MM120 Théorie des nombres — Loïc Merel
Année 2012-2013 — Dominique Bernardi, Pierre Charollois

**Feuille 1**

## Entiers

**Exercice 1** Montrer que, dans un corps de nombres $K$ de degré $n$, tout idéal (entier) non nul contient une infinité d'entiers naturels mais que, si $b$ est un entier naturel non nul, il n'est pas contenu dans plus de $b^n$ idéaux entiers.

**Exercice 2** Soit $K$ un corps de nombres de degré $n$ et $p$ un nombre premier totalement décomposé dans $K$. Montrer que si $p < n$, l'anneau des entiers $\mathbb{Z}_K$ ne peut pas s'écrire sous la forme $\mathbb{Z}[\alpha]$. Montrer que le polynôme $X^3 - X + 8$ fournit un exemple d'une telle situation.

**Exercice 3** Soit $m$ un entier naturel sans facteur cubique. On peut écrire de façon unique $m = ab^2$, où $a$ et $b$ sont des entiers naturels sans facteur carré. On note $\theta = \sqrt[3]{m}$, $K = \mathbb{Q}(\theta)$ et $d$ le discriminant de $\mathbb{Z}[\theta]$.

a) Calculer $d$. Montrer que si $x + y\theta$ est un entier de $K$, avec $x$ et $y$ dans $\mathbb{Q}$, alors $x$ et $y$ sont dans $\mathbb{Z}$.

b) Montrer que si $\alpha = x + y\theta + z\theta^2$ est un entier de $K$, avec $x$, $y$ et $z$ dans $\mathbb{Q}$, alors $3x$, $3y$ et $3bz$ sont dans $\mathbb{Z}$. On pourra calculer le polynôme caractéristique de $\alpha$ et montrer successivement que $3x$, $3my$, $3mz$, $3by$, $3bz$ et $3y$ sont dans $\mathbb{Z}$.

c) Montrer que si $m \not\equiv \pm 1 \pmod 9$, on a même $x$, $y$ et $bz$ dans $\mathbb{Z}$. On pourra considérer séparément les cas où $3|m$.

d) Montrer que $\theta^2/b$ est entier, et que si $m \equiv \epsilon = \pm 1 \pmod 9$, $(1 + \epsilon\theta + \theta^2)/3$ est entier.

e) Dans tous les cas, donner une base des entiers de $K$, et son discriminant.

**Exercice 4 Critère de Dedekind.** Soit $h \in \mathbb{Z}[X]$ un polynôme unitaire irréductible de degré $n$, $\theta$ une racine de $h$ et $K = \mathbb{Q}(\theta)$. Soit $p$ un nombre premier. La réduction modulo $p$ de $h$ se décompose en facteurs irréductibles dans $\mathbb{F}_p[X]$ sous la forme $\overline{h} = \prod_i \overline{h_i}^{e_i}$. On note $h_i$ un relèvement unitaire de $\overline{h_i}$ dans $\mathbb{Z}[X]$, $T = \prod_i h_i$ et $L = \prod_i h_i^{e_i - 1}$. Il existe donc un polynôme $g \in \mathbb{Z}[X]$ tel que $h = TL + pg$. On définit le $p$-radical de $\mathbb{Z}[\theta]$ :

$$R_p = \{\alpha \in \mathbb{Z}[\theta]; \exists k \geq 0,\ \alpha^k \in p\mathbb{Z}[\theta]\}$$

a) Montrer que

$$\alpha \in R_p \Leftrightarrow \exists A, U, V \in \mathbb{Z}[X]; A = TU + pV \text{ et } \alpha = A(\theta)$$

b) On suppose que $p$ divise $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Montrer qu'il existe $a \in \mathbb{Z}_K$ tel que $a \notin \mathbb{Z}[\theta]$ et $pa \in \mathbb{Z}[\theta]$. Montrer qu'il existe $b \in \mathbb{Z}_K$ tel que $b \notin \mathbb{Z}[\theta]$, $pb \in \mathbb{Z}[\theta]$ et $T(\theta)b \in \mathbb{Z}[\theta]$.

c) Montrer que sous les hypothèses de b), on a $pb \in R_p$ et $T(\theta)b \in R_p$.

d) On suppose maintenant que $\overline{g}$ et $\overline{L}$ sont premiers entre eux. Montrer que, pour $b \in \mathbb{Z}_K$, les conditions $pb \in R_p$ et $T(\theta)b \in R_p$ impliquent $b \in \mathbb{Z}[\theta]$.

e) On suppose $e_1 \geq 2$ et $\overline{h_1}$ divise $\overline{g}$. Posons $R = h_1^{e_1-1} \prod_{i \neq 1} h_i^{e_i}$. Montrer que $\alpha = R(\theta)/p$ est un entier algébrique. En déduire le critère de Dedekind : $\overline{g}$ est premier à $\overline{L}$ si et seulement si $p$ ne divise pas l'indice $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. On dit dans ce cas que $\mathbb{Z}[\theta]$ est un ordre $p$-maximal.

f) Montrer que si $\mathbb{Z}[\theta]$ est $p$-maximal, la décomposition de $p$ dans $K$ est

$$p\mathbb{Z}_K = \prod_i \mathfrak{p}_i^{e_i}$$

où $\mathfrak{p}_i = p\mathbb{Z}_K + h_i(\theta)\mathbb{Z}_K$, et les $\mathfrak{p}_i$ sont des idéaux premiers distincts.

g) Montrer que le critère d'Eisenstein est un cas particulier du critère de Dedekind.

