Feuille 3 : Unités, groupe des classes

Outils en vrac

1. La borne de Minkowski d'un corps K de degré n et de signature (r_1, r_2) est
$$M_K = \sqrt{|\operatorname{disc}(K)|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}$$
2. Tout idéal fractionnaire I de $\mathcal{O}_K$ contient un élément α tel que
$$|\operatorname{Norm}_{K/\mathbb{Q}}(\alpha)| \leq M_K \operatorname{Norm}_{K/\mathbb{Q}}(I).$$
3. Quelques constantes de Minkowski

Signature(r_1, r_2)	$\left(\frac{\pi}{4}\right)^{-r_2}\frac{n!}{n^n}$
$(2,0)$	0.5
$(0,1)$	0.63661
$(3,0)$	0.2222
$(1,1)$	0.28299
$(4,0)$	0.09375
$(2,1)$	0.11937
$(0,2)$	0.15198

4. Le discriminant de $x^3 + px + q$ est $-4p^3 - 27q^2$.
5. Si un polynôme unitaire $f(x) \in \mathbb{Z}[x]$ est un polynôme d'Eisenstein en un premier p, alors en notant α une racine de f, (p) est totalement ramifié dans $\mathbb{Q}(\alpha)$ et $\mathbb{Z}[\alpha]$ y est p-maximal.
6. Soit $f(x) \in \mathbb{Z}[x]$ irréductible unitaire, dans $K = \mathbb{Q}(\alpha)$ on a
$$\operatorname{Norm}_{K/\mathbb{Q}}(k - \alpha) = f(k).$$
7. Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique, où $d \in \mathbb{Z}$ est sans facteur carré. On note d_K son discriminant : si $d \equiv 1 \mod 4$, on a $d_K = d$ et $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, sinon $d_K = 4d$ et $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Un premier $p > 3$ qui ne divise pas d_K est décomposé dans K si d_K est un carré modulo p, et inerte sinon.

Exercice 1. Montrer que toute classe d'idéaux contient un idéal entier J de norme $\operatorname{Norm}_{K/\mathbb{Q}}(J) \leq M_K$ (considérer un élément $\alpha \in I^{-1}$).

Indications 1. Soit I un idéal fractionnaire, et $\alpha \in I^{-1}$ tel que
$$|\operatorname{Norm}_{K/\mathbb{Q}}(\alpha)| \leq M_K \operatorname{Norm}_{K/\mathbb{Q}}(I^{-1}).$$

Alors $J = \alpha I$ est un idéal de la classe de I, c'est un idéal entier puisque $J \subseteq II^{-1} = \mathcal{O}_K$, et

$$\mathrm{Norm}_{K/\mathbb{Q}}(J) = \mathrm{Norm}_{K/\mathbb{Q}}(\alpha I) = |\,\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|\,\mathrm{Norm}_{K/\mathbb{Q}}(I) \leq M_K$$

car la norme est multiplicative.

Exercice 2. On considère le corps $K = \mathbb{Q}(\sqrt{-43})$.

1. Calculer la décomposition de (2) et (3) dans $\mathcal{O}_K$.
2. Calculer M_K, et montrer que $\mathcal{O}_K$ est principal.
3. Soit $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ qui engendre un idéal premier, montrer que $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$ est un nombre premier.
4. Montrer que si $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ alors $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \geq 11$.
5. Soient x et $y \neq 0$ deux entiers premiers entre eux tels que $x^2+xy+11y^2 < 121$. Montrer que $x^2 + xy + 11y^2$ est un nombre premier.

Remarque : 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.

Indications 2.

