIVERSITAIRE 2018 / 2019** SESSION 1 D'AUTOMNE **PARCOURS / ÉTAPE : 4TMA903U** **Code UE : 4TTN901S, 4TTN901S** **Épreuve :** Algebraic number theory **Date :** 7/01/2019 **Heure :** 9h30 **Durée :** 3h Documents : non autorisés Épreuve de Mr Brinon	**Collège Sciences et technologies**

Documents are not allowed.
The quality of writing will be an important assessment factor.

Exercise 1

Let p be a prime number.
(1) Show that $\mathbf{Z}_{\geqslant 0}$ is dense in $\mathbf{Z}_p$.
(2) Is it true that $\mathbf{Z}_p \cap \mathbf{Q} = \mathbf{Z}$?
(3) Show that $\mathbf{Q}_p^{\times 2} = \{x^2\}_{x\in\mathbf{Q}_p^\times}$ is open in $\mathbf{Q}_p^\times$.
(4) Let $a \in \mathbf{Z}$. Show that the polynomial $X^2 + X + a$ has a root in $\mathbf{Q}_2$ if and only if a is even.
(5) Assume that p is odd. Show that $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times p} \simeq (\mathbf{Z}/p\mathbf{Z})^2$.

Exercise 2

Let $P(X) = X^3 - 17$ and $j \in \overline{\mathbf{Q}}_3$ a primitive cubic root of unity.
(1) Show that $j \notin \mathbf{Q}_3$ [hint: compute $(j-1)^2$].
(2) What are the degrees of the irreducible factors of P in $\mathbf{Q}_3[X]$ [hint: compute $P(5)$]?
(3) How many extensions to $\mathbf{Q}(\sqrt[3]{17})$ does the 3-adic absolute value have?

Exercise 3

Let A be a Dedekind ring, $K = \mathsf{Frac}(A)$ and L/K a finite and separable field extension. Denote by B the integral closure of A in L, and $\mathscr{P}_A$ the set of nonzero prime ideals of A. An A-*order* of L is a subring R of L such that $A \subset R$ and R is an A-module of finite type.
(1) Let R be a subring of L such that $A \subset R$. Show that R is an A-order of L if and only if $R \subset B$.
(2) Assume that R is an A-order of L.
 (i) Show that for all $\mathfrak{p} \in \mathscr{P}_A$, the localization $R_\mathfrak{p}$ is an $A_\mathfrak{p}$-order of L.
 (ii) Show that $R = B$ if and only if $R_\mathfrak{p} = B_\mathfrak{p}$ for all $\mathfrak{p} \in \mathscr{P}_A$.
 (iii) Show that nonzero prime ideals of R are maximal.
(3) Let R be an A-order of L and $\theta \in R$ such that $L = K(\theta)$. Denote by $P(X)$ the minimal polynomial of θ over K. Let $\mathfrak{p} \in \mathscr{P}_A$ and $\overline{P}$ the image of P in $\kappa(\mathfrak{p})[X]$, where $\kappa(\mathfrak{p}) = A/\mathfrak{p}$. Show that if $\overline{P}$ is separable, then $R_\mathfrak{p} = B_\mathfrak{p}$ and the prime ideals of B above $\mathfrak{p}$ are unramified [hint: recall that $A[\theta]^* = \frac{1}{P'(\theta)}A[\theta]$].
(4) Let $R \subset R'$ be an extension of rings, the *conductor* of R'/R is $\mathfrak{c}_{R'/R} = \{r \in R\,;\, rR' \subset R\}$.
 (i) Show that $\mathfrak{c}_{R'/R}$ is the largest ideal of R' that is contained in R.
 (ii) Let R be an A-order of L and $S \subset R$ a multiplicative part. Show that $\mathfrak{c}_{S^{-1}B/S^{-1}R} = S^{-1}\mathfrak{c}_{B/R}$ [hint: use the fact that B is finite over R].
 (iii) Let R be an A-order of L. Show that $\mathfrak{c} := \mathfrak{c}_{B/R} \neq \{0\}$ if and only if $\mathsf{Frac}(R) = L$.
Assume henceforth that $\mathsf{Frac}(R) = L$.
(5) Show that $\mathfrak{c}R^* \subset \mathfrak{D}_{B/A}^{-1}$ (where $R^* = \{y \in L\,;\, (\forall x \in R)\ \mathsf{Tr}_{L/K}(xy) \in A\}$), and that this inclusion is an equality when $R = A[\theta]$ for some $\theta \in L$ such that $L = K(\theta)$.
(6) In this question we assume that $A = \mathbf{Z}$.
 (i) Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_L$ and put $R = \mathbf{Z} + \mathfrak{a}$. Show that R is a $\mathbf{Z}$-order of L, with conductor $d\,\mathbf{Z} + \mathfrak{a}$, where $d \in \mathbf{Z}_{>0}$ is such that $\mathbf{Z} \cap \mathfrak{a} \subset d\,\mathbf{Z}$.
 (ii) Assume that $L = \mathbf{Q}(\sqrt{5})$. Show that $R = \mathbf{Z}[\sqrt{5}]$ is a $\mathbf{Z}$-order of L. What is its conductor?
(7) Let $\mathfrak{q} \in \mathscr{P}_B$. Show that $\mathfrak{c} \subset \mathfrak{q}$ if and only if $\mathfrak{c} \subset \mathfrak{q} \cap R$. Deduce that if $\mathsf{Frac}(R) = L$, there are only finitely many prime ideals of R that contain $\mathfrak{c}$.

(8) (hard) Let $\mathfrak{p}$ be a nonzero prime ideal of R. Show that the following are equivalent:

(a) $\mathfrak{p}$ does not contain $\mathfrak{c}$;

(b) $R = \{x \in L\,;\, x\mathfrak{p} \subset \mathfrak{p}\}$;

(c) $\mathfrak{p}$ is invertible;

(d) $R_{\mathfrak{p}}$ is a DVR.