**Exercice 5** On considère le corps $K = \mathbb{Q}(\sqrt{-43})$. On pose $\omega = \frac{-1+\sqrt{-43}}{2}$, et on rappelle que l'anneau des entiers de $K$ admet $\{1, \omega\}$ comme base sur $\mathbb{Z}$.

a) Calculer le polynôme minimal de $\omega$. Montrer que 2 et 3 sont inertes dans $K$.

b) Calculer la constante de Minkowski de $K$. Montrer que $\mathcal{O}$ est principal.

c) Soit $\alpha \notin \mathbb{Z}$ un élément de $\mathcal{O}$ qui engendre un idéal premier. Montrer que $N_{L/\mathbb{Q}}(\alpha)$ est un nombre premier.

d) Soit $x$ et $y \neq 0$ deux entiers premiers entre eux tels que $x^2 + xy + 11y^2$ soit strictement inférieur à 121. Montrer que $x^2 + xy + 11y^2$ est un nombre premier.

## Unités

**Exercice 6** Montrer que les unités des corps quadratiques réels forment un sous-ensemble $U$ discret de $\mathbb{R}^*$. Quel est la plus petite unité fondamentale ? Expliciter $U \cap [1, 10]$.

**Exercice 7** Montrer que, si $\varepsilon \in \mathbb{Q}(\sqrt{d})$ est une unité de norme 1 d'un corps quadratique, il existe un entier $\gamma$ tel que $\varepsilon = \frac{\gamma}{\gamma'}$, où $\gamma'$ est le conjugué de $\gamma$.

**Exercice 8 Équations de Pell-Fermat** On rappelle que pour un corps quadratique réel $K$, le théorème de Dirichler affirme l'existence d'une *unité fondamentale*, plus petit entier $\varepsilon > 1$ de $K$ tel $N_{K\mathbb{Q}}\varepsilon = \pm 1$.

a) Soit $d > 1$ un entier sans facteur carré congru à 2 ou 3 (mod 4). Montrer que l'équation $x^2 - dy^2 = 1$ a une infinité de solutions entières.

b) Montrer qu'il en est de même si $d \equiv 1 \bmod 4$.

c) Montrer qu'on peut remplacer l'hypothèse "$d > 1$ sans facteur carré" par "$d > 0$ n'est pas un carré".

d) Soit $d$ un entier naturel qui n'est pas un carré, et $k$ un entier relatif. Montrer que si l'équation $x^2 - dy^2 = k$ a une solution en entiers, elle en a une infinité. Que se passe-t'il si $d$ est un carré, ou si $d < 0$ ?

e) Montrer que l'unité fondamentale de $\mathbb{Q}(\sqrt{2})$ est $1 + \sqrt{2}$.

f) Décrire toutes les solution entières de l'équation

$$x^2 - 50y^2 = 41.$$

## Groupes des classes

**Exercice 9** Dans le corps $K = \mathbb{Q}(\sqrt{-47}$, on note $\omega = (1+\sqrt{-47})/2$ et $\mathfrak{O} = \mathbb{Z}[\omega]$ l'anneau des entiers. On se propose d'étudier le groupe $C$ des classes d'ideaux fractionnaires de $K$.

a) Montrer que si $\mathfrak{p}$ est l'idéal engendré par 2 et $\omega$, $\mathfrak{p}$ est un idéal de norme 2 distinct de son conjugué $\overline{\mathfrak{p}}$ et que l'on a $2\mathfrak{O} = \mathfrak{p}\overline{\mathfrak{p}}$.

b) Montrer que si $A$ est la norme d'un idéal entier principal $\mathfrak{a}$, alors l'équation

$$x^2 + 47y^2 = 4A$$

admet une solution dans $\mathbb{Z}^2$. Montrer que $\mathfrak{p}$, $\mathfrak{p}^2$, $\mathfrak{p}^3$ et $\mathfrak{p}^4$ ne sont pas principaux.

c) Montrer qu'il existe deux idéaux principaux de norme 32. Donner la liste des idéaux entiers de norme 32 et montrer que $\mathfrak{p}^5$ est principal.

d) Montrer qu'il y a au plus huit idéaux entiers de norme inférieure ou égale à 4. À l'aide du théorème de Minkowski, montrer que $C$ est cyclique d'ordre 5.

e) Montrer que l'idéal $\mathfrak{q}$ engendré par 3 et $\omega$ est de norme 3. Pour quelles valeurs de $n$ l'idéal $\mathfrak{p}^n\mathfrak{q}$ est-il principal ?

**Exercice 10** Soit $K = \mathbb{Q}(\sqrt{-23})$ et $\alpha = \frac{1+\sqrt{-23}}{2}$.

a) Calculer le polynôme minimal de $\alpha$, le discriminant $D_K$ de $K$ et la constante de Minkowski $M_K$ de $K$.

b) Montrer que les idéaux $\mathfrak{p} = (2, \alpha)$ et $\mathfrak{q} = (3, \alpha)$ sont premiers non principaux.

c) Donner la factorisation de $2\mathcal{O}_K$ et $3\mathcal{O}_K$ en produit d'idéaux premiers.

d) Montrer que $\mathfrak{p}^3$ est principal.

e) Calculer le nombre de classes $h_K$. On pourra commencer par montrer que $h_K$ est inférieur ou égal à 5.