1. Puisque $-43 \equiv 1 \mod 4$, on a $d_K = -43$ et $\mathcal{O}_K = \mathbb{Z}[\theta]$ où $\theta = \frac{1+\sqrt{-43}}{2}$ vérifie $\theta^2 - \theta + 11 = 0$.
   Le polynôme $x^2 - x + 11$ est irréductible modulo 2 et 3, donc (2) et (3) sont inertes.
2. La borne de Minkowski vaut $M_K = \frac{4}{\pi}\frac{2}{4}\sqrt{43} < 5$, donc toute classe d'idéaux contient un idéal de norme inférieure à 5. Il n'y a pas d'idéal de norme 2 ou 3 (un idéal I de norme 2 contient (2), qui est maximal, donc $I = (2)$ qui est de norme 4, absurde). Si I est de norme 4 et $\mathfrak{p}$ est un idéal premier qui divise I, alors $4 \in I \subseteq \mathfrak{p}$, donc $\mathfrak{p}$ divise $(2)^2$ et donc il divise (2), ce qui implique que $\mathfrak{p} = (2)$ et finalement $I = (2)$. En particulier I est principal et donc $\mathcal{O}_K$ est principal.
3. 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 $p\mathcal{O}_K$. Si $\alpha\mathcal{O}_K$ et $p\mathcal{O}_K$ sont égaux, α/p est une unité de $\mathcal{O}_K$. Or, les seules unités de $\mathcal{O}_K$ sont 1 et -1. Cela contredirait l'hypothèse selon laquelle $\alpha \notin \mathbb{Z}$.
4. Soit $\alpha = x + y\theta$. On a $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = x^2 + xy + 11y^2$.
   Pour $y \neq 0$, on a $10y^2 \geq 10$ et $x^2 + xy + y^2 \geq 1$, donc $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \geq 11$.
5. Soit $\alpha = x + y\theta$. Si $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$ n'est pas premier, soit $\mathfrak{p}$ un diviseur premier de (α) de norme $\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p}) < 11$. Puisque $\mathfrak{p} = (\beta)$, on doit avoir $\beta \in \mathbb{Z}$ qui est un diviseur commun à x et y, ce qui est impossible. Donc $x^2 + xy + 11y^2$ est premier pour $0 \leq x \leq 9$.

Exercice 3. Soit $d > 1$ un entier sans facteur carré, $K = \mathbb{Q}(\sqrt{-d})$ et d_K son discriminant. Soit p un nombre premier décomposé dans K, et $\mathfrak{p}$ un idéal au dessus de p.

1. Montrer que pour tout $i > 1$ tel que $p^i < \frac{|d_K|}{4}$, $\mathfrak{p}^i$ n'est pas principal.
2. En déduire que $h_K > 1 + \left\lfloor \frac{\log |d_K|}{\log p} \right\rfloor$.

Indications 3. 1. Puisque p est décomposé, $\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p}) = p$. On suppose que $\mathfrak{p}^i = (z)$, de sorte que $\mathrm{Norm}_{K/\mathbb{Q}}(z) = p^i$. Si $d_K = -4d$, on décompose $z = x + y\sqrt{d}$ et $x^2 + dy^2 = p^i$, en particulier $y^2 \leq p^i/d$ donc $y = 0$ et $p \mid z$, impossible. Si $d_K = -d$, on obtient plutôt $\left(x + \frac{y}{2}\right)^2 + d\left(\frac{y}{2}\right)^2 = p^i$. On déduit de même $y^2 \leq 4p^i/d < 1$ donc $y = 0$, impossible.

2. Les puissances $\mathfrak{p}^i$ sont donc distinctes dans le groupe de classes. En ajoutant la classe triviale on obtient l'égalité.

Exercice 4. Soit $K = \mathbb{Q}(\zeta_p)$ le p-ème corps cyclotomic, pour p premier et $p \leq 11$. Démontrer que $\mathcal{O}_K$ est principal (le cas $p = 11$ est difficile).

Indications 4. Si $p = 2$ on $K = \mathbb{Q}$ et donc $\mathcal{O}_K = \mathbb{Z}$.

Pour $p = 3$ et $p = 5$ la borne de Minkowski est inférieure à 2, donc chaque classe contient un idéal de norme 1 et elle donc triviale.

