Examen d'Arithmétique

Mercredi 15 avril 2026. 3 heures.

Documents, calculatrices, montres connectées et téléphones interdits.

On rappelle la borne de Minkowski : si $K = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{N}^*$ non carré, alors toute classe d'idéaux de K contient un idéal I de $\mathcal{O}_K$ dont la norme vérifie $N(I) \leqslant \frac{1}{2}\sqrt{|\Delta_{\mathcal{O}_K/\mathbb{Z}}|}$.

Exercice 1 On considère le corps de nombres $K = \mathbb{Q}(\sqrt{15})$.

1. Montrer que l'anneau des entiers $\mathcal{O}_K$ de K est $\mathbb{Z}[\sqrt{15}]$.
2. Montrer que $x + y\sqrt{15} \in \mathcal{O}_K^\times$ avec $x, y \in \mathbb{Z}$ si et seulement si $x^2 - 15y^2 = \pm 1$.
3. Calculer le développement en fraction continue de $\sqrt{15}$.
4. Déduire des deux points précédents que $\mathcal{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ et en identifier des générateurs.
5. Donner toutes les fractions irréductibles $\frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \{1, 2, \ldots, 99, 100\}$ qui sont des meilleures approximations de $\sqrt{15}$.
6. On note $P_2 = 2\mathcal{O}_K + (1 + \sqrt{15})\mathcal{O}_K$ et $P_3 = 3\mathcal{O}_K + \sqrt{15}\mathcal{O}_K$.
   Montrer que $P_2^2 = 2\mathcal{O}_K$ et que $P_3^2 = 3\mathcal{O}_K$.
7. En déduire la norme de P_2 et de P_3. Les idéaux P_2 et P_3 sont-ils premiers ?
8. Donner une base de P_2 et de P_3 en tant que $\mathbb{Z}$-modules libres.
9. Pour tout idéal non nul I de $\mathcal{O}_K$, montrer que $N(I) \in I \cap \mathbb{Z}$.
10. Montrer que le groupe des classes $\mathrm{Cl}(\mathcal{O}_K)$ est engendré par les classes des idéaux P_2 et P_3 (on pourra utiliser la borne de Minkowski).
11. Calculer la norme de $3 + \sqrt{15}$. En considérant la factorisation de l'idéal $(3 + \sqrt{15})\mathcal{O}_K$ en produit d'idéaux premiers dans $\mathcal{O}_K$, montrer que $\mathrm{Cl}(\mathcal{O}_K)$ est engendré par la classe de P_2.
12. Montrer que le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est d'ordre 2.

Corrigé :

1. Comme $15 \equiv 3 \bmod 4$, par un résultat du cours on a $\mathcal{O}_K = \mathbb{Z}[\sqrt{15}]$.
2. Si $x + y\sqrt{15} \in \mathcal{O}_K^\times$ alors $N_{K/\mathbb{Q}}(x + y\sqrt{15}) = x^2 - 15y^2 \in \mathbb{Z}^\times = \{-1, +1\}$. Réciproquement, si $x^2 - 15y^2 = \pm 1$ alors $\pm(x - y\sqrt{15})$ est un inverse pour $x + y\sqrt{15}$ dans $\mathbb{Z}[\sqrt{15}]$.
3. La partie entière de $\sqrt{15}$ est $3 = a_0$. On obtient $r_1 = \frac{1}{\sqrt{15}-3} = \frac{\sqrt{15}+3}{6}$, qui a pour partie entière $1 = a_1$. On obtient $r_2 = \left(\frac{\sqrt{15}+3}{6} - 1\right)^{-1} = \sqrt{15} + 3$ qui a pour partie entière $6 = a_2$. On obtient $r_3 = \frac{1}{\sqrt{15}-3} = r_1$, de sorte que le développement devient périodique de période $s = 2$ à partir de a_1. Ainsi, $\sqrt{15} = [3, \overline{1, 6}]$.

