ENS de Lyon
M1 Introduction à la théorie des nombres

Examen du 23 avril 2019

Ce sujet comporte un exercice et deux problèmes

Exercice

Soit $f \in \mathbf{Z}[T]$ un polynôme unitaire non constant. Démontrer qu'il existe une infinité de nombres premiers p tels que f ait une racine modulo p.

Problème 1

Première partie

On dit qu'une forme binaire q représente *primitivement* un entier n s'il existe $(x, y) \in \mathbf{Z}^2$ tel que $\mathrm{pgcd}(x, y) = 1$ et $q(x, y) = n$.

1. (i) Démontrer que $\mathrm{SL}_2(\mathbf{Z})$ agit transitivement sur l'ensemble des couples $(x, y) \in \mathbf{Z}^2$ tels que $\mathrm{pgcd}(x, y) = 1$.
   (ii) En déduire qu'une forme binaire q représente primitivement un entier n si et seulement si $q \overset{+}{\sim} (n, b', c')$, avec $b', c' \in \mathbf{Z}$.
2. Soit $n \neq 0$ et D deux nombres entiers. Démontrer que les conditions suivantes sont équivalentes :
   (a) il existe une forme binaire de discriminant D qui représente primitivement n ;
   (b) D est un carré modulo $4n$.
3. En déduire que si un entier n est représenté par une forme binaire de discriminant D et si p est un nombre premier impair tel que $\left(\frac{D}{p}\right) = -1$, alors la valuation p-adique de n est paire.

Deuxième partie

L'objectif des questions suivantes est de caractériser les entiers pouvant s'écrire sous la forme $x^2 + 5y^2$, avec $x, y \in \mathbf{Z}$.

On rappelle que $q_1 = (1, 0, 5)$ et $q_2 = (2, 2, 3)$ sont les deux formes réduites de discriminant -20.

4. Démontrer que le produit de deux entiers représentés par q_2 est représenté par q_1.
   (*Indication : exprimer q_2 à l'aide de* $\mathrm{N}_{K/\mathbf{Q}}$.)
5. Démontrer qu'un nombre premier p est représenté par q_1 ou q_2 si et seulement si $p \equiv 1, 2, 3, 5, 7, 9 \pmod{20}$, et qu'alors seule l'une de ces deux formes représente p.
6. Déduire de ce qui précède qu'un nombre entier $n \geqslant 1$ s'écrit sous la forme $x^2 + 5y^2$ si et seulement s'il satisfait aux deux conditions suivantes :
   (a) la valuation p-adique de n est paire pour tout nombre premier $p \equiv 11, 13, 17, 19 \pmod{20}$;
   (b) la somme des valuations p-adiques de n pour $p \equiv 2, 3, 7 \pmod{20}$ est paire.

Problème 2

Soit K un corps de nombres quadratique. Son discriminant D_K s'écrit sous la forme

$$D_K = \pm p_1^{\alpha} p_2 \cdots p_t$$

avec $t \geqslant 1$, $p_1 = 2, p_2, \ldots, p_t$ des nombres premiers deux à deux distincts et $\alpha \in \{0, 2, 3\}$. Pour tout $i \in \{1, \ldots, t\}$, on désigne par $\mathfrak{p}_i$ l'unique idéal premier de $\mathcal{O}_K$ divisant p_i.

On rappelle que le *groupe de classes restreint* de K est le quotient $\mathrm{Cl}^+(K)$ du groupe des idéaux fractionnaires de K par le sous-groupe $\mathrm{P}^+(K)$ des idéaux principaux engendrés par un élément x de $K^\times$ tel que $\mathrm{N}_{K/\mathbf{Q}}(x) > 0$. La classe d'un idéal fractionnaire $\mathfrak{a}$ dans $\mathrm{Cl}^+(K)$ est notée $[\mathfrak{a}]_+$. Le *nombre de classes restreint* de K est

$$h_K^+ = \mathrm{Card}\ \mathrm{Cl}^+(K).$$

On désigne par σ l'unique automorphisme non trivial de K. On vérifie aisément que l'on définit une *involution* de $\mathrm{Cl}^+(\mathcal{O}_K)$ en posant

$$\sigma([\mathfrak{a}]_+) = [\sigma(\mathfrak{a})]_+$$

pour tout idéal fractionnaire $\mathfrak{a}$.

Un élément x de $K^\times$ est dit *totalement positif* si $\tau(x) > 0$ pour tout plongement τ de K dans $\mathbf{R}$; on le note $x \gg 0$. On observera que, si K n'admet aucun plongement réel, alors tous les éléments de $K^\times$ sont totalement positifs.