Pour $p = 7$, la borne de Minkowski est entre 4 et 5, et il faut donc regarder la factorisation de (2) et (3) dans $\mathcal{O}_K$, ce qui revient à regarder la factorisation de $\Phi_7 = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ sur $\mathbb{F}_q$ pour $q = 2, 3$. Le 7-ème polynôme cyclotomique se factorise sur $\mathbb{F}_q$ (pour $q \neq 7$) en $6/f$ facteurs irréductibles de dégrée f, où f est l'ordre de q mod 7. En particulier on voit que $2 = \mathfrak{q}_1\mathfrak{q}_2$ et que (3) est inerte. De plus, $\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{q}_1) = \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{q}_2) = 8$ et $\mathrm{Norm}_{K/\mathbb{Q}}(3) = 3^6$. On en déduit qu'il n'y a pas d'idéaux de norme 2, 3 ou 4 et donc $\mathcal{O}_K$ est principal.

Pour $p = 11$, la borne de Minkowski est entre 58 et 59. On veut raisonner comme pour $p = 7$, mais il faut tout d'abord traiter le cas $q = 11$: on sait que $11 = \mathfrak{q}^{10}$ est totalement ramifié avec $\mathfrak{q} = (1 - \zeta_{11})$ est principal, et donc il ne pose pas de problèmes. Pour $q \leq 58$ premier différent de 11, on raison comme ci-dessus.

— Pour $q = 2$ on a $f = 10$ et donc (2) est inerte de norme $2^{10} > 58$, donc il n'y a pas d'idéaux de norme 2.

— Pour $q = 3$ on a $f = 5$ et donc (3) est le produit de deux idéaux de norme $3^5 > 58$, donc il n'y a pas d'idéaux de norme 3.

— Pour $q = 5$ on a $f = 5$ et donc (5) est le produit de deux idéaux de norme $5^5 > 58$, donc il n'y a pas d'idéaux de norme 5.

— Pour $q = 7$ on a $f = 10$ et donc (7) est inerte de norme $7^{10} > 58$, donc il n'y a pas d'idéaux de norme 7.

Pour $q > 7$ (et différent de 11), on a $q^2 > 58$, donc les seuls premiers à traiter sont ceux qui sont totalement décomposés, c'est-à-dire les q qui ont ordre 1 dans $(\mathbb{Z}/11\mathbb{Z})^*$, ce qui équivaut à $q \equiv 1 \bmod 11$. On voit immédiatement que $q = 23$ est la seule possibilité.

On a $(23) = \mathfrak{q}_1 \cdots \mathfrak{q}_{10}$ où chaque $\mathfrak{q}_i$ est un premier de norme 23 et correspond à un facteur de degré 1 de $\Phi_1 1$ sur $\mathbb{F}_{23}$, c'est-à-dire à une racine de Φ_{11} dans $\mathbb{F}_{23}$.

Les racines de Φ_{11} sont les racines primitive 11-èmes de l'unité, donc les $\alpha \in \mathbb{F}_{23}$ tels que $\alpha \neq 1$ et $\alpha^{11} = 1$. Les $\mathfrak{q}_i$ sont tous conjugués par rapport à l'action du groupe de Galois, donc il suffit de montrer qu'un seul $\mathfrak{q}_i$ est principal pour en déduire que les autres les sont aussi. On vérifie aisément que $2^{11} \equiv 1 \bmod 23$ et donc pour terminer il suffit de montrer que $\mathfrak{q} = (23, \zeta_{11} - 2)$ est principal (les autres racines de Φ_{11} sont donnée par les puissances de 2 et elles sont 3, 4, 6, 8, 9, 12, 13, 16 et 18). Montrer à la main que $\mathfrak{q}$ (ou n'importe quel autre idéale de norme 23) est principal n'est pas facile. La technique classique est de trouver $z \in \mathcal{O}_K$ tel que $\mathrm{Norm}_{K/\mathbb{Q}}(z) = 23$: en effet l'idéal (z) serait un idéal premier (étant sa norme un premier de $\mathbb{Z}$) de norme 23 et donc forcement (z) serait un des $\mathfrak{q}_i$. Ceci est la partie compliquée (on n'utilise donc pas la forme explicite des $\mathfrak{q}_i$).