4. La solution minimale de l'équation de Pell-Fermat $x^2-15y^2=\pm 1$ est donnée par $x=p_1$ et $y=q_1$ avec $\frac{p_1}{q_1}=[3,1]=\frac{4}{1}$. L'ensemble des solutions est donné par $\{\pm(x_n+y_n\sqrt{15})=\pm(4+\sqrt{15})^n, n\in\mathbb{Z}\}$. On a donc bien $\mathbb{Z}[\sqrt{15}]^\times = \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}$, où -1 est un générateur du facteur $\mathbb{Z}/2\mathbb{Z}$ et $4+\sqrt{15}$ est un générateur du facteur $\mathbb{Z}$.
5. Les meilleures approximations de $\sqrt{15}$ sont des réduites de son développement en fraction continue. Les premières réduites de $\sqrt{15}=[3,\overline{1,6}]$ sont $[3]=\frac{3}{1}$, $[3,1]=\frac{4}{1}$, $[3,1,6]=\frac{6\times4+3}{6\times1+1}=\frac{27}{7}$, $[3,1,6,1]=\frac{27+4}{7+1}=\frac{31}{8}$, $[3,1,6,1,6]=\frac{6\times31+27}{6\times8+7}=\frac{213}{55}$, $[3,1,6,1,6,1]=\frac{213+31}{55+8}=\frac{244}{63}$. Le dénominateur de la réduite suivante $[3,1,6,1,6,1,6]$ est égal à $6\times63+55$, donc supérieur à 100, de même que les dénominateurs de toutes les réduites suivantes. La première réduite $\frac{3}{1}$ n'est pas une meilleure approximation de $\sqrt{15}$ car $\sqrt{15}>\lfloor\sqrt{15}\rfloor+\frac{1}{2}$, mais les autres réduites le sont. On obtient donc les meilleures approximations $\frac{4}{1}$, $\frac{27}{7}$, $\frac{31}{8}$, $\frac{213}{55}$ et $\frac{244}{63}$ ayant un dénominateur ne dépassant pas 100.
6. D'une part, on calcule $P_2^2=(2\mathcal{O}_K+(1+\sqrt{15})\mathcal{O}_K)^2=4\mathcal{O}_K+2(1+\sqrt{15})\mathcal{O}_K+(16+2\sqrt{15})\mathcal{O}_K=2\left(2\mathcal{O}_K+(1+\sqrt{15})\mathcal{O}_K+(8+\sqrt{15})\mathcal{O}_K\right)$. Comme l'idéal entre parenthèses contient $1+\sqrt{15}$ et $8+\sqrt{15}$, il contient aussi $(8+\sqrt{15})-(1+\sqrt{15})=7$. Comme il contient 2 et 7, il contient aussi $2\wedge 7=1$, donc c'est $\mathcal{O}_K$, de sorte que $P_2^2=2\mathcal{O}_K$.
   D'autre part, on calcule $P_3^2=(3\mathcal{O}_K+\sqrt{15}\mathcal{O}_K)^2=9\mathcal{O}_K+3\sqrt{15}\mathcal{O}_K+15\mathcal{O}_K$. Comme P_3^2 contient 9 et 15, il contient aussi $9\wedge 15=3$. Comme 9, $3\sqrt{15}$ et 15 sont des multiples de 3 dans $\mathcal{O}_K$, l'élément 3 engendre P_3^2, de sorte que $P_3^2=3\mathcal{O}_K$.
7. D'une part, on a $N(P_2)^2=N(P_2^2)=N_{K/\mathbb{Q}}(2)=4$, de sorte que $N(P_2)=2$. D'autre part, on a $N(P_3)^2=N(P_3^2)=N_{K/\mathbb{Q}}(3)=9$, de sorte que $N(P_3)=3$. Comme les normes de P_2 et P_3 sont des nombres premiers, P_2 et P_3 sont des idéaux premiers.
8. D'une part, montrons que $P_2=2\mathbb{Z}+(1+\sqrt{15})\mathbb{Z}$. Il est clair que $2\mathbb{Z}+(1+\sqrt{15})\mathbb{Z}\subset P_2$. Pour montrer que $P_2\subset 2\mathbb{Z}+(1+\sqrt{15})\mathbb{Z}$, il reste à montrer que ce $\mathbb{Z}$-module est stable par multiplication par $\sqrt{15}$. Or $2\sqrt{15}=2\times(1+\sqrt{15})-2$ et $\sqrt{15}(1+\sqrt{15})=15+\sqrt{15}=8(1+\sqrt{15})+7(1-\sqrt{15})$.
   D'autre part, montrons que $P_3=3\mathbb{Z}+\sqrt{15}\mathbb{Z}$. Il est évident que $3\mathbb{Z}+\sqrt{15}\mathbb{Z}\subset P_3$. Pour l'inclusion réciproque, il suffit de montrer que $3\mathbb{Z}+\sqrt{15}\mathbb{Z}$ est stable par multiplication par $\sqrt{15}$. Or $3\sqrt{15}\in\sqrt{15}\mathbb{Z}$ et $\sqrt{15}^2=15\in 3\mathbb{Z}$.
9. Considérons $\mathcal{O}_K/I$ comme un groupe additif de cardinal $N(I)\in\mathbb{N}^*\subset\mathbb{Z}$. La projection $\overline{1}$ de $1\in\mathcal{O}_K$ dans ce groupe est donc d'ordre divisant $N(I)$. En particulier, la somme de $N(I)$ termes $\overline{1}$ est nulle dans $\mathcal{O}_K/I$, autrement dit $N(I)\in I$.
10. Le discriminant de $\mathcal{O}_K$ est donné par $\Delta_{\mathcal{O}_K/\mathbb{Z}}=4\times 15$ puisque $15\equiv 3 \bmod 4$.

