Université Pierre et Marie Curie - Paris VI
Master Mathématiques fondamentales

Faculté de Mathématiques
2013–2014

Théorie algébrique des nombres

Corrigé succinct de l'examen du 21 Octobre 2013.

Exercice 1. i. L'extension $\mathbb{Q}(\zeta_q) \supset \mathbb{Q}$ est Galoisienne de groupe de Galois $\mathbb{F}_q^\times$. Puisque ce groupe est abélien, tout sous-corps K de $\mathbb{Q}(\zeta_q)$ est Galoisien sur $\mathbb{Q}$ et son groupe de Galois est un quotient de $\mathbb{F}_q^\times$ qui est cyclique, donc est cyclique.

ii. On sait que $\{\text{premiers } p \text{ ramifiés dans } \mathbb{Q}(\zeta_q)\} = \{q\}$, donc $\{\text{premiers } p \text{ ramifiés dans } K\} \subseteq \{q\}$. Par ailleurs, cet ensemble est non vide puisque $K \neq \mathbb{Q}$.

iii. On sait que le degré résiduel $f(\mathfrak{p}|p)$ est l'ordre du Frobenius $\left(\frac{K/\mathbb{Q}}{p}\right)$ dans $G_{K/\mathbb{Q}}$. Ce dernier est l'image du Frobenius $\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right) = p$ dans $G_{\mathbb{Q}(\zeta_q)/\mathbb{Q}} = \mathbb{F}_q^\times$ par la surjection $G_{\mathbb{Q}(\zeta_q)/\mathbb{Q}} \longrightarrow G_{K/\mathbb{Q}}$. Maintenant on applique la remarque suivante sur les groupes cycliques : si $x \in \mathbb{Z}/n\mathbb{Z}$, et $n = n_1 n_2$, alors l'ordre de x dans le quotient $\mathbb{Z}/n_1\mathbb{Z}$ est l'ordre de $n_2 x$ dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 2. i. Ecrivons, $\alpha = a + b\sqrt{d}$ dans K. Alors $(\mathfrak{p}')^m = (a - b\sqrt{d})$. Donc si $\alpha \in \mathbb{Z}$, on obtient $\mathfrak{p}^m = \mathfrak{p}'^m$, ce qui contredit l'unicité de la factorisation en produit d'idéaux premiers (puisque $\mathfrak{p} \neq \mathfrak{p}'$). Par ailleurs on a $p^m = |N_{K/\mathbb{Q}}(\alpha)| = |\mathcal{O}_K : (\alpha)| = |\mathcal{O}_K/\mathfrak{p}^m| = |\mathcal{O}_K/\mathfrak{p}|^m = p^m$.

ii. On a $|N_{K/\mathbb{Q}}(\alpha)| = a^2 - db^2 \geqslant db^2$. Or $b \in \frac{1}{2}\mathbb{Z} \setminus \{0\}$, donc $p^m \geqslant d^2/4$. On en déduit que $\mathfrak{p}$ est d'ordre $\geqslant \log(|d|/4)/\log(p)$ dans le groupe de classes.

iii. Si on sait qu'il existe une infinité de premiers $p \equiv -1(3)$ alors il exite évidemment une infinité de d comme demandé. Sinon c'est qu'il existe une infinité de premiers $p \equiv 1(3)$ et les $d = 5p$ font l'affaire. Dans tous les cas, la congruence $d \equiv 1 (\text{mod } 3)$ assure que 3 est décomposé, donc le nombre de classes de $\mathbb{Q}(\sqrt{d})$ est $\geqslant \log(|d|/4)/\log(3)$.

Exercice 3. i. Si $\mathfrak{p}^m = (\alpha)$, on prend $L = K(\alpha^{1/m})$. On a alors $(\mathfrak{p}.\mathcal{O}_L)^m = (\alpha^{1/m})^m$ donc $(\mathfrak{p}.\mathcal{O}_L) = (\alpha^{1/m})$ car le groupe des idéaux fractionnaires est sans torsion (libre avec pour base les idéaux premiers).

TSVP

ii. On sait que $\mathcal{C}\ell(\mathcal{O}_K)$ est fini. Soient $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ des éléments dont les classes engendrent le groupe de classes, et $m_1, \cdots, m_r$ les ordres de ces classes, de sorte que $\mathfrak{p}_i^{m_i} = (\alpha_i)$. Il suffit de prendre $L = K(\alpha_1^{1/m_1}, \cdots, \alpha_r^{1/m_r})$.

Exercice 4. Montrer que le polynôme $(X^2-2)(X^2-17)(X^2-34)$ admet une racine dans $\mathbb{Z}_p$ pour tout premier p. Si $p \neq 2, 17$, alors les trois polynômes $(X^2-2), (X^2-17)$ et (X^2-34) sont séparables, et au moins l'un d'eux est scindé (car le produit de deux non-carrés mod p est un carré mod p). Donc par le lemme de Hensel, on trouve une racine dans $\mathbb{Z}_p$. Si $p = 17$, $X^2 - 2 \equiv (X-6)(X+6) \pmod{17}$ donc idem avec Hensel. Pour $p = 2$, on ne peut pas raisonner comme ceci, car les trois polynômes sont inséparables. En fait X^2-2 et X^2-34 sont irréductibles par le critère d'Eisenstein, donc notre seule chance est avec $f(X) = X^2 - 17$. Mais si on remarque que que $|f(1)|_2 = 2^{-4} < |f'(1)|_2^2 = 2^{-2}$, on peut appliquer l'algorithme de Newton pour construire une racine de f dans $\mathbb{Z}_2$.

Exercice 5. Soit $f(X) = X^3 - 3X + 1$.

i. On peut remarquer que $f(T-1) = T^3 - 3T^2 + 3$ est d'Eisenstein en 3, donc f est irréductible.

ii. On calcule que $|\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})| = 81$, donc $\mathcal{O}_K \supset \mathbb{Z}[\alpha] \supset 9\mathcal{O}_K$. Mais puisque $f(T-1)$ est Eisenstein en 3, un résultat du cours nous donne $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

iii. La majoration de Minkowski montre que $|\mathcal{C}\ell(\mathcal{O}_K)| \leqslant 2$. Il faut donc montrer que les idéaux premiers contenant 2 sont principaux. Or 2 est inerte puisque $X^3 - 3X + 1$ n'a pas de racine dans $\mathbb{F}_2$ (donc y est irréductible).