UNIVERSITÉ DE BORDEAUX
M1, Théorie des Nombres
2020-2021

Feuille 9. Groupe des unités. Groupe de classes

Exercice 1. Cet exercice fait suite à l'exemple 4.2.7 du cours. Soit $d > 1$ un entier sans facteurs carrés. On note $\sqrt{d}$ la racine carré positive de d et on pose $K = \mathbf{Q}[\sqrt{d}]$. On suppose que $d \equiv 1 \pmod 4$.

1) Rappeler pourquoi le groupe des unités $U(O_K)$ est isomorphe aux produit direct $\{-1, 1\} \times \mathbf{Z}$. En déduire que les unités **positives** de O_K forment un groupe cyclique $U^+(O_K)$.

Le groupe $U^+(O_K)$ admet un seul générateur > 1. On l'appelle l'unité fondamentale de K.

2) Montrer que $\frac{a+b\sqrt{d}}{2}$ $(a, b \in \mathbf{Z})$ est une unité de O_K si et seulement si

$$a^2 - db^2 = \pm 4. \tag{1}$$

3) Soit $u_1 = \frac{a_1+b_1\sqrt{d}}{2}$ l'unité fondamentale. Montrer que $a_1, b_1 > 0$.
Montrer que les solutions de l'équation (1) en nombres entiers > 0 sont

$$u_n = \frac{a_n + b_n\sqrt{d}}{2}, \qquad n \geqslant 1,$$

où $a_n + b_n\sqrt{d} = 2^{1-n}(a_1 + b_1\sqrt{d})^n$. En particulier, u_1 est le plus nombre réel de la forme $\frac{a+b\sqrt{d}}{2}$ tel que a et b sont des entiers positifs vérifiant l'équation (1).

4) Trouvez les unités fondamentales des corps $K = \mathbf{Q}[\sqrt{d}]$ pour $d = 5, 13, 17$.

Exercice 2. Soit K un corps de nombres. Montrer que $U(O_K)$ est fini si et seulement si $K = \mathbf{Q}$ ou K est quadratique imaginaire.

Exercice 3. Soit $p > 2$ un nombre premier et soit $K = \mathbf{Q}[\zeta_p]$ où ζ_p est une racine primitive de l'unité d'ordre p . On a montré que l'idéal pO_K est totalement ramifié dans O_K:

$$pO_K = \mathfrak{p}^{p-1},$$

où $\mathfrak{p}$ est un idéal maximal de O_K. Montrer que $\mathfrak{p}$ est l'idéal principal engendré par $\zeta_p - 1$.

Indication: On sait que $p = N_{K/\mathbf{Q}}(1 - \zeta_p)$, où $N_{K/\mathbf{Q}}$ est la norme (cf. question 4b) de l'exercice 5,feuille 4). Écrire p sous la forme $p = (\zeta_p - 1)^{p-1}u$. Utiliser la proposition 4.2.8 du cours pour montrer que u est une unité.

Exercice 4. Soit $p > 2$ un nombre premier. Soit $K = \mathbf{Q}[\zeta_p]$ où ζ_p est une racine primitive de l'unité d'ordre p. On considère K comme un sous-corps de $\mathbb{C}$. On note G le groupe de Galois de $K/\mathbf{Q}$ et $c \in G$ la conjugaison complexe $c(x) = \bar{x}$. Soit $K^+ = K^{<c>}$ le sous-corps de K fixé par c. On pose $\alpha = \zeta_p + \zeta_p^{-1}$.

1) Rappeler pourquoi $[K : K^+] = 2$ et $K^+ = \mathbf{Q}[\alpha]$.

2) Soit $u \in U_K$ une unité de O_K. Montrer que $g(u) \in U_K$ pour tout $g \in G$.

3) Montrer que pour tout $g \in G$ on a

$$\left| g\left(\frac{u}{\bar{u}}\right) \right| = 1.$$

4) Montrer que $u/\bar{u}$ est une racine de l'unité (cf. Feuille 2, Ex. 3).

5) Supposons que $u/\bar{u} = \zeta_p^a$, où $0 \leqslant a \leqslant p-1$. Montrer qu'il existe $k \in \mathbf{Z}$ tel que $u\zeta_p^k \in K^+$.

6) Supposons que $u/\bar{u} = -\zeta_p^a$, où $0 \leqslant a \leqslant p-1$. On note $\mathfrak{p}$ l'unique idéal maximal au dessus de p. Montrer que $u \equiv -u \pmod{\mathfrak{p}}$ et en déduire une contradiction. Indication: utiliser l'exercice 3 et le fait que $O_K = \mathbf{Z}[\zeta_p]$.

7) En déduire que $U_K = \langle \zeta_p \rangle \, U_{K^+}$.

Exercice 5.
Soit $K = \mathbf{Q}[\zeta_5]$. Utiliser l'exercice précédent pour montrer que

$$U(O_K) = \left\{ \pm \zeta_5^k \left(\frac{1+\sqrt{5}}{2} \right)^m \mid 0 \leqslant k \leqslant 4, \quad m \in \mathbf{Z} \right\}.$$

Exercice 6. Soit K un corps de nombres. Rappelons que tout élément non nul de O_K se décompose en produit d'éléments irréductibles (cf. exercice 4 de la feuille 1), mais que, en général, cette factorisation n'est pas unique. Le but de cet exercice est de prouver l'assertion suivante (théorème de Carlitz):

Supposons que $h_K = 2$. Soit

$$x = \pi_1 \pi_2 \cdot \cdot \pi_n = \pi'_1 \pi'_2 \cdot \cdot \pi'_m$$

deux factorisations d'un élément non nul $x \in O_K$ en produit d'irréductibles. Alors $m = n$. On suppose que $h_K = 2$.

1) Soit $\pi \in O_K$ un élément irréductible. Montrer que soit l'idéal principal πO_K est maximal, soit il s'écrit comme le produit de deux idéaux maximaux non principaux.

2) Let $I(K)$ l'ensemble des idéaux non nuls de O_K. Montrer qu'il existe une application $\psi : I(K) \to \mathbf{N}$ telle que :
a) $\psi(IJ) = \psi(I)\psi(J)$ pour tous $I, J \in I(K)$.
b) Pour tout idéal premier $\mathfrak{p}$, $\psi(\mathfrak{p}) = 1$ si $\mathfrak{p}$ n'est pas principal et $\psi(\mathfrak{p}) = 2$ sinon.
3) Prouver le théorème de Carlitz.