1. Questions préliminaires.

1. Démontrer que les conditions suivantes sont équivalentes pour tout $x \in K^\times$:
   (a) $\mathrm{N}_{K/\mathbf{Q}}(x) > 0$
   (b) $x \gg 0$ ou $-x \gg 0$.
2. Démontrer l'identité
   $$\mathfrak{a} \cdot \sigma(\mathfrak{a}) = (\mathrm{N}(\mathfrak{a}))$$
   pour tout idéal fractionnaire $\mathfrak{a}$ de K.
3. Soit x un élément de $K^\times$ tel que $\mathrm{N}_{K/\mathbf{Q}}(x) = 1$.
   (i) Démontrer que l'image de l'application $K \to K$, $y \mapsto y - x\sigma(y)$, est un sous-$\mathbf{Q}$-espace vectoriel strict.
   (ii) En déduire qu'il existe $y \in K^\times$ tel que $x = y/\sigma(y)$.

2. Unités totalement positives

Désignons par ψ l'automorphisme de $K^\times$ défini par $\psi(x) = x/\sigma(x)$. On vérifie immédiatement que le sous-groupe

$$E(K) = \{u \in \mathcal{O}_K^\times \mid u \gg 0\}$$

est stabilisé par ψ.

4. Décrire la structure du groupe $E(K)$.
5. En déduire l'identité
   $$(E(K) : \psi(E(K))) = 2.$$
6. Si $D_K > 0$ et D_K est divisible par un nombre premier $p \equiv 3 \pmod 4$, démontrer que l'on a
   $$E(K) = \mathcal{O}_K^\times.$$

3. Classes ambiguës.

On dit qu'un idéal fractionnaire $\mathfrak{a}$ (resp. une classe $c \in \mathrm{Cl}^+(K)$) est *ambigu* (resp. *ambiguë*) si $\sigma(\mathfrak{a}) = \mathfrak{a}$ (resp. $\sigma(c) = c$). Posons

$$A(K) = \{\mathfrak{a} \text{ idéal non nul de } \mathcal{O}_K \mid \sigma(\mathfrak{a}) = \mathfrak{a}\}$$

et

$$\mathrm{Am}^+(K) = \{c \in \mathrm{Cl}^+(K) \mid \sigma(c) = c\}.$$

7. Démontrer que l'application $\lambda^+ : A(K) \to \mathrm{Am}^+(K),\ \mathfrak{a} \mapsto [\mathfrak{a}]_+$ est surjective.
8. Démontrer qu'un idéal fractionnaire est ambigu si et seulement s'il est de la forme

$$(r) \cdot \mathfrak{p}_1^{\varepsilon_1} \cdots \mathfrak{p}_t^{\varepsilon_t}$$

avec $r \in \mathbf{Q}^\times$ et $\varepsilon_1, \ldots, \varepsilon_t \in \{0, 1\}$.

9. Soit I le sous-groupe de $P^+(K)$ engendré par les nombres rationnels. Construire un isomorphisme entre $\ker(\lambda^+)/I$ et $E(K)/\psi(E(K))$.
10. En déduire que le groupe $\mathrm{Am}^+(K)$ est isomorphe à $\{\pm 1\}^{t-1}$.
11. Démontrer que le nombre de classes restreint h_K^+ est impair si et seulement si $t = 1$.

4. Application : une démonstration de la loi de réciprocité quadratique

Les questions précédentes conduisent à une nouvelle preuve de l'identité

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$$

pour tous nombres premiers impairs distincts p, q, où l'on a posé $q^* = (-1)^{(q-1)/2} q$.

12. Supposons tout d'abord $p \equiv 1 \pmod 4$.
    (i) Démontrer que les nombres de classes des corps $K = \mathbf{Q}(\sqrt{p})$ et $L = \mathbf{Q}(\sqrt{q^*})$ sont impairs.
    (ii) Si $\left(\frac{p}{q}\right) = 1$, en déduire qu'il existe $x, y \in \mathbf{Z}$ tels que $4q^{h_K} = \pm(x^2 - py^2)$, puis que l'on a $\left(\frac{q}{p}\right) = 1$.
    (iii) Si $q \equiv 3 \pmod 4$ et $\left(\frac{q}{p}\right) = 1$, prouver qu'il existe $x, y \in \mathbf{Z}$ tels que $4p^{h_L} = x^2 - q^* y^2$, puis que l'on a $\left(\frac{p}{q}\right) = 1$.
13. Supposons $p \equiv q \equiv 3 \pmod 4$.
    (i) Démontrer que le nombre de classes du corps $\mathbf{Q}(\sqrt{pq})$ est impair.
    (ii) En déduire que l'idéal $\mathfrak{p} = (p, \sqrt{pq})$ est principal.
    (iii) En déduire qu'il existe $x, y \in \mathbf{Z}$ tels que $4 = \pm(px^2 - qy^2)$.
    (iv) En déduire $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.