Examen d'Arithmétique

Jeudi 25 avril 2024. 3 heures.

Documents, calculatrices, montres connectées et téléphones interdits.

Exercice 1 On considère le corps de nombres $K = \mathbb{Q}(\sqrt{23})$.

1. Déterminer l'anneau des entiers $\mathcal{O}_K$ de K, en utilisant les résultats du cours.
2. Calculer la décomposition en fraction continue de $\sqrt{23}$ et vérifier qu'elle est ultimement périodique de période 4.
3. Soit $\mathcal{O}_K^\times$ le groupe des inversibles multiplicatifs de $\mathcal{O}_K$. Caractériser les éléments de $\mathcal{O}_K^\times$ parmi ceux de $\mathcal{O}_K$ au moyen de la norme $N_{K/\mathbb{Q}}$ et écrire explicitement l'équation diophantienne correspondante.
4. En déduire que le quotient $\mathcal{O}_K^\times/\{\pm 1\}$ est infini monogène et en calculer un générateur.
5. Peut-on trouver une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients entiers et de déterminant ± 1 telle que $\frac{a\sqrt{23}+b}{c\sqrt{23}+d}$ ait un développement en fraction continue ultimement périodique de période 3 ?

Corrigé :

1. Comme $K = \mathbb{Q}(\sqrt{23})$ avec 23 sans diviseur carré et $23 \equiv 3$ modulo 4, l'anneau des entiers $\mathcal{O}_K = \mathbb{Z}[\sqrt{23}]$.
2. La partie entière de $\sqrt{23}$ est $4 = a_0$. Le reste $r_0 = \sqrt{23} - 4$ a pour inverse $\frac{1}{7}(\sqrt{23}+4)$, de partie entière $1 = a_1$. Le reste suivant $r_1 = \frac{1}{7}(\sqrt{23}-3)$ a pour inverse $\frac{1}{2}(\sqrt{23}+3)$, de partie entière $3 = a_2$. Le reste suivant $r_2 = \frac{1}{2}(\sqrt{23}-3)$ a pour inverse $\frac{1}{7}(\sqrt{23}+3)$, de partie entière $1 = a_3$. Le reste suivant $r_3 = \frac{1}{7}(\sqrt{23}-4)$ a pour inverse $\sqrt{23}+4$, de partie entière $8 = a_3$. Le reste suivant $r_4 = \sqrt{23} - 4 = r_0$, donc la suite des coefficients se répète avec une période 4. On obtient donc $\sqrt{23} = [4; \overline{1, 3, 1, 8}]$.
3. Comme la norme est multiplicative et prend des valeurs entières sur $\mathcal{O}_K$, la norme d'un élément de $\mathcal{O}_K^\times$ est dans $\mathbb{Z}^\times = \{\pm 1\}$. Réciproquement, si u est de norme ± 1, l'idéal principal (u) est de norme 1 de sorte que c'est $\mathcal{O}_K = (1)$ et donc u est inversible. Un élément $u \in \mathcal{O}_K$ s'écrit $u = x + y\sqrt{23}$ avec $x, y \in \mathbb{Z}$. Sa norme est donnée par $N_{K/\mathbb{Q}}(u) = x^2 - 23y^2$, de sorte que les coefficients x et y sont des solutions de l'équation de Pell-Fermat $x^2 - 23y^2 = \pm 1$.
4. Les solutions de l'équation de Pell-Fermat sont de la forme $\pm(x_1 + y_1\sqrt{23})^n$ avec $n \in \mathbb{Z}$, où (x_1, y_1) est la solution minimale. Le quotient $\mathcal{O}_K^\times/\{\pm 1\}$ est donc le groupe infini cyclique engendré multiplicativement par $x_1 + y_1\sqrt{23}$. La fraction continue pour $\sqrt{23}$ étant de période 4, la solution minimale est

obtenue par la réduite d'ordre $4-1=3$, qui s'écrit $\frac{x_1}{y_1} = [4;1,3,1] = 24/5$. Le générateur recherché est donc $24+5\sqrt{23}$.

5. Par un résultat du cours, tous les nombres réels dans une même orbite de l'action homographique de $GL_2(\mathbb{Z})$ ont un développement en fraction continue ayant la même queue. On a calculé que celui de $\sqrt{23}$ est ultimement périodique de période 4, donc il en va de même pour tous les réels de la forme $A \cdot \sqrt{23}$ avec $A \in GL_2(\mathbb{Z})$. En particulier, on ne peut pas obtenir de cette manière une fraction continue ultimement périodique de période 3.

Exercice 2 On considère la fonction sommatoire $M_\mu(x) = \sum_{n\leq x} \mu(n)$ de la fonction de Möbius μ.