On peut écrire

$$z = a_0 + a_1\zeta_{11} + a_2\zeta_{11}^2 + \cdots a_9\zeta_{11}^9$$

et l'idée est de tester, avec un ordinateur, les cas ou tous les $a_i \in \{0, 1, -1\}$. Pour calculer la norme on travail dans $\mathbb{Z}[x]/(\Phi_{11}(x)) \cong \mathcal{O}_K$, où z correspond à l'élément

$$z = a_0 + a_1x + a_2x^2 + \cdots a_9x^9$$

La norme de z est égale au produit de ses conjugués, et on a

$$(\mathbb{Z}/11\mathbb{Z})^* \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q})$$
$$n \mapsto (\zeta_{11} \mapsto \zeta_{11}^n)$$

Donc, dans $\mathbb{Z}[x]/(\Phi_{11}(x))$, on a

$$\mathrm{Norm}_{K/\mathbb{Q}}(z) = \prod_{j=1}^{10} \sum_{i=0}^{9} a_i x^{ji} \tag{1}$$

On va utiliser PARI/GP. Le code suivant défini une fonction `allvecs(n)` qui produit une liste contenant tous les vecteurs de longueur n avec coefficients dans $\{0, \pm 1\}$.

```
allvecs(n) =
{
  my(L = List());
  my(box = vector(n, i, [-1,1]));
  forvec(v = box, listput(L, v));
  Vec(L)
};
```

Par exemple `allvecs(3)` donne

```
[[-1, -1, -1], [-1, -1, 0], [-1, -1, 1], [-1, 0, -1], [-1, 0, 0],
[-1, 0, 1], [-1, 1, -1], [-1, 1, 0], [-1, 1, 1], [0, -1, -1],
[0, -1, 0], [0, -1, 1], [0, 0, -1], [0, 0, 0], [0, 0, 1],
[0, 1, -1], [0, 1, 0], [0, 1, 1], [1, -1, -1], [1, -1, 0],
[1, -1, 1], [1, 0, -1], [1, 0, 0], [1, 0, 1], [1, 1, -1],
[1, 1, 0], [1, 1, 1]]
```

On pose `L = allvecs(10)`. Avec mon ordinateur il faut avant exécuter

```
default(parisize, 100000000000)
```

sinon PARI/GP n'a pas suffisamment de mémoire. Le calcul de la norme dans (1) devient alors (pour le vecteur de coordonnées correspondant à `L[1]`, le premier élément de `L`).

```
prod(j=1, 10, sum(i = 0, 9, L[1][i+1]*Mod(x,polcyclo(11))^(i*j)))
```

Attention : les indice commencent à `1` dans PARI/GP. Dans ce cas le résultat est

```
Mod(1, x^10+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)
```

et `L[1]` est

```
[-1, -1, -1, -1, -1, -1, -1, -1, -1, -1]
```

donc

$$\mathrm{Norm}_{K/\mathbb{Q}}(-1-\zeta_{11}-\zeta_{11}^2-\ldots-\zeta_{11}^9)=1$$

(et l'élément est donc une unité). On peut maintenant tester facilement tous les élément de `L`, en s'arrêtant si le résultat est 23 :

```
for(k=1, length(L), P = prod(j=1, 10, sum(i = 0, 9,
  L[k][i+1]*Mod(x,polcyclo(11))^(i*j)));
  if(P == 23, print(k); break))
```

Le programme nous donne très rapidement la réponse `11`, et `L[11]` est

```
[-1, -1, -1, -1, -1, -1, -1, 0, -1, 0]
```

Donc

$$z=-1-\zeta_{11}-\zeta_{11}^2-\zeta_{11}^3-\zeta_{11}^4-\zeta_{11}^5-\zeta_{11}^6-\zeta_{11}^8$$

est un élément de norme 23 et finalement $\mathcal{O}_K$ est principal (parmi les 59049 vecteurs de `L` il y en a 4080 qui marchent, presque le 70% !).