**Exercice 11** On note $\zeta = e^{\frac{2i\pi}{23}}$ et $L = \mathbb{Q}(\zeta)$. On rappelle que le degré de $L$ sur $\mathbb{Q}$ est 22. On veut montrer que l'anneau $\mathcal{O}$ des entiers de $L$ n'est pas principal.

a) Montrer que $2^{23}-1$ est divisible par 47 mais pas pas $47^2$. Calculer $N_{L/\mathbb{Q}}(\zeta-2)$.

b) Notons $\mathfrak{a}$ l'idéal de $\mathcal{O}$ engendré par 47 et $\zeta-2$. Montrer que, pour tout élément $\beta$ de $\mathfrak{a}$, 47 divise $N_{L/\mathbb{Q}}(\beta)$.

c) On suppose que $\mathfrak{a}$ est principal, engendré par $\alpha$. Montrer que la norme $N(\alpha)$ divise $47^{22}$ et $N(\zeta - 2)$. Calculer $N(\alpha)$.

d) Montrer que $L$ contient un corps $K$ quadratique sur $\mathbb{Q}$ et un seul.

e) Posons $\omega = N_{L/K}(\alpha)$. Montrer que $\omega$ est un entier de $K$ de norme 47.

f) On sait, grâce à une formule de Gauß, que $K = \mathbb{Q}(\sqrt{-23})$. Montrer que $K$ ne contient pas d'entier de norme 47, et conclure.

**Solution 1** Tout idéal entier non nul $\mathfrak{a}$ contient sa norme, qui est un entier naturel non nul. Il contient aussi tous les multiples de cette norme, qui sont en nombre infini. Inversement, tout idéal qui contient $b$ est engendré par $b$ et un autre entier, disons $x$. Exprimons $x$ dans une base d'entiers, et réduisons ses composantes modulo $b$. Le nombre de valeurs possibles de $x$ est inférieur ou égal à $b^n$, d'où le résultat. Il est facile de voir que, même pour $n = 1$, cette majoration est grossière.

**Solution 2** Supposons $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. Soit $f$ je polynôme minimal de $\alpha$. La réduction $\overline{f}$ de $f$ modulo $p$ doit être un produit de $n$ facteurs irréductibles unitaires de degré 1 distincts, soit $\overline{f} = \prod_{i=1}^{n}(X - \lambda_i)$. Les $\lambda_i$ sont $n$ éléments distincts de $\mathbb{F}_p$, donc $p \geq n$.

Le polynôme $P = X^3 - X + 8$ est irréductible puisqu'il l'est modulo 3. On a $P(0) = P(-1) = P(1) = 8$ et $P'(0) = -1$, $P'(1) = P'(-1) = 2$. Le lemme de Hensel montre que $P$ a trois racines distinctes dans $\mathbb{Q}_2$, l'une congrue à 0 (mod 8), les deux autres congrues à $-1$ et 1 respectivement (mod 4). On a donc $\mathbb{Q}_2 \otimes K \simeq \mathbb{Q}_2^3$ et 2 est totalement décomposé dans $K$. On peut appliquer la première partie pour $p = 2$ et $n = 3$. Plus précisément, si $\alpha$ est un entier du corps $K$ engendré par une racine de $P$, l'indice $[\mathbb{Z}_K : \mathbb{Z}[\alpha]]$ est forcément pair.

**Solution 3**

a) On peut appliquer la formule valable pour les trinômes, donc *a fortiori* pour les binômes :

$$d = (-1)^{\frac{3.2}{2}} 3^3 . d^2 = -27d^2.$$

Le polynôme caractéristique de $\theta$ est $X^3 - m$, donc celui de $x + y\theta$ est

$$y^3 \left( \left( \frac{X - x}{y} \right)^3 - m \right) = (X - x)^3 - my^3 = X^3 - 3xX^2 + 3x^2X + x^3 - my^3.$$

On en déduit que $3x^2$ est entier, donc le dénominateur de $x$ ne peut être divisible par aucun nombre premier, c'est-à-dire que $x$ est entier. Donc $my^3$ est aussi entier, et le dénominateur de $y$ est lui aussi égal à 1 puisque $m$ est sans facteur cubique.

b) Dans le cas général, on peut écrire la matrice $M$ de la multiplication par $\alpha$ dans la base $\{1, \theta, \theta^2\}$ :

$$M = \begin{pmatrix} x & mz & my \\ y & x & mz \\ z & y & x \end{pmatrix}$$

dont le déterminant est $x^3 + my^3 + m^2z^3 - 3mxyz$. Pour obtenir le polynôme caractéristique de $\alpha$, il suffit de remplacer $x$ par $x - X$ dans cette expression. On trouve donc que $\alpha$ est entier si et seulement si les trois quantités suivantes sont dans $\mathbb{Z}$ :

$$\begin{cases} 3x \\ 3x^2 - 3myz \\ x^3 + my^3 + m^2z^3 - 3mxyz \end{cases}.$$

La première condition appliquée à $\alpha$, $\alpha\theta$ et $\alpha\theta^2$ respectivement implique que $3x$, $3mz$ et $3my$ sont dans $\mathbb{Z}$. En multipliant la dernière condition par $3^3m$, tous les termes sont entiers sauf peut-être $3^3m^2y^3 = a^2b(3by)^3$, ce qui montre encore que le dénominateur de $3by$ est 1. On recommence en multipliant seulement par $3^3b$. Tous les termes sont entiers sauf peut-être $3^3b^3m^2z^3 = a^2b^2(3bz)^3$, donc $3bz$ est dans $\mathbb{Z}$. Enfin, en multipliant seulement par $3^3$, tous les termes sont entiers sauf peut-être $3^3my^3 = ab^2(3y)^3$, donc $3y \in \mathbb{Z}$.

