6. Exercices du chapitre 6

Exercice 6.2 On a $\Pi_{\alpha,\mathbb{Q}} = X^2 + X + 5$ donc $\mathrm{disc}(A) = -19$. D'après Minkowski tout idéal non nul de A est équivalent à un idéal contenant N avec $1 \leq N \leq C(A) = \frac{1}{2}\frac{4}{\pi}\sqrt{19} < 3$ (voir la table). Mais X^2+X+5 est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$ donc les seuls idéaux de A contenant 2 sont $2A$ et A. Ainsi, $\mathrm{Cl}(A) = 1$ et donc A est principal. On a vu au chapitre 4 qu'il n'est pas euclidien.

Exercice 6.3 On a $\Pi_{\alpha,\mathbb{Q}} = X^2 + 5$ donc $\mathrm{disc}(A) = -20$. D'après Minkowski, tout idéal non nul de A est équivalent à un idéal contenant N avec $1 \leq N \leq C(A) = \frac{1}{2}\frac{4}{\pi}\sqrt{20} < 3$ (voir la table). Comme $X^2 + 5 \equiv (X-1)^2 \bmod 2$, les idéaux contenant 2 sont $2A$, $2A + (\alpha - 1)A = I$ et A. Ainsi, tout idéal est équivalent à I ou bien principal.

Si $I = zA$ alors $\mathrm{N}(I) = |\mathrm{N}(z)|$. Mais $\mathrm{N}(I) = 2$ (pourquoi ?) et $x^2 + 5y^2$ ne représente pas 2, donc I n'est pas principal. Ainsi, $[I] \neq [A]$ et donc $|\mathrm{Cl}(A)| = 2$.

On a $I^2 = (4, (\alpha-1)^2, 2(\alpha-1))$. Mais $(\alpha-1)^2 = -4 - 2\alpha = -2(2+\alpha)$, donc

$$I^2 = (2)(2, 2+\alpha, \alpha - 1) = (2)$$

car $1 = (2+\alpha) - 2 - (\alpha - 1)$. Ainsi, $[I]^2 = 1 = [A]$ dans $\mathrm{Cl}(A)$, et donc $\mathrm{Cl}(A) \simeq \mathbb{Z}/2\mathbb{Z}$. Si J est un idéal non nul de A, alors J est principal si et seulement si $[J] = 1$ dans $\mathrm{Cl}(A)$. On conclut car $[J] \neq [IJ]$ dans le groupe $\mathrm{Cl}(A)$, car $[I] \neq [A]$.

Exercice 6.4 Le (i) et (ii) sont similaires à l'exercice précédent. Comme $(\alpha-1)^2 = -2(1+\alpha)$, on a $I^2 = (4, -2(1+\alpha), 2(\alpha-1)) = 2(2, \alpha+1, \alpha-1) = 2I$. La structure de $\mathrm{Cl}(A) = \{[A], [I]\}$ est donc telle que $[I]^2 = [I]$: ce n'est donc pas un groupe (c'est l'unique monoïde unitaire à deux éléments qui n'est pas un groupe !). Si J est un idéal non nul de A, alors on constate que $[JI] = [J][I] = [I]$ quel que soit $[J]$, donc IJ n'est jamais principal.

Exercice 6.7 On a $\mathrm{disc}(X^3 - d) = -27d^2$. Si $K = \mathbb{Q}(\sqrt[3]{d})$ alors $r_1 = 1$ et $r_2 = 1$. Quand $d = 2$, Minkowski nous dit que tout idéal non nul de A est équivalent à un idéal contenant un entier $\leq \frac{4}{\pi}\frac{3!}{3^3}6\sqrt{3} = \frac{16}{\pi\sqrt{3}} < 3$ (donnée). Les idéaux de A contenant 2 sont $A, 2A$, $I = 2A + \alpha A$ et $J = 2A + \alpha^2 A$, donc $\mathrm{Cl}(A) = \{[A], [I], [J]\}$. On a $\alpha^3 = 2$ donc $2 \in \alpha^2 A \subset \alpha A$, donc $I = (\alpha)$ et $J = (\alpha)^2$ sont principaux, puis $|\mathrm{Cl}(A)| = 1$. L'anneau A est un ordre de $\mathbb{Q}(\alpha)$. Il est principal, donc intégralement clos, et donc il contient $\mathcal{O}_{\mathbb{Q}(\alpha)}$: c'est donc exactement l'anneau des entiers de $\mathbb{Q}(\alpha)$.