PARI/GP est capable de calculer la norme d'un élément dans un corps de nombre, et il nous confirme que z a norme 23 :

```
K = nfinit(polcyclo(11));
idealnorm(K, -1-x-x^2-x^3-x^4-x^5-x^6-x^8)
```

La première ligne déclare que `K` est le corps de nombre associé à Φ_{11} (la variable, qui correspond à ζ_{11} s'appelle `x` par défaut). La deuxième calcule la norme de l'élément donné et la réponse est bien 23.

On peut préciser quel idéal on a montré être maximal (ça n'a aucune importance pour l'exercice) : on a

$$(23,\zeta_{11}-6)=(-1-\zeta_{11}-\zeta_{11}^2-\zeta_{11}^3-\zeta_{11}^4-\zeta_{11}^5-\zeta_{11}^6-\zeta_{11}^8)$$

En effet

$$23 = (-1-\zeta_{11}-\zeta_{11}^2-\zeta_{11}^3-\zeta_{11}^4-\zeta_{11}^5-\zeta_{11}^6-\zeta_{11}^8)\cdot$$
$$(3+15\zeta_{11}+17\zeta_{11}^2+2\zeta_{11}^3+11\zeta_{11}^4+\zeta_{11}^5+7\zeta_{11}^6+8\zeta_{11}^7+12\zeta_{11}^8+5\zeta_{11}^9)$$

et

$$\zeta_{11}-6 = (-1-\zeta_{11}-\zeta_{11}^2-\zeta_{11}^3-\zeta_{11}^4-\zeta_{11}^5-\zeta_{11}^6-\zeta_{11}^8)\cdot$$
$$(-1-4\zeta_{11}-4\zeta_{11}^2-3\zeta_{11}^4-2\zeta_{11}^6-2\zeta_{11}^7-3\zeta_{11}^8-\zeta_{11}^9)$$

Donc

$$(23, \zeta_{11}-6) \subseteq (-1-\zeta_{11}-\zeta_{11}^2-\zeta_{11}^3-\zeta_{11}^4-\zeta_{11}^5-\zeta_{11}^6-\zeta_{11}^8)$$

et on déduit l'égalité par maximalité de $(23, \zeta_{11}-6)$.

On a $r_2 = 5$, donc $\mathcal{O}_K^* \cong \mu_{11} \times \mathbb{Z}^5$: ce n'est pas facile en général de trouver une système fondamentale d'unités, mais on peut demander à PARI/GP avec la commande `K.fu` et on obtient les 5 unité suivantes

$$1,\ z_1 = \zeta_{11}+1, z_2 = \zeta_{11}^2+1, z_3 = \zeta_{11}^2+\zeta_{11}+1 \text{ et } z_4 = -\zeta_{11}^6-\zeta_{11}$$

Par exemple,

$$\zeta(z z_1^2 z_3^4) =$$
$$26+65\zeta_{11}+108\zeta_{11}^2+141\zeta_{11}^3+150\zeta_{11}^4+129\zeta_{11}^5+86\zeta_{11}^6+39\zeta_{11}^7+5\zeta_{11}^8-8\zeta_{11}^9$$

est un autre élément de norme 23.

Exercice 5. Soit K un corps de nombres cubique, tel que $\mathrm{disc}(K) < 0$.

