Autour des anneaux d'entiers quadratiques

Travaux dirigés du 2 et du 5 décembre 2025

Rappels (voir l'exercice 7 du TD précédent pour les preuves)

Soit $d \in \mathbb{Z}$ non carré, soit $\sqrt{d} \in \mathbb{C}$ une racine carrée de d (pour fixer les idées on suppose $\sqrt{d} \in \mathbb{R}_+^* \cup i\mathbb{R}_+^*$). On considère les sous-anneaux de $\mathbb{C}$

$$\mathbb{Z}[\sqrt{d}] := \mathbb{Z} + \mathbb{Z}\sqrt{d} \quad \text{et} \quad \mathbb{Q}[\sqrt{d}] := \mathbb{Q} + \mathbb{Q}\sqrt{d}.$$

Pour $x, y \in \mathbb{Q}$, et $z := x + y\sqrt{d}$, on pose

$$\overline{z} := x - y\sqrt{d} \quad \text{et} \quad \mathrm{N}(z) := z\overline{z} = x^2 - dy^2,$$

on dit que $\overline{z}$ est le *conjugué* de z et que $\mathrm{N}(z)$ est la *norme* de z. Alors $z \mapsto \overline{z}$ est un automorphisme des anneaux $\mathbb{Q}[\sqrt{d}]$ et $\mathbb{Z}[\sqrt{d}]$, les éléments de $\mathbb{Q}[\sqrt{d}]$ sont les a/b avec $a, b \in \mathbb{Z}[\sqrt{d}]$ et $b \neq 0$, et $\mathrm{N} : \mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times$ est un morphisme de groupes qui vérifie $\mathrm{N}(\mathbb{Z}[\sqrt{d}]) \subseteq \mathbb{Z}$. On en déduit

$$\mathbb{Z}[\sqrt{d}]^\times = \{z \in \mathbb{Z}[\sqrt{d}] \mid \mathrm{N}(z) = \pm 1\},$$

d'où $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ et $\mathbb{Z}[\sqrt{d}]^\times = \{\pm 1\}$ pour $d < -1$. Dans le cas $d > 0$, on peut montrer que $\mathbb{Z}[\sqrt{d}]^\times$ est infini, que tout élément > 1 de $\mathbb{Z}[\sqrt{d}]^\times$ est de la forme $x + y\sqrt{d}$ avec $x, y \geq 1$, qu'il existe un unique plus petit tel élément η_d (appelé *unité fondamentale* de $\mathbb{Z}[\sqrt{d}]$), et qu'on a $\mathbb{Z}[\sqrt{d}]^\times = \langle -1, \eta_d \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Exercice 1. Exemples et contre-exemples

Soit $d \in \mathbb{Z}$ non carré.

1. Montrer que si $\pi \in \mathbb{Z}[\sqrt{d}]$ est de norme irréductible dans $\mathbb{Z}$, alors π est irréductible dans $\mathbb{Z}[\sqrt{d}]$.
2. En justifiant que les éléments de norme 4 de $\mathbb{Z}[\sqrt{-3}]$ sont irréductibles, montrer que la réciproque à l'assertion de la question précédente est fausse.
3. *(Un élément irréductible mais pas premier)* Montrer que 2 n'est pas premier dans $\mathbb{Z}[\sqrt{-3}]$.
4. Montrer que $\mathbb{Z}[\sqrt{d}]$ vérifie la propriété de factorisation.
5. *(Un anneau non factoriel qui vérifie la propriété de factorisation)* Montrer que l'anneau $\mathbb{Z}[\sqrt{-3}]$ n'est pas factoriel.
6. Montrer que pour $d \in \{-2, -1, 2\}$, l'anneau $\mathbb{Z}[\sqrt{d}]$ est euclidien pour $|\mathrm{N}|$ (donc principal, donc factoriel).

Exercice 2. Noethérianité de tous

Soient $d \in \mathbb{Z}$ non carré et $A = \mathbb{Z}[\sqrt{d}]$.

1. Montrer que tout idéal non nul I de A contient un entier $n \in \mathbb{N}^*$.
2. Montrer qu'il n'y a qu'un nombre fini d'idéaux de A contenant un entier $n \in \mathbb{N}^*$ donné.
3. Montrer que A est noethérien, et que tout idéal non nul y est d'indice fini.
4. Montrer que A n'a qu'un nombre fini d'idéaux principaux zA avec $\mathrm{N}(z)$ fixé.

Exercice 3. Non-principalité de certains

On se propose de montrer que $\mathbb{Z}[\sqrt{d}]$ est non principal pour $d < -2$. On pose $\alpha = \sqrt{d}$ si d est pair, $\alpha = 1 + \sqrt{d}$ sinon.

1. Traiter directement les cas $d = -3, -4$.
2. Montrer $(2, \alpha) = 2\mathbb{Z} + \alpha\mathbb{Z}$.
3. Montrer que pour $d < -4$, les éléments de $\mathbb{Z}[\sqrt{d}]$ de norme $\leqslant 4$ sont 0, ± 1, ± 2.
4. En déduire que l'idéal $(2, \alpha)$ n'est pas principal.