c) Notons donc $x' = 3x$, $y' = 3y$ et $z' = 3bz$. Ce sont des entiers relatifs, et on doit avoir $x'^2 - 3aby'z' \equiv 0 \pmod 3$ et $x'^3 + ab^2y'^3 + a^2bz'^3 - 3abx'y'z' \equiv 0 \pmod{27}$. Supposant d'abord $3|ab$, on déduit immédiatement de la première condition que $3|x'$, puis de la seconde que $27|ab^2y'^3 + a^2bz'^3$, donc $3|y'$ puis $3|z'$ si $3|a$ (dans l'ordre inverse si $3|b$. Restent les cas $m \equiv \pm 2, \pm 4 \pmod 9$. Si l'une des trois quantités $x'$, $y'$ et $z'$ est divisible par 3, la première condition donne que deux d'entre elles le sont, la deuxième donne alors qu'elle le sont toutes trois. On peut essayer toutes les possibilités restantes (mod 9) pour $x'$, $y'$ et $z'$, et le mieux est de le faire faire par une machine... On trouve encore que 3 doit diviser $x'$, $y'$ et $z'$.

d) $\theta^2/b$ est racine du polynôme $X^3 - a^2b$, et donc entier. Avec les notations précédentes, on a $x' = 1$, $y' = \epsilon$ et $z' = b$. La première condition devient $|1 - m\epsilon \equiv 1 - \epsilon^2 \equiv 0$, ce qui est trivial. Pour la deuxième, on calcule $1 + m\epsilon + m^2 - 3m\epsilon = (\epsilon - m)^2 \equiv 0 \pmod{27}$.

e) Dans tous les cas, le réseau $\Lambda$ de base $\{1, \theta, \theta^2/b\}$ est inclus dans l'anneau des entiers. Son discriminant est $-3^3ab$ puisque $\mathbb{Z}[\theta]$ en est un sous-groupe d'indice $b$. On a vu au c) que si $m \not\equiv \pm 1 \pmod 9$, c'était l'anneau des entiers de $K$. Dans le cas $m \not\equiv \pm 1$, la question b) montre seulement que $3\mathfrak{O}_K \subset \Lambda$. Le groupe $\Lambda'$ engendré par $\Lambda$ et $(1 + \epsilon\theta + \theta^2)/3$ est inclus dans $\mathfrak{O}_K$. Son discriminant est $-3ab$, et n'est pas divisible par 9. On en déduit que dans ce cas, $\mathfrak{O}_K = \Lambda'$.

**Solution 4**

a) On peut toujours écrire $\alpha = A(\theta)$ avec $A \in \mathbb{Z}[X]$. La condition est alors $A^k = pB + fC$, qui implique $\overline{A}^k = \overline{hC}$. La décomposition en facteurs irréductibles dans $\mathbb{F}_p[X]$ donne $\overline{T}$ divise $\overline{A}$ ce qui revient à la condition de l'énoncé. Réciproquement, si $\overline{T}$ divise $\overline{A}$, il est clair que $\overline{h}$ divise $\overline{A}^n$.

b) Si l'ordre du groupe $\mathbb{Z}_K/\mathbb{Z}[\theta]$ est divisible par $p$, il y a un élément $a$ d'ordre $p$. Comme $a \notin \mathbb{Z}[\theta]$ et $T(\theta)^n a \in \mathbb{Z}[\theta]$, il existe un entier $k < n$ tel que $b = T(\theta)^k a$ vérifie les conditions énoncées.

c) Posons $d = v_p([\mathbb{Z}_K : \mathbb{Z}[\theta]]$. L'ordre de $b^k$ dans $\mathbb{Z}_K/\mathbb{Z}[\theta]$ est un diviseur commun de $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ et $p^k$, donc on a en fait $p^d b^k \in \mathbb{Z}[\theta]$. Il suffit de prendre $k > d$ pour avoir $(pb)^k \in p\mathbb{Z}[\theta]$, donc $pb \in R_p$. De même, on a $T(\theta)^{(d+1)n} \in p^{d+1}\mathbb{Z}[\theta]$, donc pour $k \geq (d+1)n$ on a $(T(\theta)b)^k \in p\mathbb{Z}[\theta]$, donc $T(\theta)b \in R_p$.

d) Il existe donc des polynômes $U, V, R, S \in \mathbb{Z}[X]$ tels que

$$pb = T(\theta)U(\theta) + pV(\theta),$$
$$T(\theta)b = T(\theta)R(\theta) + pS(\theta).$$

En multipliant la première équation par $T(\theta)$ et la deuxième par $p$, on obtient deux polynômes en $\theta$ qui prennent la même valeur, et diffèrent donc par un multiple de $h = TL + pg$. Il existe donc un polynôme $Z \in \mathbb{Z}[X]$ tel que

$$T^2U + pTV = pTR + p^2S + (TL + pg)Z.$$

En réduisant modulo $T$, on trouve que $T$ divise $p^2S + pgZ$ (dans $\mathbb{Z}[X]$), donc $T$ divise $pS + gZ$ et $\overline{T}$ divise $\overline{g}\,\overline{Z}$, donc si $e_i > 1$, $\overline{h_i}$ divise aussi $\overline{Z}$ puisque $\overline{g}$ et $\overline{L}$ sont premiers entre eux. En réduisant modulo $p$, on trouve $\overline{TU} = \overline{LZ}$. Ce qui précède montre que le second membre est divisible par $\overline{h_i}^{e_i}$ si $e_i > 1$. Le premier membre est divisible par $\overline{h_i}^{e_i}$ si $e_i = 1$. On en conclut que $\overline{h}$ divise $\overline{TU}$, donc $pb \in p\mathbb{Z}[\theta]$ et $b \in \mathbb{Z}[\theta]$.

