

---

### 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

$$M_K = \sqrt{|\text{disc}(K)|} \left( \frac{4}{\pi} \right)^{r_2} \frac{n!}{n^n}$$

2. Tout idéal fractionnaire  $I$  de  $\mathcal{O}_K$  contient un élément  $\alpha$  tel que

$$|\text{Norm}_{K/\mathbb{Q}}(\alpha)| \leq M_K \text{Norm}_{K/\mathbb{Q}}(I).$$

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  $\alpha$  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

$$\text{Norm}_{K/\mathbb{Q}}(k - \alpha) = f(k).$$

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  $d \equiv 1 \pmod{4}$ , 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  $\text{Norm}_{K/\mathbb{Q}}(J) \leq M_K$  (considérer un élément  $\alpha \in I^{-1}$ ).

**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  $\text{Norm}_{K/\mathbb{Q}}(\alpha)$  est un nombre premier.
4. Montrer que si  $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$  alors  $\text{Norm}_{K/\mathbb{Q}}(\alpha) \geq 11$ .
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.*

**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  $h_K > 1 + \left\lfloor \frac{\log |d_K|}{\log p} \right\rfloor$ .

**Exercice 4.** Soit  $K$  un corps de nombres cubique, tel que  $\text{disc}(K) < 0$ .

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  $\varepsilon$  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 :  $|\text{disc}(g(x))| < 4(\varepsilon^3 + 6)$  (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  $4(u^{3/2} + 6) < |\text{disc}(K)|$ , 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  $\mathbb{R}$ ).

**Exercice 5.** 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).

**Exercice 6.** Soit  $K = \mathbb{Q}(\alpha)$ , où  $\alpha$  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  $\text{Norm}_{K/\mathbb{Q}}(\alpha)$  et  $\text{Norm}_{K/\mathbb{Q}}(\alpha + 2)$  et en déduire que  $\text{Cl}(K)$  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  $\text{Cl}(K)$ .

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

1. Montrer que si  $h_K$  est premier à  $m$ , alors  $\text{Cl}(K)[m] = \{1\}$ . 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  $\phi: S_m(K) \rightarrow \text{Cl}(K)[m]$  défini par  $\phi(x) = a_x$ , où  $a_x$  est l'unique idéal fractionnaire tel que  $a_x^m = (x)$ .
3. Montrer que  $\phi$  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  $\text{Norm}_{K/\mathbb{Q}}(x) = 1$ . Montrer qu'il existe  $y \in K^*$  tel que  $x = \frac{y}{\bar{y}}$ , où  $\bar{y}$  désigne le conjugué complexe de  $y$  (on pourra considérer l'application  $\psi: K \rightarrow K$  définie par  $\psi(y) = \bar{y} - xy$ ).
5. Soit  $\mathfrak{a} \in \text{Cl}(K)[2]$ , on pose  $a = \text{Norm}_{K/\mathbb{Q}}(\mathfrak{a})$ . Montrer qu'il existe  $y \in K^*$  tel que  $\mathfrak{a}^2 = \left(\frac{a\bar{y}}{y}\right)$ .
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  $\mathfrak{a} \in \text{Cl}(K)[2]$  est dans la classe d'un produit d'idéaux ramifiés.
8. On note  $\mathfrak{p}_1, \dots, \mathfrak{p}_t$  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  $\text{Cl}(K)[2] \cong \mathbb{F}_2^{t-1}$ .