1. Montrer que la signature de K est $(1,1)$ (commencer par supposer $\mathcal{O}_K$ monogène).
2. Désormais, on utilise le plongement réel pour voir K comme un sous-corps de $\mathbb{R}$. Montrer qu'il existe $\varepsilon > 1$ tel que $\mathcal{O}_K^* = \{\pm\varepsilon^k, k \in \mathbb{Z}\}$.
3. Montrer que $K = \mathbb{Q}(\varepsilon)$, et que le polynôme minimal de ε est de la forme $g(x) = (x-\varepsilon)(x-\sqrt{\varepsilon^{-1}}e^{it})(x-\sqrt{\varepsilon^{-1}}e^{-it})$ pour $t \in \mathbb{R}$.
4. Montrer l'inégalité d'Artin : $|\mathrm{disc}(g(x))| < 4(\varepsilon^3+6)$ (utiliser sans preuve l'inégalité magique $\left(\frac{u^3+u^{-3}}{2}-\cos t\right)^2 \sin^2 t < \frac{u^6+6}{4}$, valable pour tous réels u, t).
5. Montrer que si $u > 1$ est une unité qui vérifie $4(u^{3/2}+6) < |\mathrm{disc}(K)|$, alors $u = \varepsilon$.
6. Soit $K = \mathbb{Q}(\alpha)$ où $\alpha^3+\alpha = 1$. Déterminer une unité fondamentale de K (on donne $\alpha \approx 0.6823$ dans $\mathbb{R}$).

Indications 5. 1. Soit α un entier algébrique tel que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ et considérons α_1, α_2 et α_3 ses conjugués. On a $\mathrm{disc}(K) = \prod_{i<j}(\alpha_i-\alpha_j)^2$. Si

on avait $r_1 = 3$, le discriminant serait un produit de carrés dans $\mathbb{R}$, donc serait positif. L'argument subsiste si $\mathbb{Z}[\alpha]$ est d'indice fini, puisque son discriminant diffère de celui de $\mathcal{O}_K$ d'un carré, et donc il a le même signe. Plus généralement, le discriminant d'un corps de nombres est toujours de signe $(-1)^{r_2}$.

2. Les racines de l'unité de K se plongent dans $\mathbb{R}$, ce sont donc ± 1. Le théorème des unités énonce que le rang vaut 1, il existe donc une unité fondamentale ε telle que $\mathcal{O}_K^* = \{\pm\varepsilon^k,\ k \in \mathbb{Z}\}$. Quitte à changer ε par $\pm\varepsilon^{\pm 1}$, on peut supposer $\varepsilon > 1$.
3. On a $\varepsilon \notin \mathbb{Q}$ car $\mathbb{Q}$ n'a pas d'unité d'ordre infini. Puisque $\mathbb{Q}(\varepsilon) \subseteq K$ est forcement de degré 3, on a égalité.
   On écrite le minimal $g(x) = (x-\varepsilon)(x-z)(x-\bar{z})$ avec la norme
   $$\mathrm{Norm}_{K/\mathbb{Q}}(\varepsilon) = \pm 1 = \varepsilon|z|^2 > 0.$$
   Donc $|z|^2 = \varepsilon^{-1}$. En écrivant une décomposition polaire on a l'écriture souhaitée.
4. Poser $u = \sqrt{\varepsilon}$ et faire le calcul.
5. Puisque $\mathrm{disc}(K) \leq \mathrm{disc}(g(x))$, on a que $|\mathrm{disc}(K)| < 4(\varepsilon^3 + 6)$. Si $u = \varepsilon^k$ avec $k \geq 2$, alors ε violerait l'inégalité d'Artin.
6. Soit $f(x) = x^3 + x - 1$. On a que $\mathrm{disc}(f) = -31$ est sans facteurs carrés, donc il est égal à $\mathrm{disc}(K)$. Étant donné la forme de l'équation, α et $\beta = \alpha + 1 \approx 1.46553329$ sont des unités. La seconde vérifie $4(\beta^{3/2} + 6) \approx 30.2953 < 31$.

Exercice 6. Soit $K = \mathbb{Q}(\alpha)$, où α est une racine de $x^3 + 6x + 6$.