e) Il existe deux polynômes $U$ et $V$ dans $\mathbb{Z}[X]$ tels que $g = h_1U + pV$. Posons encore $S = h_1^{e_1-2} \prod_{i\neq 1} h_i^{e_i}$, de sorte que $R = h_1S$ et

$$R^2 = h_1RS = TLS = (h - pg)S = hS - pRU - p^2VS.$$

On a donc

$$R(\theta)^2 + pR(\theta)U(\theta) + p^2V(\theta)S(\theta) = 0$$

et $\alpha^2 + U(\theta)\alpha + V(\theta)S(\theta) = 0$, c'est à dire que $\alpha$ est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}[\theta]$, donc $\alpha \in \mathbb{Z}_K$. Les coefficients de $p\alpha$ dans la base des puissances de $\theta$ sont ceux du polynôme unitaire $R \in \mathbb{Z}[X]$, il est donc clair que $p\alpha \in \mathbb{Z}[\theta]$ et $\alpha \notin \mathbb{Z}[\theta]$, donc $p$ divise $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Les deux conditions : $\mathbb{Z}[\theta]$ $p$-maximal et $\overline{g}$ premier à $\overline{L}$ sont donc équivalentes.

f) L'application naturelle $\mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \to \mathbb{Z}_K/p\mathbb{Z}_K$ est, d'après ce qui précède un isomorphisme de groupes additifs. Or c'est un morphisme d'anneaux. C'est donc un isomorphisme d'anneaux. Le premier membre se décompose naturellement en $\prod_i \mathbb{Z}[X]/(\overline{h_i}^{e_i})$ dont les idéaux premiers sont engendrés par les $\overline{h_i}$. On en déduit que les idéaux premiers de $\mathbb{Z}_K/p\mathbb{Z}_K$ sont engendrés par les $h_i(\theta)$ et les idéaux premiers de $K$ au dessus de $p$ sont engendrés par $h_i(\theta)$ et $p$. Le degré résiduel est donné par

$$f_i = [\mathbb{Z}_K/\mathfrak{p}_i : \mathbb{F}_p] = [\mathbb{F}_p[X]/(\overline{h_i}) : \mathbb{F}_p] = \deg \overline{h_i}.$$

g) Sous les hypothèses du critère d'Eisenstein, on a $\overline{h} = X^n$ et $g = (h - X^n)/p$. Le coefficient constant de $g$ est $a_0/p$ qui n'est pas nul modulo $p$. On a bien $\overline{g}$ et $X^{n-1}$ premiers entre eux : $\mathbb{Z}[\theta]$ est $p$-maximal et il y a un seul idéal premier au dessus de $p$, qui est engendré par $p$ et $\theta$. le degré résiduel est 1 et le degré de ramification est $n$.

**Solution 5**

a) On a $Tr(\omega) = \omega + \omega' = -1$ et $N(\omega) = \omega\omega' = 11$. Le polynôme minimal de $\omega$ est donc $X^2 + X + 11$. Modulo 2 ou 3, ce polynôme est irréductible. La première proposition permet de conclure : 2 et 3 sont encore premiers dans $K$.

b) Ici, $n = 2$, $t = 1$ et $D_K = 43$. La formule donne donc

$$M_K = \frac{4}{\pi}\frac{2}{4}\sqrt{43} = \frac{2\sqrt{43}}{\pi} < 5.$$

On vient de voir qu'il n'y a pas d'idéal de norme 2 ou 3, et que le seul idéal entier de norme 4 est $2\mathcal{O}$, qui est principal. Le théorème de Minkowski permet donc de conclure que $K$ est principal.

c) La norme d'un idéal premier d'un corps quadratique est soit un nombre premier ramifié ou décomposé, soit le carré $p^2$ d'un nombre premier inerte $p$. Mais dans ce dernier cas, l'idéal en question est forcément $p\mathcal{O}$. Si $\alpha\mathcal{O}$ et $p\mathcal{O}$ sont égaux, $\alpha/p$ est une unité de $\mathcal{O}$. Or, les seules unités de $\mathcal{O}$ sont 1 et $-1$. Cela contredirait l'hypothèse selon laquelle $\alpha$ n'appartient pas à $\mathbb{Z}$.

d) La norme d'un entier de $K$ qui n'est pas dans $\mathbb{Z}$ vaut $\frac{u^2+43v^2}{4} \geq \frac{43}{4}$, et comme c'est un entier, elle vaut au moins 11. Considérons l'entier $\alpha = x + y\omega$. Il n'appartient pas à $\mathbb{Z}$ puisque $y \neq 0$. Sa norme vaut $\alpha\alpha' = x^2 + xy + 11y^2 < 121$. Si ce n'était pas un nombre premier, il y aurait un diviseur premier de $\alpha$ de norme inférieure à 11, et, d'après ce qui précède, son générateur $a$ serait dans $\mathbb{Z}$. Mais si un entier rationnel $a$ divise $\alpha$, il divise $x$ et $y$, une contradiction.