1. Montrer par un argument très simple que $M_\mu(x) = O(x)$ lorsque $x \to \infty$.
2. Montrer que l'inverse de la fonction zêta peut s'écrire sous la forme suivante :

$$\frac{1}{\zeta(s)} = s\int_1^\infty \frac{M_\mu(x)}{x^{s+1}}dx,$$

lorsque $\mathrm{Re}(s) > 1$.

3. Soit $c \in [\frac{1}{2}, 1]$ tel que $M_\mu(x) = O(x^c)$ lorsque $x \to \infty$. Montrer que la formule ci-dessus pour l'inverse de la fonction zêta est valide pour $\mathrm{Re}(s) > c$.
4. En déduire que, si on suppose que $M_\mu(x) = O(x^{\frac{1}{2}+\varepsilon})$ pour tout $\varepsilon > 0$, alors l'hypothèse de Riemann est vérifiée.

Corrigé :

1. Comme $\mu(n) = (-1)^k$ si n est le produit de k nombres premiers distincts, et $\mu(n) = 0$ sinon, on a en particulier $|\mu(n)| \leq 1$ pour tout $n \in \mathbb{N}^*$. Par conséquent, $|M_\mu(x)| \leq x$ pour tout réel $x > 0$, de sorte que $M_\mu(x) = O(x)$ lorsque $x \to \infty$.
2. Calculons $\sum_{n\leq x} \frac{\mu(n)}{n^s}$ en appliquant le lemme de sommation par parties à la fonction arithmétique μ et à la fonction $g(x) = x^{-s}$ de classe $\mathcal{C}^1$. On obtient

$$\begin{aligned}\sum_{\frac{1}{2}<n\leq x} \frac{\mu(n)}{n^s} &= M_\mu(x)x^{-s} - M_\mu(\frac{1}{2})x^{-\frac{1}{2}} - \int_{\frac{1}{2}}^x M_\mu(y)(-sy^{-s-1})dy \\ &= M_\mu(x)x^{-s} + s\int_1^x \frac{M_\mu(y)}{y^{s+1}}dy,\end{aligned}$$

puisque $M_\mu(x) = 0$ lorsque $x < 1$. Lorsque $\mathrm{Re}(s) > 1$, l'expression $M_\mu(x)x^{-s}$ tend vers 0 lorsque $x \to \infty$ puisque $M_\mu(x) = O(x)$. D'autre part, l'intégrale converge lorsque $x \to \infty$ puisque l'intégrande est majoré en module par

$\frac{1}{y^{\mathrm{Re}(s)}}$. Par conséquent, la série de Dirichlet de μ est donnée par $D_\mu(s) = s\int_1^\infty \frac{M_\mu(x)}{x^{s+1}}dx$. D'autre part, $D_\mu D_{\mathbb{1}} = D_{\mu * \mathbb{1}} = D_e = 1$ et $D_{\mathbb{1}} = \zeta$, de sorte que $D_\mu(s) = \frac{1}{\zeta(s)}$ et on obtient la formule souhaitée.

3. Si $M_\mu(x) = O(x^c)$ lorsque $x \to \infty$, l'expression $M_\mu(x)x^{-s}$ tend vers 0 lorsque $x \to \infty$ dès que $\mathrm{Re}(s) > c$. De même, l'intégrale obtenue par sommation par parties a son intégrande majoré en module par $y^{c-\mathrm{Re}(s)-1}$ de sorte que l'intégrale de 1 à ∞ converge dès que $\mathrm{Re}(s) > c$.
4. La formule précédente montre que la fonction $\frac{1}{\zeta(s)}$ est holomorphe lorsque $\mathrm{Re}(s) > \frac{1}{2} + \varepsilon$ pour tout $\varepsilon > 0$, donc lorsque $\mathrm{Re}(s) > \frac{1}{2}$. En particulier, la fonction zêta ne s'annule pas lorsque $\frac{1}{2} < \mathrm{Re}(s) \leq 1$. Comme les zéros de la fonction zêta situés dans la bande $0 \leq \mathrm{Re}(s) \leq 1$ occupent des positions symétriques par rapport à la droite d'équation $\mathrm{Re}(s) = \frac{1}{2}$, en vertu de l'équation fonctionnelle satisfaite par la fonction zêta, il n'y a pas non plus de zéros sur la bande $0 \leq \mathrm{Re}(s) < \frac{1}{2}$. Par conséquent, les zéros de la fonction zêta dans la bande $0 \leq \mathrm{Re}(s) \leq 1$ doivent satisfaire $\mathrm{Re}(s) = \frac{1}{2}$, c'est l'hypothèse de Riemann.

Exercice 3 On considère le corps de nombres $\mathbb{Q}(\sqrt{-14})$.

