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 $\mathbb{Z}[\sqrt{d}]$.

   Si on a $\pi = ab$, on déduit du fait que $\pm\mathrm{N}(\pi)$ est un nombre premier que $\mathrm{N}(a) = \pm 1$ ou $\mathrm{N}(b) = \pm 1$ et donc a ou $b \in \mathbb{Z}[\sqrt{d}]^\times$.

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.

   On rappelle que les unités de $\mathbb{Z}[\sqrt{-3}]$ sont ± 1. Comme $x^2 + 3y^2 = 2$ n'a pas de solution $(x, y) \in \mathbb{Z}^2$, il n'y a pas d'élément $a \in \mathbb{Z}[\sqrt{-3}]$ de norme ± 2. On en déduit que les éléments de norme 4 de $\mathbb{Z}[\sqrt{-3}]$ sont irréductibles : ce sont les 6 éléments $\pm 2, \pm(1 + \sqrt{3})$ et $\pm(1 - \sqrt{3})$.

3. *(Un élément irréductible mais pas premier)* Montrer que 2 n'est pas premier dans $\mathbb{Z}[\sqrt{-3}]$.

   L'élément 2 de $\mathbb{Z}[\sqrt{-3}]$ ne divise pas $1 \pm \sqrt{-3}$, car sinon on aurait $1 \pm \sqrt{-3} = 2(x + y\sqrt{-3}) = 2x + 2y\sqrt{-3}$ et donc $2x = \pm 1$ et $2y = \pm 1$ avec $x, y \in \mathbb{Z}$: absurde. Pourtant il divise $2.2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$: il n'est donc pas premier.

4. Montrer que $\mathbb{Z}[\sqrt{d}]$ vérifie la propriété de factorisation.

   Vérifions par récurrence sur l'entier $|\mathrm{N}(a)| \geq 1$ que tout $a \in A$ non nul est produit fini d'irréductibles et d'une unité. Si a est une unité (i.e. $|\mathrm{N}(a)| = 1$) ou est irréductible, il y a rien à démontrer. Sinon, on a $a = bc$ avec $1 < |\mathrm{N}(b)|, |\mathrm{N}(c)| < |\mathrm{N}(a)|$. Ainsi, b et c sont produits finis d'irréductibles et d'unités, et donc $a = bc$ également.

5. *(Un anneau non factoriel qui vérifie la propriété de factorisation)* Montrer que l'anneau $\mathbb{Z}[\sqrt{-3}]$ n'est pas factoriel.

   On a $2.2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$ alors que $2, 1 + \sqrt{-3}$ et $1 - \sqrt{-3}$ sont irréductibles deux à deux non associés.

6. Montrer que pour $d \in \{-2, -1, 2\}$, l'anneau $\mathbb{Z}[\sqrt{d}]$ est euclidien pour $|\mathrm{N}|$ (donc principal, donc factoriel).

   Observons qu'il suffit de montrer que pour tout $t \in \mathbb{Q}[\sqrt{d}]$, il existe $q \in \mathbb{Z}[\sqrt{d}]$ avec $|\mathrm{N}(t - q)| < 1$. En effet, si on a $a, b \in \mathbb{Z}[\sqrt{d}]$ avec $a, b \neq 0$, appliquant ceci à $t = a/b \in \mathbb{Q}[\sqrt{d}]$ il existe $q \in \mathbb{Z}[\sqrt{d}]$ avec $|\mathrm{N}(a/b - q)| < 1$. Par multiplicativité de la norme, on a $|\mathrm{N}(a - bq)| < |\mathrm{N}(b)|$ puis $r := a - qb$ convient.

   Pour montrer l'observation on écrit $t = x + y\sqrt{d}$ avec $x, y \in \mathbb{Q}$. Il existe $u, v \in \mathbb{Z}$ avec $|u - x| \leq 1/2$ et $|v - y| \leq 1/2$. Posons $q = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. On a bien $|\mathrm{N}(t - q)| \leq (x - u)^2 + |d|(y - v)^2 \leq \frac{1+|d|}{4} < 1$ pour $|d| < 3$.

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 $n \in \mathbb{N}^*$.

   Soit $z \in I$ non nul. On constate $\mathrm{N}(z) = \overline{z}z \in I$. Mais $\mathrm{N}(z)$ est un entier non nul.