On en déduit en particulier que $x^2 + x + 11$ est un nombre premier pour $x$ compris entre 0 et 9. Le même raisonnement avec $\mathbb{Q}(\sqrt{-163})$ montre que $x^2 + x + 41$ est premier pour $x$ allant de 0 à 39.

**Solution 6** Si $\varepsilon = \frac{a+b\sqrt{d}}{2}$ est une unité, on a

$$\{\pm\varepsilon, \pm\varepsilon^{-1}\} = \{\frac{\pm a \pm b\sqrt{d}}{2}\}.$$

On en déduit que $\varepsilon > 1 \Leftrightarrow a, b \geq 0$. Si de plus $\varepsilon < M$, on a $\frac{\pm a \pm b\sqrt{d}}{2}$

**Solution 7** Soit $\alpha$ un entier quelconque de $K$. On pose $\gamma = \alpha + \alpha'\varepsilon$. On a $\varepsilon\gamma' = \varepsilon(\alpha' + \alpha\varepsilon') = \gamma$. Pour conclure, il reste à prouver que l'on peut choisir $\alpha$ de façon à ce que $\gamma$ ne soit pas nul. Si $\varepsilon \neq -1$, on peut prendre $\alpha = 1$, sinon on prend $\alpha = \sqrt{d}$.

**Solution 8**

a) Dans ce cas, les entiers de $K$ s'écrivent $x+y\sqrt{d}$ et la norme d'un tel entier vaut $x^2-dy^2$. La norme d'une unité vaut 1 ou -1. Si la norme de l'unité fondamentale vaut 1, il y a donc une solution par unité de $K$. Dans le cas contraire, les unités de norme 1 forment un sous-groupe d'indice 2 du groupe des unités, mais il est quand même infini.

b) Le problème est ici que l'unité fondamentale pourrait être du type $\varepsilon = \frac{a+b\sqrt{d}}{2}$, avec $a$ et $b$ impairs. Dans ce cas, on a $a^2 - db^2 = \pm 4$. Or, $a$ et $b$ étant impairs, $a^2$ et $b^2$ sont congrus à 1 modulo 8. Si $d \equiv 1 \pmod 8$, il y a une contradiction :

l'unité fondamentale est forcément de la forme $a+b\sqrt{d}$, et le raisonement du a) est encore valable. Si, au contraire, $d \equiv 5 \pmod 8$, on calcule

$$\varepsilon^2 = \frac{(a^2-db^2)/2+ab\sqrt{d}}{2}, \quad \varepsilon^3 = a(a^2+3db^2)/8 + b(3a^2+db^2)/8.$$

On en déduit que $\varepsilon^2$ n'appartient pas à $\mathbb{Z}[\sqrt{d}]$ et que $\varepsilon^3$ lui appartient. On peut donc appliquer le même raisonnement à $\varepsilon^3$ au lieu de $\varepsilon$.

c) Si $d > 0$ n'est pas un carré, on peut écrire $d = d'f^2$, où $d' > 1$ est sans facteur carré. Si $\varepsilon > 1$ est un élément de norme 1 de $\mathbb{Z}[\sqrt{d'}]$ (dont l'existence est une conséquence des questions a) et b)), il s'agit de montrer qu'il existe un entier $r \geq 1$ tel que $\varepsilon^r \in \mathbb{Z}[\sqrt{d}] = \mathbb{Z}[f\sqrt{d'}]$. Pour cela, considérons le groupe $(\mathbb{Z}[\sqrt{d}]/f)^\times$ des éléments inversibles de $\mathbb{Z}[\sqrt{d}]/f$. L'image de $\varepsilon$ modulo $f$ est un élément de ce groupe fini : l'ordre $r$ de cet élément est donc fini, ce qui donne bien la condition cherchée.

d) Pour chacun des éléments $\eta = a+b\sqrt{d}$ (en nombre infini d'après les questions précédentes) de norme 1 dans $\mathbb{Z}[\sqrt{d}]$, on peut prendre le produit $\eta(x+y\sqrt{d})$ pour obtenir un nouvel élément de norme $k$. Il y a donc une infinité d'éléments de norme $k$ dans $\mathbb{Z}[\sqrt{d}]$.

e) Soient $a$ et $b$ deux entiers naturels tels que $a^2-2b^2 = \pm 1$. Si $b > 0$, posons $a'+b'\sqrt{2} = (a+b\sqrt{2})/(1+\sqrt{2}) = (2b-a)+(a-b)\sqrt{2}$, c'est-à-dire que $a' = 2b-a$ et $b' = a-b$. On voit que $a'$ et $b'$ sont encore des entiers naturels. On peut donc recommencer l'opération jusqu'à obtenir, au bout de $m$ pas, $b = 0$ et $a = 1$. En d'autres termes, $a+b\sqrt{2} = (1+\sqrt{2})^m$. Toutes les unités $a+b\sqrt{2}$ avec $a$ et $b$ positifs sont donc des puissances positives de $1+\sqrt{2}$. Si $b$ est négatif on trouve par conjugaison une puissance négative. Enfin, si $a$ est négatif, il faut prendre l'opposé. Toutes les unités sont donc au signe près des puissances de $1+\sqrt{2}$ qui est donc l'unité fondamentale $\varepsilon$.

