UPS – Centre d'Orsay
Mathématiques

Arithmétique – Maîtrise
Année 2003–2004

FEUILLE D'EXERCICES n° 4

Soit $K/\mathbb{Q}$ un corps de nombres de degré n, d'anneau d'entiers $\mathcal{O}_K$ et $M \subset \mathcal{O}_K$ un sous-$\mathbb{Z}$-module de base $(f_i)_{1\leqslant i\leqslant n}$. On définit $\operatorname{disc}_{K/\mathbb{Q}} M := \operatorname{disc}_{K/\mathbb{Q}}(f_1,\ldots,f_n)$, qui ne dépend pas de la $\mathbb{Z}$-base choisie. On note $\delta_K := \operatorname{disc}_{K/\mathbb{Q}} \mathcal{O}_K$. On dira que M est p-maximal si $p \nmid [\mathcal{O}_K : M]$.

Exercice 1 – Soit $K = \mathbb{Q}(\sqrt{-13})$. Décomposer l'idéal (10) en produit d'idéaux premiers dans $\mathcal{O}_K$. Vérifier le résultat en effectuant le produit des idéaux premiers obtenus.

Exercice 2 – Soit $K = \mathbb{Q}(\sqrt{51})$. On note $A = (2, 1+\sqrt{51}) := 2\mathcal{O}_K + (1+\sqrt{51})\mathcal{O}_K$.

a) Montrer que $A = 2\mathbb{Z} + (1+\sqrt{51})\mathbb{Z}$

b) Déterminer l'idéal fractionnaire A^{-1}.

c) Démontrer que A est premier dans $\mathcal{O}_K$.

d) Calculer $\mathrm{N}_{K/\mathbb{Q}}(A)$.

Exercice 3 –

a) Soit α un nombre algébrique, $P(X)$ son polynôme minimal, $\alpha_1 = \alpha, \ldots, \alpha_n$ les racines de ce dernier, et $K = \mathbb{Q}(\alpha)$. Montrer que

$$\operatorname{disc}_{K/\mathbb{Q}} \mathbb{Z}[\alpha] = \prod_{i<j} (\alpha_j - \alpha_i)^2 = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(P'(\alpha)).$$

b) On suppose $P(X) = X^n + aX + b$ irréductible et $n \geqslant 2$. Calculer $\operatorname{disc}_{K/\mathbb{Q}} \mathbb{Z}[\alpha]$. Expliciter la formule quand $n = 2$ ou 3.

Exercice 4 –

a) Soient $f_1, \ldots, f_n \in \mathcal{O}_K$ linéairement indépendants sur $\mathbb{Q}$ et M le $\mathbb{Z}$-module qu'ils engendrent. Montrer que $\delta_K[\mathcal{O}_K : M]^2 = \operatorname{disc}_{K/\mathbb{Q}} M$. En déduire que si $\operatorname{disc}_{K/\mathbb{Q}} M$ est sans facteur carré, alors $f_1, \ldots, f_n$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$.

b) Soit p un nombre premier. Montrer que p divise $(\operatorname{disc}_{K/\mathbb{Q}} M)/\delta_K$, si et seulement si il existe des entiers $a_1, \ldots, a_n$ tels que $(a_1, \ldots, a_n, p) = 1$ et $(a_1 f_1 + \cdots + a_n f_n)/p \in \mathcal{O}_K$ [*traduire en termes d'éléments d'ordre p dans $\mathcal{O}_K/M$*].

★ **Exercice 5** – On suppose $K = \mathbb{Q}(\alpha)$ où le polynôme minimal P_α de α est d'Eisenstein en p. C'est-à-dire que P_α est unitaire, congru à X^n modulo p, et de coefficient constant non nul modulo p^2. Montrer que $\mathbb{Z}[\alpha]$ est p-maximal. [*En supposant que le Théorème 1 s'applique, on aurait $p = (p,\alpha)^{\dim_{\mathbb{Q}} K}$. Montrer cette identité directement.*]

Exercice 6 –

a) Déterminer $\mathcal{O}_K$ lorsque $K = \mathbb{Q}(\alpha)$, avec $\alpha^3 = 2$ [*appliquer les trois exercices précédents : montrer en particulier que* $\mathbb{Z}[\alpha]$ *est* 2 *et* 3*-maximal.*].

b) Même question avec $\alpha^3 - \alpha - 1 = 0$.