Exercice 6.8 Soient $\zeta = e^{2i\pi/5}$, $K = \mathbb{Q}(\zeta)$ et $A = \mathbb{Z}[\zeta]$. On a $r_1 = 0$ et $r_2 = 2$. De plus $\mathrm{disc}(A) = \mathrm{disc}(X^4 + X^3 + X^2 + X + 1) = 5^3$ (exercice 5.14). On vérifie que

$$C(2,4) \cdot 5\sqrt{5} \simeq 1,7 < 2,$$

donc A est principal par Minkowski.

7. Exercices du chapitre 7

Exercice 7.1 (i) Soit $\alpha = \sqrt{6}$, alors $A = \mathbb{Z}[\alpha]$ est l'anneau des entiers de $\mathbb{Q}(\sqrt{6})$. Les idéaux contenant 15 sont donc les facteurs de (15). Comme $X^2 - 6 \equiv X^2 \bmod 3$, on a $(3) = T^2$ avec $T = (3, \alpha)$ premier. Comme $X^2 - 6 \equiv (X-1)(X+1) \bmod 5$ on a $(5) = C_+C_-$ avec $P_\pm = (5, \alpha \pm 1)$ premier. Ainsi, $(15) = T^2C_+C_-$. Les idéaux cherchés sont donc les 12 idéaux suivants :

$$A,\ T,\ C_+,\ C_-,\ T^2 = (3),\ TC_+,\ TC_-,\ C_+C_- = (5),\ T^2C_+,\ T^2C_-,\ TC_+C_-,\ T^2C_+C_- = (15).$$

(ii) Soit $\alpha = \sqrt{5}$, alors $A = \mathbb{Z}[\alpha]$ est l'anneau des entiers de $\mathbb{Q}(\alpha)$. L'idéal principal engendré par $\beta = 1 + 2\alpha$ est de norme $N(\beta) = 1 + 4.5 = 21 = 3 \cdot 7$. Il est donc produit d'un idéal premier de norme 3 par un autre de norme 7. Les idéaux premiers contenant 3 sont les deux idéaux $T_\pm = (3, \alpha \pm 1)$ et ceux contenant 7 sont $S_\pm = (7, \alpha \pm 3)$. Mais $\beta = 2\alpha + 1 = 2(\alpha - 1) + 3 \in T_-$ et $\beta = 2(\alpha - 3) + 7 \in S_-$, donc T_- et S_- divisent (β), puis $(\beta) = T_-S_-$ (identité pas très difficile à vérifier à posteriori !).

Exercice 7.4 Traitons d'abord le cas de $A = \mathbb{Z}[\alpha]$ avec $\alpha = \sqrt{-13}$. On a $\mathrm{disc}(A) = \mathrm{disc}(X^2 + 13) = -52$. Les estimées de Minkowski démontrent que tout idéal non nul de A est équivalent à un idéal contenant un entier N tel que $1 \leq N \leq \frac{2}{\pi}\sqrt{52} < 5$. Les idéaux de A contenant 2 sont $2A$, $D = (2, \alpha + 1)$ (premier) et A car $X^2 + 13 \equiv (X+1)^2 \bmod 2$. De plus, $X^2 + 13$ est irréductible modulo 3, donc les seuls idéaux de A contenant 3 sont $3A$ et A. De plus, A est l'anneau des entiers de $\mathbb{Q}(\sqrt{-13})$, car -13 est sans facteur carré et $\equiv 3 \bmod 4$. D'après le cours (ou par un calcul direct) on a $(2) = D^2$, donc $(4) = D^4$, de sorte que les idéaux contenant 4 sont les D^i par la propriété de Dedekind. Il s'ensuit qu'en tant que groupes

$\mathrm{Cl}(A) = \langle [D] \rangle$. Mais D n'est pas principal car 2 n'est pas représenté par $x^2 + 13\,y^2$, et $[D]^2 = [A]$, donc $\mathrm{Cl}(A) = \mathbb{Z}/2\mathbb{Z}$.

Supposons maintenant $A = \sqrt{26}$, donc $\mathrm{disc}(A) = -92$ et tout idéal non nul de A est équivalent à un idéal contenant un entier N tel que $1 \leq N \leq \frac{2}{\pi}\sqrt{92} < 7$(Minkowski). A est l'anneau des entiers de $\mathbb{Q}(\sqrt{-26})$ car -26 est sans facteur carré et $\equiv 2 \bmod 4$. Il s'ensuit que $\mathrm{Cl}(A)$ est engendré *comme groupe* par les idéaux premiers divisant $2, 3, 4, 5, 6$, i.e. par les idéaux premiers contenant $2, 3$ ou 5. Ce sont respectivement $D = (2, \alpha)$, $T_\pm = (3, \alpha \pm 1)$ et $C_\pm = (5, \alpha \pm 2)$ (de normes 2, 3 et 5). D'après le cours on a les relations $(2) = D^2$, $(3) = T_+T_-$ et $(5) = C_+C_-$. La forme $x^2 + 26\,y^2$ représente $27 = \mathrm{N}((1+\alpha)) = 3^3$ et $30 = \mathrm{N}((2+\alpha)) = 2 \cdot 3 \cdot 5$. Mais $1 + \alpha \in T_+$ et $1 + \alpha \notin T_-$ (sinon on aurait $3 - (1+\alpha) - (1-\alpha) = 1 \in T_-$ et donc $T_- = A$), et $2 + \alpha$ est manifestement dans D, T_- et C_+, donc