f) Les unités de $\mathbb{Z}[\sqrt{50}]$ sont au signe près des puissances de $\varepsilon^3 = 7+5\sqrt{2} = 7+\sqrt{50}$ qui est de norme -1. La solution "évidente" $3^2-50 = -41$ doit être multipliée par $\varepsilon^3$ pour obtenir la plus petite solution $(71, 10)$. Toutes les autres s'obtiennent en mulipliant par des puissances de $\varepsilon^6 = 99+14\sqrt{50}$. On pose $u_0 = 71$, $v_0 = 10$, $u_{n+1} = 99u_n + 700v_n$ et $v_{n+1} = 99v_n + 14u_n$ pour trouver tous les couples de solutions positives $(u_n, v_n)$ de l'équation proposée. Ici, il n'y a qu'une solution de base, mais dans d'autre cas il pourrait y en avoir plusieurs.

**Solution 9** Le polynôme minimal de $\omega$ est $f = X^2 - X + 12$.

a) Modulo 2, on a $f \equiv X(X+1)$. On peut donc appliquer la proposition 7 : 2 se décompose en deux facteurs, dont l'un, noté $\mathfrak{p}$, est engendré par 2 et $\omega$.

b) Supposons $\mathfrak{a}$ principal, engendré par l'entier $\alpha = a+b\omega$. la norme $A$ de $\mathfrak{a}$ est la valeur absolue de celle de $\alpha$, soit $A = (a+b\omega)(a+b\overline{\omega}) = a^2+ab+12b^2$, donc $4A = (2a+b)^2+47b^2$, d'où le résultat en posant $x = 2a+b$ et $y = b$. Il est facile de voir que les équations $x^2+47y^2 = m$ n'ont pas de solution entière pour $m = 8$ ou $m = 32$, donc $\mathfrak{p}$ et $\mathfrak{p}^3$ ne sont pas principaux, et que les

seules solutions pour $m = 16$ ou $m = 64$ sont données par $x = \pm 4, y = 0$ et $x = \pm 8, y = 0$ respectivement, correspondant aux idéaux 2 et 4, donc $\mathfrak{p}^2$ et $\mathfrak{p}^4$ ne sont pas principaux.

c) Pour $m = 128$, on trouve les solutions $x = \pm 9, y = \pm 1$, qui correspondent a deux idéaux principaux entiers de norme 32. Les idéaux entiers de norme 32 sont $\mathfrak{p}^5$, $2\mathfrak{p}^3$, $4\mathfrak{p}$, $4\overline{\mathfrak{p}}$, $2\overline{\mathfrak{p}}^3$ et $\overline{\mathfrak{p}}^5$. Seuls les deux extrêmes peuvent être principaux : ils le sont donc.

d) Modulo 3, on a aussi $f \equiv X(X+1)$, donc on peut appliquer la proposition 7 : 3 se décompose en deux facteurs, dont l'un, noté $\mathfrak{q}$, est engendré par 3 et $\omega$. La liste complète des idéaux entiers de norme au plus 4 est donc la suivante : $\{1, \mathfrak{p}, \overline{\mathfrak{p}}, \mathfrak{q}, \overline{\mathfrak{q}}, \mathfrak{p}^2, \overline{\mathfrak{p}}^2, 2\}$. La constante de Minkowski du corps est $2/\pi\sqrt{47} \approx 4.364445271138074545056000371 < 5$. On déduit du théorème 5 que le nombre de classes de $K$ est inférieur ou égal à 8. Comme la classe $\mathfrak{p}$ est d'ordre 5 dans ce groupe, $C$ est cyclique d'ordre 5.

e) L'élément $\omega$ est de norme 12, et il est contenu dans $\mathfrak{p}$ et $\mathfrak{q}$. L'idéal engendré par $\omega$ est donc $\mathfrak{p}^2\mathfrak{q}$ ou bien $2\mathfrak{q}$. Comme $\mathfrak{q}$ n'est pas principal ($x^2 + 47y^2 = 12$ n'a pas de solution entière), c'est $\mathfrak{p}^2\mathfrak{q}$. De la structure de groupe, on tire immédiatement que $\mathfrak{p}^n\mathfrak{q}$ est principal si et seulement si $n \equiv 2 \pmod 5$.

**Solution 10**

a) La trace et la norme de $\alpha$ valent respectivement 1 et 6. Le polynôme minimal de $\alpha$ est donc $P = X^2 - X + 6$. Le discriminant de $K$ est celui de $\mathbb{Z}[\alpha]$ ou encore celui du polynôme, c'est-à-dire $-23$. La constante de Minkowski vaut

$$M_K = \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2}\sqrt{23} \approx 3.05.$$

b) et c) Comme il résulte de la proposition 7 du cours, la décomposition dans $K$ de 2 et de 3 reflète celle du polynôme $P$ modulo 2 ou 3. On a $P \equiv X(X-1) \pmod 2$ et $\pmod 3$, donc les idéaux $\mathfrak{p} = (2, \alpha)$, $\mathfrak{p}' = (2, \alpha - 1)$, $\mathfrak{q} = (3, \alpha)$, $\mathfrak{q}' = (3, \alpha - 1)$ sont premiers de norme respective 2, 2, 3 et 3, et l'on a $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ et $3\mathcal{O}_K = \mathfrak{q}\mathfrak{q}'$. Si $\mathfrak{p}$ (resp. $\mathfrak{q}$) était premier, il serait engendré par un entier de norme 2 (resp. 3). Il existerait donc une solution $(a, b)$ entière à l'équation $a^2 + 23b^2 = 8$ (resp. $a^2 + 23b^2 = 12$), ce qui n'est pas le cas.