Exercice 4. Étude des idéaux dans des cas non principaux

Soit A est un anneau commutatif intègre. Si I et J sont deux idéaux non nuls de A, on dira que I et J sont *équivalents*, et on notera $I \sim J$, s'il existe $a, b \in A - \{0\}$ avec $aI = bJ$. C'est clairement une relation d'équivalence sur les idéaux non nuls de A, dont on notera $\mathrm{Cl}(A)$ l'ensemble des classes.

1. Montrer qu'un idéal non nul de A est principal si, et seulement si, il est équivalent à A.
2. En déduire que A est principal si, et seulement si, on a $|\mathrm{Cl}(A)| = 1$.

On considère $A = \mathbb{Z}[\sqrt{d}]$ avec $-7 \leqslant d \leqslant -3$.

3. Soit $t \in \mathbb{R}$ avec $0 < t < 1+\sqrt{3}$. Montrer que pour tout $z \in \mathbb{C}$, il existe $v \in \mathbb{Z}+\mathbb{Z}\,i\,t$ avec soit $|z-v| < 1$, soit $|z-v/2| < 1/2$.
4. En déduire que pour tout $a, b \in A$ avec $b \neq 0$, il existe des éléments $q, r \in A$ avec $\mathrm{N}(r) < \mathrm{N}(b)$ et soit $a = qb + r$, soit $2a = qb + r$.
5. Montrer que tout idéal non nul de A est équivalent à un idéal contenant $2A$.
6. Montrer que les idéaux de A contenant $2A$ sont $2A$, J et A, où J est l'idéal $(2, \alpha)$ comme défini dans l'exercice 3 (on rappelle que J n'est pas principal pour $d < -4$).
7. Démontrer $\mathrm{Cl}(A) = \{[A], [J]\}$ et que J est non équivalent à A.

Exercice 5. Une équation diophantienne

Soient $x, y \in \mathbb{Z}$ tels que $y^2 = x^3 - 2$. Considérons la factorisation

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$$

dans $\mathbb{Z}[\sqrt{-2}]$. On a vu à l'exercice 1 que ce dernier est euclidien, donc principal et factoriel.

1. Vérifier que $y + \sqrt{-2}$ et $y - \sqrt{-2}$ sont premiers entre eux dans $\mathbb{Z}[\sqrt{-2}]$.
2. Justifier que si dans un anneau factoriel A, on a une relation $a^n = bc$ avec b et c premiers entre eux et $n \geqslant 1$, alors il existe $d \in A$ et $u \in A^\times$ tels que $b = d^n u$.
3. En déduire les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation $y^2 = x^3 - 2$.

Exercice 6. Irréductibles de l'anneau des entiers de Gauss

On se propose d'étudier les irréductibles de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss.

1. Montrer que tout irréductible de $\mathbb{Z}[i]$ divise un et un seul nombre premier $p \in \mathbb{Z}$ usuel.

Soit donc $p \in \mathbb{Z}$ un nombre premier usuel.

2. Si $p = 2$, montrer qu'on a $2 = -i(1+i)^2$ avec $1 + i$ irréductible (de norme 2).
3. Si $p \equiv 3 \bmod 4$, montrer que p est irréductible dans $\mathbb{Z}[i]$ (de norme p^2),
4. Si $p \equiv 1 \bmod 4$, montrer qu'on a $p = \pi\overline{\pi}$ avec π et $\overline{\pi}$ des irréductibles de $\mathbb{Z}[i]$ non associés (de norme p).

On va maintenant présenter des applications de la classification des irréductibles de $\mathbb{Z}[i]$ que l'on vient d'établir.

5. Factoriser $-3 + 15i$ et $4 + 7i$ en irréductibles dans $\mathbb{Z}[i]$.
6. Trouver tous les $(x, y) \in \mathbb{Z}^2$ avec $y^2 = x^3 - 1$.
7. Montrer que tout nombre premier $p \equiv 1 \bmod 4$ s'écrit de manière unique sous la forme $p = a^2 + b^2$ avec $a, b \in \mathbb{N}$.

Pour finir, on présente un choix de représentants des irréductibles de $\mathbb{Z}[i]$.

8. Montrer que 4 et $2(1+i)$ forment une $\mathbb{Z}$-base de l'idéal $(2+2i)$ de $\mathbb{Z}[i]$.
9. En déduire un isomorphisme de groupes abéliens bien défini $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[i]/(2+2i)$, $(\overline{a}, \overline{b}) \mapsto \overline{a+bi}$. À quelle condition sur $a, b \in \mathbb{Z}$ a-t-on $a + bi \equiv 3 \bmod 2 + 2i$?
10. On munit $A := \mathbb{Z}[i]/(2+2i)$ de sa structure d'anneau quotient. Montrer que l'application naturelle $\mathbb{Z}[i]^\times \to A^\times$ est un isomorphisme de groupes.
11. Montrer que l'ensemble des irréductibles de $\mathbb{Z}[i]$ de la forme $1 + i$, ou congrus à 3 modulo $2 + 2i$, est un système de représentants de tous les irréductibles.