1. Donner un élément $\alpha \in K$ tel que $\mathcal{O}_K = \mathbb{Z}[\alpha]$, en utilisant les résultats du cours.
2. Déterminer toutes les formes quadratiques binaires définies positives, réduites et primitives de discriminant -56.
3. Montrer que le cardinal du groupe des classes de $\mathcal{O}_K$ est égal à 4.
4. Montrer que la forme quadratique binaire $[1, 0, 14]$ obtenue précédemment correspond à la classe des idéaux principaux de $\mathcal{O}_K$.
5. Montrer que $2, 3$ et 11 sont des éléments irréductibles de $\mathcal{O}_K$.

Dans la suite de cet exercice on va s'intéresser aux idéaux (p) pour $p \in \{2, 3, 11\}$.

6. Montrer que l'idéal (11) est premier dans $\mathcal{O}_K$.
7. Décomposer l'idéal (2) en produit d'idéaux premiers de $\mathcal{O}_K$.
8. Soit I le sous-groupe additif de $\mathcal{O}_K$ engendré par 3 et $1 + i\sqrt{14}$. Montrer que I est un idéal de $\mathcal{O}_K$, de norme 3.
9. Trouver une base directe de l'idéal I^2 en tant que $\mathbb{Z}$-module libre et calculer la forme quadratique binaire associée.
10. En déduire la structure du groupe des classes de $\mathcal{O}_K$.
11. Décomposer l'idéal (3) en produit d'idéaux premiers de $\mathcal{O}_K$.

Corrigé :

1. Comme $-14 \equiv 2$ modulo 4, $\mathcal{O}_K = \mathbb{Z}[i\sqrt{14}]$, de sorte que $\alpha = i\sqrt{14}$.
2. On cherche les formes quadratiques binaires $[a, b, c]$ avec $0 < a \leq \sqrt{\frac{56}{3}} < 5$, $-a < b \leq a \leq c$, $b^2 - 4ac = -56$ et $a \wedge b \wedge c = 1$. Les valeurs possibles de a sont $1, 2, 3$ et 4. Par l'équation du discriminant, b doit être pair. Ainsi, si $a = 1$, alors $b = 0$ et l'équation du discriminant donne $c = 14$ et donc la forme quadratique $[1, 0, 14]$. Si $a = 2$, $b = 0$ ou 2. L'équation du discriminant montre alors que b^2 est multiple de 8, donc b est multiple de 4 et seul $b = 0$ convient. On obtient $c = 7$ et la forme quadratique $[2, 0, 7]$. Si $a = 3$, l'équation du discriminant montre que b ne peut être multiple de 3, de sorte que seul $b = \pm 2$ convient. On obtient alors $c = 5$ et les formes quadratiques $[3, \pm 2, 5]$. Si $a = 4$, l'équation du discriminant montre que b^2 doit être multiple de 8 mais pas de 16, ce qui est impossible.
3. On a obtenu ci-dessus 4 formes quadratiques binaires définies positives, réduites et primitives de discriminant $D = -56 = 4d$ avec $d = -14 \equiv 2$ modulo 4, de sorte que D est le discriminant de $\mathcal{O}_K$ et donc $h_K = h(-56) = 4$.
4. La forme quadratique $[1, 0, 14]$ représente l'entier 1, contrairement aux 3 autres formes quadratiques binaires obtenues. La classe des idéaux principaux contient $(1) = \mathcal{O}_K$ qui est de norme 1, donc $[1, 0, 14]$ correspond à l'inverse de cette classe, c'est-à-dire à cette classe elle-même puisque c'est le neutre dans le groupe des classes d'idéaux.
5. La norme d'un élément $a + bi\sqrt{14} \in \mathcal{O}_K$ (avec donc $a, b \in \mathbb{Z}$) est donnée par $N_{K/\mathbb{Q}}(a + bi\sqrt{14}) = a^2 + 14b^2$. En particulier, 2 est de norme 4. Si $2 = uv$ avec u et v pas inversibles dans $\mathcal{O}_K$, alors les normes de u et v sont positives, ont pour produit 4 et sont différentes de 1, donc sont égales à 2. Mais si $a^2 + 14b^2 = 2$ alors $b = 0$ puis $a^2 = 2$, ce qui n'a pas de solution dans $\mathbb{Z}$, de sorte que 2 est irréductible dans $\mathcal{O}_K$. Le même raisonnement avec la norme 9 de 3 (resp. la norme 121 de 11) et la norme 3 (resp. la norme 11) pour u et v montre que 3 (resp. 11) est également irréductible.
6. Considérons le quotient $\mathcal{O}_K/(11) \simeq \mathbb{F}_{11}[X]/(X^2 + 14)$. Comme $\left(\frac{-14}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{2}{11}\right) = \left(\frac{-9}{11}\right) = \left(\frac{-1}{11}\right) = -1$, le polynôme $X^2 + 14$ n'a pas de racine dans $\mathbb{F}_{11}$ et est donc irréductible. Ainsi, l'anneau quotient est intègre, de sorte que l'idéal (11) est premier.
7. Considérons le quotient $\mathcal{O}_K/(2) \simeq \mathbb{F}_2[X]/(X^2 + 14)$. Comme $X^2 + 14 = X^2$ dans $\mathbb{F}_2[X]$, cet anneau quotient n'est pas intègre puisque $X \cdot X = 0$ dans $\mathbb{F}_2[X]/(X^2 + 14)$, donc (2) n'est pas premier dans $\mathcal{O}_K$. Les idéaux contenant (2) se projettent sur des idéaux de $\mathbb{F}_2[X]/(X^2)$, et seul (X) est un idéal propre non nul. L'idéal $(2, i\sqrt{14})$ est son image réciproque dans $\mathcal{O}_K$. Ses éléments sont de la forme $2a + bi\sqrt{14}$ avec $a, b \in \mathbb{Z}$. Le carré de cet idéal est $(4, 2i\sqrt{14}, -14) = (2)$. La norme de $(2, i\sqrt{14})$ est le nombre premier 2