La borne de Minkowski montre alors que $\mathrm{Cl}(\mathcal{O}_K)$ est engendré par les classes d'idéaux de norme $\leqslant \frac{1}{2}\sqrt{60} < 4$. Il ne faut donc considérer que les idéaux de normes 2 et 3. D'une part, tout idéal I de norme 2 contient $N(I) = 2$, de sorte que $I \supset 2\mathcal{O}_K = P_2^2$. Mais le seul diviseur de P_2^2 de norme 2 est P_2 lui-même. Donc P_2 est l'unique idéal de $\mathcal{O}_K$ de norme 2. De même, tout idéal I de norme 3 contient $N(I) = 3$, de sorte que $I \supset 3\mathcal{O}_K = P_3^2$. Mais le seul diviseur de P_3^2 de norme 3 est P_3 lui-même. Donc P_3 est l'unique idéal de $\mathcal{O}_K$ de norme 3. Ainsi, $\mathrm{Cl}(\mathcal{O}_K)$ est engendré par les classes de P_2 et de P_3.

11. On a $N_{K/\mathbb{Q}}(3+\sqrt{15}) = 9 - 15 = -6$. Ainsi, l'idéal principal $(3+\sqrt{15})\mathcal{O}_K$ est de norme $|-6| = 6$. Comme 3 et $\sqrt{15}$ sont clairement des éléments de P_3, on a $P_3 \supset I$, de sorte qu'il existe un idéal J de $\mathcal{O}_K$ tel que $I = P_3 J$. Par multiplicativité de la norme, on doit avoir $N(J) = 2$, de sorte que $J = P_2$, et donc $I = P_2P_3$. Ainsi, la classe de P_3 est l'inverse de celle de P_2 dans $\mathrm{Cl}(\mathcal{O}_K)$, et ce dernier est engendré par la seule classe de P_2.
12. On sait déjà que $P_2^2 = 2\mathcal{O}_K$ est principal, de sorte que la classe de P_2 dans $\mathrm{Cl}(\mathcal{O}_K)$ est d'ordre divisant 2. Pour que celle-ci soit d'ordre 2, il suffit donc de montrer que P_2 n'est pas principal. Si c'était le cas, il serait engendré par un élément $x + y\sqrt{15}$ avec $x, y \in \mathbb{Z}$ ayant pour norme $\pm N(P_2) = \pm 2$. Mais l'équation $x^2 - 15y^2 = \pm 2$ n'a pas de solution entières. En effet, en réduisant celle-ci modulo 5, on obtient $x^2 \equiv \pm 2 \bmod 5$, qui est sans solution dans $\mathbb{Z}/5\mathbb{Z}$ puisque $\left(\frac{\pm 2}{5}\right) = -1$.

Exercice 2 On considère la fonction "nombre de diviseurs premiers" ω définie par $\omega(n) = \mathrm{Card}\{p \in \mathcal{P} : p \mid n\}$.

1. Montrer que l'abscisse de convergence de la série de Dirichlet D_ω associée à ω est égale à 1.
2. Montrer que pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$, on a
$$D_\omega(s) = \zeta(s) \sum_p \frac{1}{p^s}.$$
3. A l'aide de l'identité $2^\omega = \mathbb{1} * \mu^2$ établie dans le partiel et dans laquelle μ désigne la fonction de Möbius, montrer que l'abscisse de convergence de la série de Dirichlet D_{2^ω} associée à 2^ω est égale à 1.
4. En utilisant le fait que la fonction 2^ω est multiplicative comme établi dans le partiel, calculer le développement en produit eulérien de D_{2^ω}, afin de montrer que pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$, on a
$$D_{2^\omega}(s) = \prod_p \frac{p^s + 1}{p^s - 1}.$$
5. En déduire que, pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$, on a
$$D_{2^\omega}(s) = \frac{\zeta(s)^2}{\zeta(2s)}.$$
6. Déduire de ce qui précède et avec l'aide du théorème d'Ikehara que la fonction sommatoire M_{μ^2} de μ^2 satisfait
$$M_{\mu^2}(x) \sim_{x \to +\infty} \frac{1}{\zeta(2)} x.$$