[hint: to show (a)⇒(b), use the fact that $\mathfrak{p} + \mathfrak{c} = R$; to show (b)⇒(c), use the fact that if $\alpha \in \mathfrak{p}\backslash\{0\}$, there exists $r \in \mathbf{Z}_{>0}$ such that $\mathfrak{p}^r R_{\mathfrak{p}} \subset \alpha R_{\mathfrak{p}}$; to show (c)⇒(d), show that nonzero ideals of $R_{\mathfrak{p}}$ are powers of $\mathfrak{p}R_{\mathfrak{p}}$, then that $R_{\mathfrak{p}}$ is integrally closed.]

(9) (hard) Show that under the equivalent conditions of question (8), $\mathfrak{p}B$ is the only maximal ideal of B that contains $\mathfrak{p}$ [hint: take $\mathfrak{q} \in \mathscr{P}_B$ such that $\mathfrak{p} \subset \mathfrak{q}$, and show that $R_{\mathfrak{p}} = B_{\mathfrak{q}}$.]

Exercise 4

Unless otherwise stated, ramification subgroups of a finite Galois extension L/K will be considered with the lower numbering. A *jump* of the extension L/K is an integer i such that $\mathsf{Gal}(L/K)_i \neq \mathsf{Gal}(L/K)_{i+1}$.

Let L/K and K/F be nontrivial finite extensions of local fields.

(1) Assume that L/F and K/F are Galois. Let $i_1 < \cdots < i_n$ be the jumps of the ramification filtration of L/K. Assume that the ramification filtration of K/F has a unique jump i_0, and that $i_0 < i_1$. Show that

$$\mathsf{Gal}(L/F)_i = \begin{cases} \mathsf{Gal}(L/F) & \text{if } i \leqslant i_0 \\ \mathsf{Gal}(L/K)_i & \text{if } i > i_0 \end{cases}$$

and deduce that the jumps of the ramification filtration of L/F are $i_0, i_1, \ldots, i_n$ [hint: Herbrand's theorem].

Assume from now on that F has mixed characteristics $(0,p)$, that $K = F(\zeta)$ where ζ is a primitive p-th root of unity, and that $L = K(\alpha)$, where $a := \alpha^p \in K$ and $\alpha \notin K$.

(2) Show that the extension K/F is cyclic of degree dividing $p-1$, and that $v_K(\zeta - 1) = \frac{e_K}{p-1} \in \mathbf{Z}_{>0}$ (where e_K is the absolute ramification index of K).

(3) Explain why K/F has at most two jumps, and exactly one when it is totally ramified.

We henceforth assume that K/F is totally ramified. Denote by v_K (resp. v_L) the normalized valuation on K (resp. on L).

(4) Show that L/K is a cyclic extension of degree p. When $a \in F$, show that L/F is Galois and describe the structure of $\mathsf{Gal}(L/F)$.

(5) Assume that $p \nmid v_K(a)$. Show that L/K is totally ramified, and that $v_L(\mathfrak{D}_{L/K}) = pe_K + p - 1$ [hint: first reduce to the case where $v_K(a) = 1$]. Deduce the jumps of L/K. If $a \in F$, what are the jumps of L/F? Under which condition on e_F are the jumps in the upper numbering integers?

Assume from now on that $p \mid v_K(a)$ and put $E = \big\{i \in \mathbf{Z}_{>0}\,;\, (\exists x \in K^\times)\, ax^{-p} \in U_K^{(i)}\big\}$.

(6) (i) Show that $1 \in E$.

(ii) Assume that $a \in U_K^{(i)}$ with $i > \frac{pe_K}{p-1}$. Show that the polynomial $Q(X) = \frac{(1+(\zeta-1)X)^p - a}{(\zeta-1)^p}$ belongs to $\mathcal{O}_K[X]$, and use Newton's lemma to show that it has a root in $\mathcal{O}_K$, contradicting the hypothesis.

The set E is thus non empty, and included in $\big\{1, \ldots, \frac{pe_K}{p-1}\big\}$. Put $c = \max E$: replacing a by ax^{-p} for some appropriate $x \in K^\times$, we may assume that $a \in U_K^{(c)}$.

(7) Show that there exists $A(X) \in \mathbf{Z}[X]$ such that $(X-1)^p = X^p - 1 + p(X-1)A(X)$ and $A(1) = -1$.

(8) Assume that $c = \frac{pe_K}{p-1}$ and put $z = \frac{\alpha - 1}{\zeta - 1} \in L$.

(i) Show that $v_L(z) = 0$ [hint: use question (7)].

(ii) Compute the minimal polynomial P of z over K, and show that its image $\overline{P}$ in $\kappa_K[X]$ is of the form $\overline{P}(X) = X^p - X - \lambda$. Explain why $\overline{P}$ is irreducible, and deduce that K/F is unramified.

(iii) If $a \in F$, what are the jumps of L/F in that case?

(9) Assume that $c \leqslant \frac{pe_K}{p-1} - 1$.

(i) Show that $p \nmid c$ [hint: assume the contrary and deduce a contradiction with the definition of c.]

(ii) Compute $v_L(\alpha - 1)$ [hint: use question (7)], and deduce that L/K is totally ramified.

(iii) Constuct a uniformizer π_L of L, and determine the jump of L/K [hint: consider the action of a generator of $\mathsf{Gal}(L/K)$ on π_L.]

(iv) Deduce that $v_L(\mathfrak{D}_{L/K}) = (p-1)\big(\frac{pe_K}{p-1} - c + 1\big)$. When $a \in F$, what are the jumps of L/F in this case?