Exercice 7 – Soit p un nombre premier.

a) Montrer que le polynôme cyclotomique $\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1$ est irréductible dans $\mathbb{Q}[X]$ [*considérer* $\Phi_p(Y+1)$].

b) Soit ζ une racine p-ième de l'unité et $K = \mathbb{Q}(\zeta)$. Montrer les formules

$$\mathrm{Tr}_{K/\mathbb{Q}}(1-\zeta^j) = p, \qquad \mathrm{N}_{K/\mathbb{Q}}(1-\zeta^j) = p \qquad (1 \leqslant j \leqslant p-1).$$

c) Montrer la relation $(1-\zeta)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$.

d) En déduire que $\mathcal{O}_K = \mathbb{Z}[\zeta]$ et calculer le discriminant d'une base de $\mathcal{O}_K$.

Exercice 8 – $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$. On veut montrer que, pour tout $\alpha \in \mathcal{O}_K$, on a $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$. Supposons qu'il existe α tel que $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

a) Calculer $[K : \mathbb{Q}]$ et donner les plongement complexes de K.

b) Montrer que 3 est non-ramifié dans $K/\mathbb{Q}$.

c) Soit $\alpha_1 = (1+\sqrt{7})(1+\sqrt{10})$, $\alpha_2 = (1+\sqrt{7})(1-\sqrt{10})$, $\alpha_3 = (1-\sqrt{7})(1+\sqrt{10})$, $\alpha_4 = (1-\sqrt{7})(1-\sqrt{10})$. Montrer que les produits $\alpha_i\alpha_j$ où $i \neq j$ sont divisibles par 3 dans $\mathcal{O}_K$ mais que 3 ne divise aucune puissance des α_i. [*Il suffit de démontrer qu'il ne divise aucun* α_i *; utiliser la norme.*]

d) Soit f le polynôme minimal de α. On pose $\alpha_i = f_i(\alpha)$ avec $f_i \in \mathbb{Z}[X]$. Montrer que $\overline{f}$ divise $\overline{f_i f_j}$ dans $\mathbb{F}_3[X]$ lorsque $i \neq j$ mais que $\overline{f}$ ne divise pas $\overline{f_i}^k$. Conclure.

e) [*Autre démonstration*] Montrer que $(3, 1 \pm \sqrt{7} \pm \sqrt{10})$ sont 4 idéaux maximaux distincts divisant 3. En utilisant le Théorème 1, montrer que $3 \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, pour tout $\alpha \in \mathcal{O}_K$ tel que $K = \mathbb{Q}(\alpha)$.

Problème I (Critère de Kummer)

Soit K une extension finie de $\mathbb{Q}$. On rappelle que tout idéal $I \neq (0)$ de $\mathcal{O}_K$ s'écrit de façon unique $I = \prod \mathfrak{p}_i^{e_i}$, où les $\mathfrak{p}_i$ sont exactement les idéaux maximaux contenant I.

Question préliminaire : Soit p un premier rationnel, on écrit $p\mathcal{O}_K = \prod \mathfrak{p}_i^{e_i}$.

a) montrer que $\mathcal{O}_K/\mathfrak{p}_i$ est un corps fini de corps premier $\mathbb{F}_p$. On définit f_i par $\mathcal{O}_K/\mathfrak{p}_i \simeq \mathbb{F}_{p^{f_i}}$.

b) Montrer que $[K : \mathbb{Q}] = \sum_i e_i f_i$.

On veut montrer le théorème suivant :

Théorème 1 (Kummer). *Soit $K = \mathbb{Q}(\alpha)$ où $\alpha \in \mathcal{O}_K$ tel que $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ et soit f le polynôme minimal de α. On suppose que*

$$f \equiv \prod_{i=1}^{g} \overline{P_i}^{e_i} \pmod{p}$$

(décomposition en produit d'irréductibles dans $\mathbb{F}_p[X]$) et on note P_i un relèvement arbitraire de $\overline{P_i}$ dans $\mathbb{Z}[X]$. Alors

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

où les $\mathfrak{p}_i := (p, P_i(\alpha))$ sont des idéaux premiers distincts et $N\mathfrak{p}_i = p^{\deg(P_i)}$.