1. Déterminer le discriminant d_K de K et son anneau d'entiers.
2. Déterminer la signature de K, et sa constante de Minkowski M_K.
3. Déterminer les idéaux premiers de norme inférieure à M_K.
4. Calculer $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$ et $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha + 2)$ et en déduire que $\mathrm{Cl}(K)$ est cyclique.
5. Montrer que $u = \alpha + 1 \in \mathcal{O}_K^*$ est une unité.
6. Montrer que u est une unité fondamentale et en déduire que u est non triviale dans $\mathcal{O}_K^*/(\mathcal{O}_K^*)^3$ (utiliser l'inégalité d'Artin avec une calculatrice : $\alpha \approx -0.884$).
7. Montrer que 2, $2u$ et $2u^2$ ne sont pas des cubes dans $\mathcal{O}_K$ (regarder modulo $\mathfrak{p}_7$, un idéal premier au-dessus de (7).
8. En déduire $\mathrm{Cl}(K)$.

Indications 6.
1. Le discriminant de $x^3 + 6x + 6$ vaut $-4 \cdot 6^3 - 27 \cdot 6^2 = -2^2 \cdot 3^3 \cdot 17$. Le polynôme étant d'Eisenstein en 2 et 3, et puisque 17 apparaît sans carré, on a $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
2. Le discriminant étant négatif, le corps n'est pas réel. La signature est $(1, 1)$ et la constante de Minkowski vaut environ 12.123.

3. Soit $\mathfrak{p}$ un idéal premier de norme inférieur ou égale à 12. Vu que $\mathfrak{p}$ divise $\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p}) = 2^a 3^b 5^c$ on a que $\mathfrak{p}$ divise au moins un parmi (2), (3) et (5) et aussi les idéaux qui apparaissaient dans leur factorisation.
   On sait que $(2) = \mathfrak{p}_2^3$ et $(3) = \mathfrak{p}_3^3$ sont totalement ramifiés. Le polynôme $x^3 + x + 1$ est irréductible modulo 5, donc (5) est inerte. On décompose $(7) : x^3 - x - 1 = (x+2)(x^2 - 2x + 3)$ donc $(7) = \mathfrak{p}_7\mathfrak{p}_7$ ou $\mathfrak{p}_7 = (7, \alpha + 2)$ et $\mathfrak{q}_7 = (7, \alpha^2 - 2\alpha + 3)$. Le polynôme $x^3 + 6x + 6$ n'a pas de racine modulo 11, donc (11) est inerte.
   Or, si $\mathfrak{p}$ divise $\mathfrak{p}_2$, on a $\mathfrak{p} = \mathfrak{p}_2$ car les deux sont premiers, et pareil pour $\mathfrak{p}_3$. Si $\mathfrak{p}$ divise (5) on doit avoir $\mathfrak{p} = (5)$, ce qui est impossible parce que $\mathrm{Norm}_{K\mathbb{Q}}(5) = 125$ et de même pour 11. Finalement, si $\mathfrak{p}$ divise (7), soit $\mathfrak{p} = \mathfrak{p}_7$ soit $\mathfrak{p} = \mathfrak{q}_7$, mais la norme de $\mathfrak{q}_7$ est 49 et donc $\mathfrak{p} = \mathfrak{p}_7$.
   En conclusion, les idéaux premier de norme inférieure à M_K sont $\mathfrak{p}_2$, $\mathfrak{p}_3$ et $\mathfrak{p}_7$, qui engendrent le groupe des classes.
4. $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = 6$, donc $(\alpha) = \mathfrak{p}_2\mathfrak{p}_3$, donc $[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1}$ dans le groupe des classes. De même, $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha + 2) = 14$, donc $\mathfrak{p}_2\mathfrak{p}_7$ est principal. Ainsi, le groupe des classes est engendré par $\mathfrak{p}_2$.
5. $\mathrm{Norm}_{K/\mathbb{Q}}(u) = -1$, donc c'est une unité.
6. On a $\alpha + 1 \approx 0.1153$ et $(\alpha + 1)^{-1} \approx 8.6671$ donc $4((\alpha + 1)^{-3/2} + 6) \approx 126.0649 < 1836 = |\operatorname{disc}(K)|$. On en déduite que $(\alpha + 1)^{-1}$ est une unité fondamentale et donc $\alpha + 1$ aussi.
7. ± 2 n'est pas un cube dans $\mathbb{Z}/7\mathbb{Z}$ et $\alpha \equiv -2 \bmod \mathfrak{p}_7$.
8. Il faut voir si $\mathfrak{p}_2$ est principal ou d'ordre 3 dans $\mathrm{Cl}(K)$ (puisque $(2) = \mathfrak{p}_2^3$ est principal). Si $\mathfrak{p}_2 = (\beta)$ on aurait $(\beta^3) = (2)$ et donc une unité $v \in \mathcal{O}_K^*$ telle que $2v = \beta^3$. Les seules unités de $\mathcal{O}_K$ d'ordre fini sont ± 1 (car K est de degré 3 et donc il ne peut pas contenir d'autres racines de l'unité), donc, étant u une unité fondamentale, $v = \pm u^n$ (le rang de $\mathcal{O}_K^*$ est 1). En écrivant la division euclidienne $n = 3q + r$ on obtient