$$(1 + \alpha) = T_-^3 \ \text{ et } \ (2 + \alpha) = DT_-C_+$$

par multiplicativité de la norme et propriété de Dedekind. On en déduit les relations $[D]^2 = [A]$, $[T_+][T_-] = [A]$, $[T_-]^3 = [A]$, $[D][T_-][C_+] = [A]$ et $[C_-][C_+] = [A]$ donc $\mathrm{Cl}(A)$ est engendré par $[D]$ et $[T_-]$. Mais $[DT_-]^3 = [D]$ et $[DT_-]^2 = [T_-]^{-1}$ donc $\mathrm{Cl}(A)$ est engendré par l'élément $[DT_-]$ dont l'ordre divise 6. Comme ni 2 ni 3 n'est représenté par $x^2 + 26\,y^2$, ni D ni T_- n'est principal et donc $\mathrm{Cl}(A) \simeq \mathbb{Z}/6\mathbb{Z}$.

Exercice 7.5 (i) Il est évident qu'un idéal principal non nul (π) d'un anneau A quelconque est premier si et seulement π est un élément premier, comme on l'a déjà remarqué dans le cours. Il faut donc simplement que vérifier que si un idéal premier $P \subset \mathcal{O}_K$ contient un élément premier π, alors $P = (\pi)$. Mais l'idéal (non nul) (π) est premier par l'observation précédente, il est donc maximal par un résultat du cours, et donc $(\pi) = P$.

(ii) Supposons $\mathcal{O}_K$ factoriel. Nous allons montrer que tous les idéaux premiers de $\mathcal{O}_K$ sont principaux. Il en résultera que $\mathcal{O}_K$ est principal par la propriété de Dedekind. Soient P un idéal premier non nul de $\mathcal{O}_K$ et $z \in P$ un élément non nul. Comme $\mathcal{O}_K$ a la propriété de factorisation (par exemple car il est noethérien), z est produit fini d'irréductibles. Comme P est premier il contient au moins un des facteurs irréductibles π de z. Mais π étant irréductible et $\mathcal{O}_K$ étant factoriel, π est premier, et donc $P = (\pi)$ d'après le (i).

(iii) Supposons qu'un ordre $A \subset \mathcal{O}_K$ est factoriel. L'anneau A étant un ordre on a $\mathrm{Frax}(A) = K$. Comme il est factoriel il est intégralement clos, donc en particulier $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K \subset A$, et donc $\mathcal{O}_K = A$.

Problème 7.1 (i) Soient Q et Q' sont deux diviseurs de $P = \overline{\Pi}_{\alpha,\mathbb{Q}} \in (\mathbb{Z}/p\mathbb{Z})[X]$. Supposons Q et Q' premiers entre eux. D'après Bezout il existe $U, V \in (\mathbb{Z}/p\mathbb{Z})[X]$ tels que $UQ + VQ' = 1$. Soient $\widetilde{U}, \widetilde{V}, \widetilde{Q}$ et $\widetilde{Q'} \in \mathbb{Z}[X]$ des relevés respectifs de U, V, Q et Q'. On a donc $\widetilde{U}\widetilde{Q} + \widetilde{V}\widetilde{Q'} - 1 \in p\mathbb{Z}[X]$. Évaluée en α cette relation montre que $(\widetilde{Q}(\alpha), \widetilde{Q'}(\alpha)) = A$. Mais

$$\mathrm{I}(Q)\mathrm{I}(Q') = (p, \widetilde{Q}(\alpha))(p, \widetilde{Q'}(\alpha)) = p^2A + p(\widetilde{Q}(\alpha), \widetilde{Q'}(\alpha)) + \widetilde{Q}(\alpha)\widetilde{Q'}(\alpha)A.$$

Ainsi, $\mathrm{I}(Q)\mathrm{I}(Q') = (p, \widetilde{Q}(\alpha)\widetilde{Q'}(\alpha)) = \mathrm{I}(QQ')$.

(ii) Le (i) s'applique récursivement et montre que $\prod_{i=1}^{g} \mathrm{I}(Q_i) = \mathrm{I}(\prod_{i=1}^{g} Q_i) = \mathrm{I}(P) = pA$.