d) L'équation $a^2 + 23b^2 = 32$ a pour solutions entières $(\pm 3, \pm 1)$. On en déduit que $\alpha + 1$ et $2 - \alpha$ engendrent les seuls idéaux principaux de norme 8. Or les idéaux de norme 8 sont $\mathfrak{p}^3$, $\mathfrak{p}'^3$, $2\mathfrak{p}$, $2\mathfrak{p}'$, et seuls les deux premiers peuvent être principaux. Reste à voir que $2 - \alpha$ appartient à $\mathfrak{p}$ pour en déduire

$$\mathfrak{p}^3 = (2 - \alpha)\mathcal{O}_K.$$

e) Toute classe d'idéaux contient un idéal entier de norme inférieure ou égale à 3. Il y a exactement 5 tels idéaux : 1, $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{q}$ et $\mathfrak{q}'$. Le nombre de classes $h_K$ vaut donc au plus 5. Mais la question précédente montre que c'est un multiple de 3, d'où le résultat $h_K = 3$.

**Solution 11**

a) On a $2^{23}-1 = 8388607 = 47.178481$ et 47 ne divise pas 178481... Le polynôme minimal de $\zeta$ est $F(X) = (X^{23}-1)/(X-1)$ et la norme de $\zeta - 2$ est sa valeur au point 2, c'est-à-dire $2^{23}-1$.

b) De façon générale, si $m$ est un entier rationnel, $\alpha$ un entier algébrique, et $p$ le pgcd de $m$ et de $N(\alpha)$, la norme de tout élément de l'idéal engendré par $m$ et $\alpha$ est divisible par $p$. Une façon de le prouver est de remarquer que si $x = my + \alpha z$, la norme de $x$ est un produit de conjugués de $x$. Un tel conjugué s'écrit $ny' + \alpha' z'$, où $y'$, $\alpha'$ et $z'$ sont les conjugués correspondants de $y$, $\alpha$ et $z$ respectivement. En développant le produit et en rassemblant tous les termes où $m$ apparaît, on trouve $N(x) = mt + N(\alpha)N(z)$. Comme $N(x)$, $N(\alpha)$ et $N(z)$ sont rationnels, il en est de même de $t$. D'autre part, $t$ est une somme de produits d'entiers algébriques, c'est donc un entier algébrique. En fin de compte, $t$ est un entier rationnel, et $N(x)$ appartient à l'idéal de $\mathbb{Z}$ engendré par $m$ et $\mathbb{N}(\alpha)$. Ici le pgcd vaut 47, qui divise tout élément de l'idéal $\mathfrak{a}$ engendré par 47 et $\zeta - 2$.

c) Comme $\mathfrak{a}$ contient $47\mathcal{O}$ et $(\zeta-2)\mathcal{O}$, sa norme divise celle de chacun d'eux, c'est-à-dire $47^{22}$ et $2^{23}-1$. Elle divise donc leur pgcd 47. D'après la question précédente, $\mathfrak{a}$ ne contient pas 1, donc sa norme n'est pas 1. On a donc montré $N\mathfrak{a} = 47$. Si $\mathfrak{a} = \alpha\mathcal{O}$ on en déduit $N\alpha = \pm 47$. Montrons que la norme absolue de tout élément $x$ de $L$ est positive. Notons $L^+ = \mathbb{Q}(\zeta + \zeta^{-1}) = L \cap \mathbb{R}$ le sous-corps réel de $L$. La norme $y = N_{L/L^+}(x)$ est un élément de $L^+$ qui est *totalement positif*, c'est-à-dire que tous ses conjugués sont positifs. En effet, comme le groupe de Galois de $L/\mathbb{Q}$ est commutatif, chacun de ces conjugués est produit d'un conjugué de $x$ par son conjugué complexe (la conjuguaison complexe commute aux automorphisme de $L$). On en déduit que $N_{L/\mathbb{Q}}(x) = N_{L^+/\mathbb{Q}}(y)$, qui est le produit de ces conjugués, est lui aussi positif. En conclusion, on a démontré que $N(\alpha) = 47$.

d, e et f) On a vu dans le cours et dans les feuilles d'exercices que le groupe cyclique d'ordre 22 $\mathrm{Gal}(L/\mathbb{Q})$ a un seul sous-groupe d'indice 2. Le corps correspondant par la théorie de Galois est un corps quadratique, engendré par la somme de Gauß $\sqrt{-23}$. On doit avoir

$$47 = N_{L/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(N_{L/K}(\alpha)) = N_{K/\mathbb{Q}}(\omega).$$

Comme $\omega$ est une norme d'entier, c'est un entier. On a vu que l'anneau des entiers de $\mathbb{Q}(\sqrt{-23})$ est engendré comme $\mathbb{Z}$-module par 1 et $\frac{1+\sqrt{-23}}{2}$, on peut donc écrire $\omega = \frac{a+b\sqrt{-23}}{2}$, où $a$ et $b$ sont deux entiers rationnels de même parité. L'équation $47 = N_{K/\mathbb{Q}}(\omega)$ s'écrit alors $188 = a^2 + 23b^2$ et il est facile de voir qu'elle n'a pas de solution (on aurait $b^2 < 9$, donc $b^2 = 0$, 1 ou 4, etc.).