Corrigé :

1. D'une part, pour tout $n \geqslant 2$, on a $\omega(n) \geqslant 1$, puisque n a au moins un diviseur premier. Donc par comparaison avec $\mathbb{1}$, on doit avoir $\sigma_c(\omega) \geqslant \sigma_c(\mathbb{1}) = 1$. D'autre part, pour tout $n \in \mathbb{N}^*$, $\omega(n) = \sum_{p|n} 1 = (\mathbb{1}_\mathcal{P} * \mathbb{1})(n)$, où $\mathbb{1}_\mathcal{P}$ est la fonction indicatrice des nombres premiers. Donc $\sigma_a(\omega) \leqslant \max(\sigma_a(\mathbb{1}_\mathcal{P}), \sigma_a(\mathbb{1}))$. Comme $0 \leqslant \mathbb{1}_\mathcal{P} \leqslant \mathbb{1}$, on a $\sigma_a(\mathbb{1}_\mathcal{P}) = \sigma_c(\mathbb{1}_\mathcal{P}) \leqslant \sigma_a(\mathbb{1}) = \sigma_c(\mathbb{1}) = 1$, donc l'inégalité précédente est $\sigma_c(\omega) = \sigma_a(\omega) \leqslant 1$. On en déduit que $\sigma_c(\omega) = 1$.
2. Comme $\omega = \mathbb{1}_\mathcal{P} * \mathbb{1}$, pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > \sigma_a(\omega) = 1$, on a
$$D_\omega(s) = D_\mathbb{1}(s) D_{\mathbb{1}_\mathcal{P}}(s) = \zeta(s) \sum_p \frac{1}{p^s}.$$

3. D'une part, pour tout $n \geqslant 2$, on a $2^\omega(n) \geqslant 2$. Donc par comparaison avec $\mathbb{1}$, on doit avoir $\sigma_c(2^\omega) \geqslant \sigma_c(\mathbb{1}) = 1$. D'autre part, comme $2^\omega = \mathbb{1} * \mu^2$, on a $\sigma_a(2^\omega) \leqslant \max(\sigma_a(\mu^2), \sigma_a(\mathbb{1}))$. Or $0 \leqslant \mu^2 \leqslant \mathbb{1}$, donc $\sigma_a(\mu^2) = \sigma_c(\mu^2) \leqslant \sigma_a(\mathbb{1}) = \sigma_c(\mathbb{1}) = 1$ et l'inégalité précédente devient $\sigma_c(2^\omega) = \sigma_a(2^\omega) \leqslant 1$. On en déduit que $\sigma_c(2^\omega) = 1$.
4. Comme 2^ω est multiplicative, pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > \sigma_a(2^\omega) = 1$, on a
$$\begin{aligned} D_{2^\omega}(s) &= \prod_p \left(1 + \sum_{k \geqslant 1} 2^\omega(p^k) p^{-ks}\right) = \prod_p \left(1 + 2\sum_{k \geqslant 1} p^{-ks}\right) \\ &= \prod_p \left(1 + 2\frac{p^{-s}}{1-p^{-s}}\right) = \prod_p \left(1 + \frac{2}{p^s - 1}\right) \\ &= \prod_p \frac{p^s + 1}{p^s - 1}. \end{aligned}$$
5. Pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$, on a
$$\zeta^2(s) = \prod_p (1 - p^{-s})^{-2}.$$
D'autre part, pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > \frac{1}{2}$, on a
$$\zeta(2s) = \prod_p (1 - p^{-2s})^{-1}.$$
Par conséquent, pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$, on a
$$\frac{\zeta^2(s)}{\zeta(2s)} = \prod_p \frac{1 - p^{-2s}}{(1 - p^{-s})^2} = \prod_p \frac{p^s + 1}{p^s - 1} = D_{2^\omega}(s).$$
6. L'identité $2^\omega = \mathbb{1} * \mu^2$ donne $2^\omega * \mu = \mu^2$, de sorte que $D_{\mu^2}(s) = D_{2^\omega}(s) D_\mu(s)$ pour tout $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1 = \sigma_a(2^\omega) = \sigma_a(\mu)$. Comme $D_\mu(s) = \frac{1}{\zeta(s)}$ pour $\mathrm{Re}(s) > 1$, cela donne $D_{\mu^2}(s) = \frac{\zeta(s)}{\zeta(2s)}$ pour $\mathrm{Re}(s) > 1$. La fonction ζ a un unique pôle simple de résidu 1 en $s = 1$, tandis que la fonction $\zeta(2s)$ n'a aucun zéro pour $\mathrm{Re}(s) > \frac{1}{2}$. Par conséquent, la fonction $D_{\mu^2}(s) - \frac{1}{\zeta(2)(s-1)}$ se prolonge continûment sur $\mathrm{Re}(s) \geqslant 1$. Par le théorème d'Ikehara, on en déduit que $M_{\mu^2}(x) \sim_{x \to +\infty} \frac{1}{\zeta(2)} x$.