1) Soit $\mathfrak{p}_i := (p, P_i(\alpha))$, $f_i := \deg P_i$. On veut d'abord montrer que, soit $\mathfrak{p}_i = \mathcal{O}_K$, soit $\mathcal{O}_K/\mathfrak{p}_i$ est un corps de cardinal p^{f_i}. Pour deux $\mathbb{Z}$-modules A et B, on note $A + B$ le $\mathbb{Z}$-module qu'ils engendrent.

a) On pose $K_i := \mathbb{F}_p[X]/(P_i)$. Montrer que $K_i \simeq \mathbb{F}_{p^{f_i}}$ et que $(p, P_i(X))$ est un idéal maximal de $\mathbb{Z}[X]$.

b) Montrer que $[\mathcal{O}_K : \mathbb{Z}[\alpha] + \mathfrak{p}_i]$ divise $\mathrm{pgcd}([\mathcal{O}_K : \mathbb{Z}[\alpha]], [\mathcal{O}_K, p\mathcal{O}_K]) = 1$.

c) On considère l'homomorphisme $\varphi : \mathbb{Z}[X] \to \mathcal{O}_K/\mathfrak{p}_i$ donné par $\varphi(X) = \alpha + \mathfrak{p}_i$. Montrer que φ est surjective. Conclure.

2) Montrer que $\mathfrak{p}_i + \mathfrak{p}_j = 1$ si $i \neq j$ [*utiliser Bezout*]

3) Montrer que $\prod \mathfrak{p}_i^{e_i} \subset (p, \prod P_i(\alpha)^{e_i}) \subset p\mathcal{O}_K$. Donc $p\mathcal{O}_K | \prod \mathfrak{p}_i^{e_i}$.

4) Montrer le théorème de Kummer [*on supposera que $\mathfrak{p}_i \neq \mathcal{O}_K$ pour $i \leqslant s$, soit $p\mathcal{O}_K = \prod_{i \leqslant s} \mathfrak{p}_i^{d_i}$, où $d_i \leqslant e_i$ pour tout $i \leqslant s$ et on utilisera la question préliminaire*]

Remarque : si $\mathbb{Z}[\alpha] = \mathcal{O}_K$, on peut aussi montrer ce théorème en prouvant que les idéaux de $\mathbb{Z}[\alpha]$ contenant p sont en bijection avec les idéaux de $\mathbb{Z}[\alpha]/(p) \simeq \mathbb{F}_p[X]/(f)$, idem pour les idéaux maximaux, puis que ces derniers dans $\mathbb{F}_p[X]/(f)$ sont les $(\overline{P_i})$. On en déduit que $(p, P_i(\alpha))$ est maximal dans $\mathcal{O}_K$ et la fin est facile. Pour se ramener du cas p-maximal au cas $\mathbb{Z}[\alpha] = \mathcal{O}_K$, il faut connaître la notion de localisation : si A est un anneau intègre, on note

$$A_p = \left\{ \frac{x}{y} \in \mathrm{Frac}(A), x, y \in A, (y, p) = 1 \right\}.$$

On vérifie que $\mathcal{O}_{K,p} = \mathbb{Z}[\alpha]_p$, puis que tout marche comme précédemment dans $\mathcal{O}_{K,p}$ (il y a des détails non triviaux).

Remarque 2 : il existe des corps de nombres K où l'hypothèse de p-maximalité de $\mathbb{Z}[\alpha]$ n'est jamais vérifiée, quel que soit $\alpha \in \mathcal{O}_K$. On montre quand même qu'alors $p < [K : \mathbb{Q}]$, donc très peu de premiers sont concernés (Hensel). Dans ce cas, il faut factoriser f modulo p^n pour n assez grand, en fait dans $\mathbb{Q}_p$, mais on est dans le cas non trivial (facteurs carrés dans $\mathbb{F}_p[X]$), donc la méthode simple (factorisation dans $\mathbb{F}_p$ puis lift de Hensel) ne marche pas.