   $$\pm 2u^{3q+r} = \beta^3 \text{ donc } 2u^r = (\pm\beta u^{-q})^3$$

   ce qui est absurde à cause de la question précédente. En conclusion $\mathrm{Cl}(K)$ est un groupe d'ordre 3, engendré par $\mathfrak{p}_2$.

Exercice 7. Soit K un corps de nombres, et $m > 1$ un entier. On pose $\mathrm{Cl}(K)[m] = \{a \in \mathrm{Cl}(K),\ a^m = 1\}$ le groupe de m-torsion.

1. Montrer que si h_K est premier à m, alors $\mathrm{Cl}(K)[m] = \{1\}$. On définit $G_m(K) = \{x^m,\ x \in K^*\}$ et $L_m(K)$ l'ensemble des éléments $x \in K^*$ tels que dans la factorisation en idéaux premiers de (x) tous les exposants sont multiples de m. On pose $S_m(K) = L_m(K)/G_m(K)$.
2. Montrer qu'on a un morphisme de groupes $\phi\colon S_m(K) \to \mathrm{Cl}(K)[m]$ défini par $\phi(x) = a_x$, où a_x est l'unique idéal fractionnaire tel que $a_x^m = (x)$.
3. Montrer que ϕ est surjectif et déterminer son noyau. On suppose désormais que $K = \mathbb{Q}(\sqrt{-d})$ est un corps quadratique imaginaire, avec $d > 0$ sans facteur carré.

4. Soit $x = a + b\sqrt{-d} \in K$ tel que $\mathrm{Norm}_{K/\mathbb{Q}}(x) = 1$. Montrer qu'il existe $y \in K^*$ tel que $x = \frac{y}{\overline{y}}$, où $\overline{y}$ désigne le conjugué complexe de y (on pourra considérer l'application $\psi : K \to K$ définie par $\psi(y) = \overline{y} - xy$).
5. Soit $\mathfrak{a} \in \mathrm{Cl}(K)[2]$, on pose $a = \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{a})$. Montrer qu'il existe $y \in K^*$ tel que $\mathfrak{a}^2 = \left(\frac{a\overline{y}}{y}\right)$.
6. On pose $\mathfrak{b} = y\mathfrak{a}$, montrer qu'il existe $b \in \mathbb{Q}^*$ tel que $\mathfrak{b}^2 = (b)$.
7. Montrer que $\mathfrak{a} \in \mathrm{Cl}(K)[2]$ est dans la classe d'un produit d'idéaux ramifiés.
8. On note $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ les premiers ramifiés de K. Soit une famille $0 \leq e_i \leq 1$, montrer que si $\prod_{i=1}^{t} \mathfrak{p}_i^{e_i}$ est principal, ce produit vaut (1) ou $(\sqrt{d})$.
9. Montrer que $\mathrm{Cl}(K)[2] \cong \mathbb{F}_2^{t-1}$.