puisque son carré est 4, la norme de (2). En particulier, $(2, i\sqrt{14})$ est premier, et $(2) = (2, i\sqrt{14})^2$ est la décomposition cherchée.

8. Il suffit de montrer que $I = 3\mathbb{Z}+(1+i\sqrt{14})\mathbb{Z}$ est stable par multiplication par $i\sqrt{14}$. Multiplions ses générateurs par $i\sqrt{14}$: d'une part $3i\sqrt{14} \in I$ et d'autre part $i\sqrt{14}(1 + i\sqrt{14}) = -14 + i\sqrt{14} \in I$. Donc I est un idéal. Considérons le quotient $\mathcal{O}_K/I$: l'image de $a + bi\sqrt{14}$ est représentée par $a - b$ modulo 3, et les entiers $0, 1$ et 2 sont distincts modulo I. Donc la norme de I est égale à 3.
9. L'idéal I^2 est donné par $(9, 3 + 3i\sqrt{14}, -13 + 2i\sqrt{14})$. La somme de ces générateurs est $-1 + 5i\sqrt{14}$ et son produit avec $-i\sqrt{14}$ est $70 + i\sqrt{14}$. En soustrayant un multiple entier de 9, on obtient l'élément $-2 + i\sqrt{14}$ de I^2. Alors $(\alpha_1, \alpha_2) = (9, -2+i\sqrt{14})$ est une base du $\mathbb{Z}$-module I^2, car $3+3i\sqrt{14} = \alpha_1 + 3\alpha_2$ et $-13 + 2i\sqrt{14} = -\alpha_1 + 2\alpha_2$. La partie imaginaire de $\alpha_1\overline{\alpha_2} - \alpha_2\overline{\alpha_1}$ est $-18\sqrt{14} < 0$, donc $(\alpha_2, \alpha_1) = (-2 + i\sqrt{14}, 9)$ est une base directe de I^2. La forme quadratique associée est

$$q(x, y) = \frac{N_{K/\mathbb{Q}}(9y - 2x + ix\sqrt{14})}{N(I^2)} = \frac{(2x - 9y)^2 + 14x^2}{9} = 2x^2 - 4xy + 9y^2.$$

10. La forme quadratique $q = [2, -4, 9]$ est proprement équivalente à $[2, 0, 7]$, ce n'est pas celle des 4 formes quadratiques ci-dessus correspondant à la classe des idéaux principaux. Donc la classe de I^2 n'est pas triviale, et l'ordre de I n'est ni 1 ni 2. Comme il divise $h(-56) = 4$, c'est 4, de sorte que le groupe des classes est cyclique d'ordre 4 car engendré par I.
11. L'idéal $I = (3, 1 + i\sqrt{14})$ a pour norme le nombre premier 3, donc I est un idéal premier. Considérons le $\mathbb{Z}$-module J engendré par 3 et par $1 - i\sqrt{14}$. Par les mêmes arguments que pour I, on montre que $J = (3, 1 - i\sqrt{14})$ est un idéal de norme 3, donc premier. L'idéal IJ est donc de norme 9, tout comme (3). De plus, $3 \in IJ$ car c'est $2 \times 3 \cdot 3 - 1 \times (1 + i\sqrt{14}) \cdot (1 - i\sqrt{14})$. Ainsi $(3) \subset IJ$ sont des idéaux de mêmes normes, donc égaux, et $(3) = IJ$ est la décomposition cherchée.