Exercice 3 On note K le corps de nombres $\mathbb{Q}(\sqrt{-71})$.

1. Déterminer l'anneau $\mathcal{O}_K$ des entiers de K ainsi que le discriminant de K.

2. Déterminer l'ensemble des formes quadratiques binaires définies positives primitives et réduites de discriminant $D = -71$.
3. En déduire que le groupe des classes de $\mathcal{O}_K$ est un groupe cyclique dont on calculera le cardinal.
4. Quelle forme quadratique binaire définie positive primitive et réduite de discriminant $D = -71$ est associée à la classe des idéaux principaux de $\mathcal{O}_K$?

Corrigé :

1. Comme $-71 \equiv 1 \bmod 4$, par un résultat du cours on a $\mathcal{O}_K = \mathbb{Z}[\alpha]$ avec $\alpha = \frac{1+\sqrt{-71}}{2}$ et $\Delta_{\mathcal{O}_K/\mathbb{Z}} = -71$.
2. De telles formes quadratiques binaires $[a, b, c]$ satisfont $1 \leqslant |a| \leqslant \sqrt{\frac{71}{3}} < 5$ et $-a < b \leqslant a \leqslant c$, ainsi que $b \geqslant 0$ si $a = c$. De plus $D = b^2 - 4ac = -71$ de sorte que b est impair. Si $a = 1$, on a $-1 < b \leqslant 1$ de sorte que $b = 1$, donc $D = 1 - 4c = -71$ c'est-à-dire $c = 18$. On obtient $[1, 1, 18]$. Si $a = 2$, on a $-2 < b \leqslant 2$ de sorte que $b = \pm 1$, donc $D = 1 - 8c = -71$ c'est-à-dire $c = 9$. On obtient $[2, \pm 1, 9]$. Si $a = 3$, on a $-3 < b \leqslant 3$ de sorte que $b = \pm 1$ ou 3. Si $b = \pm 1$, alors $D = 1 - 12c = -71$ c'est-à-dire $c = 6$. On obtient $[3, \pm 1, 6]$. Si $b = 3$, alors $D = 9 - 12c = -71$ n'a pas de solution entière. Si $a = 4$, on a $-4 < b \leqslant 4$ de sorte que $b = \pm 1$ ou ± 3. Si $b = \pm 1$, alors $D = 1 - 16c = -71$ n'a pas de solution entière. Si $b = \pm 3$, alors $D = 9 - 16c = -71$ c'est-à-dire $c = 5$. On obtient $[4, \pm 3, 5]$.
3. Le groupe des classes $\mathrm{Cl}(\mathcal{O}_K)$ est en bijection avec l'ensemble des formes quadratiques binaires définies positives primitives et réduites de discriminant $D = -71$. Par conséquent, ce groupe est de cardinal 7. Comme 7 est premier, tout élément non trivial de ce groupe est d'ordre 7 donc engendre $\mathrm{Cl}(\mathcal{O}_K)$, qui est donc cyclique.
4. La norme d'un élément $x + y\alpha$ de $\mathcal{O}_K$, avec $x, y \in \mathbb{Z}$ est donnée par $N_{K/\mathbb{Q}}(x + y\alpha) = (x + \alpha y)(x + y\overline{\alpha}) = x^2 + xy + 18y^2$. Comme la norme de l'idéal principal $\mathcal{O}_K$ est 1, il s'agit de la forme quadratique $[1, 1, 18]$ trouvée au point 2, et qui correspond donc au neutre dans $\mathrm{Cl}(\mathcal{O}_K)$.