2. Montrer qu'il n'y a qu'un nombre fini d'idéaux de A contenant un entier $n \in \mathbb{N}^*$ donné.
   Comme on a $\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}^2$, on a aussi $\mathbb{Z}[\sqrt{d}]/n\mathbb{Z}[\sqrt{d}] \simeq (\mathbb{Z}/n\mathbb{Z})^2$. En particulier, c'est un groupe fini, et il n'a donc qu'un nombre fini de sous-groupes. On conclut car les sous-groupes de $\mathbb{Z}[\sqrt{d}]/n\mathbb{Z}[\sqrt{d}]$ sont en bijection naturelle avec ceux de $\mathbb{Z}[\sqrt{d}]$ contenant $n\mathbb{Z}[\sqrt{d}]$ (dont les idéaux contenant n font partie).
3. Montrer que A est noethérien, et que tout idéal non nul y est d'indice fini.
   Soit I un idéal non nul de A. On a vu que I contient $(n) = nA$ pour un certain entier $n \geqslant 1$. Observons que les sous-groupes de $\mathbb{Z}^2$ contenant $n\mathbb{Z}^2$ sont clairement de type fini, engendrés par $(n,0)$, $(0,n)$ et par un sous-ensemble de l'ensemble fini des (a,b) avec $0 \leqslant a,b < n$. On en déduit que tout idéal de A (isomorphe à $\mathbb{Z}^2$ comme groupe abélien) est finiment engendré comme groupe abélien, et donc a fortiori de type fini comme idéal. On a $nA \subseteq I$ et nA d'indice fini dans A, donc I est d'indice fini dans A (en clair, on a une surjection $A/nA \to A/I$).
4. Montrer que A n'a qu'un nombre fini d'idéaux principaux zA avec $\mathrm{N}(z)$ fixé.
   On peut supposer $\mathrm{N}(z)$ non nul. On a $z \in zA$ donc $\mathrm{N}(z) \in zA$ et on a vu qu'il n'y a qu'un nombre fini d'idéaux de A contenant $\mathrm{N}(z)$.

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 $d = -3, -4$.
   On a vu à la question 5 de l'exercice 1 que $\mathbb{Z}[\sqrt{-3}]$ est non factoriel, donc non principal, en examinant l'identité $2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$. De même, $\mathbb{Z}[\sqrt{-4}] = \mathbb{Z} + 2\mathbb{Z}i$ est non factoriel à cause de l'identité $2 \cdot 2 = -(2i)(2i)$. En effet, $\mathbb{Z}[\sqrt{-4}]$ n'a pas d'élément de norme ± 2, puisque $x^2 + 4y^2 = \pm 2$ n'a aucune solution $x, y \in \mathbb{Z}$. Cela montre que ± 2 et $\pm 2i$ sont irréductibles. Ils sont non associés car les inversibles de $\mathbb{Z}[2i]$ sont ± 1 (bien noter que $\pm i$ n'est pas dans $\mathbb{Z}[2i]$).
2. Montrer $(2,\alpha) = 2\mathbb{Z} + \alpha\mathbb{Z}$.
   On a $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\alpha$. Ainsi, l'idéal $(2,\alpha) = 2(\mathbb{Z}+\alpha\mathbb{Z}) + \alpha(\mathbb{Z}+\alpha\mathbb{Z})$ est engendré comme groupe abélien par $2, \alpha, 2\alpha$ et α^2. Mais les éléments 2α et α^2 sont dans $2\mathbb{Z}+\alpha\mathbb{Z}$ (si d est pair on a $\alpha^2 = d$, et si d est impair on a $\alpha^2 = d-1+2(1+\sqrt{d})$). On a donc bien $(2,\alpha) = 2\mathbb{Z} + \alpha\mathbb{Z}$.
3. Montrer que pour $d < -4$, les éléments de $\mathbb{Z}[\sqrt{d}]$ de norme $\leqslant 4$ sont $0, \pm 1, \pm 2$.
   L'équation $x^2 - dy^2 \leqslant 4$ avec $x, y \in \mathbb{Z}$ implique bien $y = 0$ et $x = 0$, 1 ou 2.
4. En déduire que l'idéal $(2,\alpha)$ n'est pas principal.
   On déduit de la question 2 que l'on a $(2,\alpha) \neq \mathbb{Z}[\sqrt{d}]$, car 1 n'est pas de la forme $2n + \alpha m$ avec $m, n \in \mathbb{Z}$ (on aurait $m = 0$). Ainsi, si on suppose $(2,\alpha) = (z)$ avec $z \in \mathbb{Z}[\sqrt{d}]$ on a $\mathrm{N}(z) > 1$. Mais on a aussi $z \mid 2$ car $2 \in (z)$, et donc $\mathrm{N}(z) \mid \mathrm{N}(2) = 4$ dans $\mathbb{Z}$. D'après la question précédente, cela implique $z = \pm 2$. Mais on a aussi $z \mid \alpha$ car $\alpha \in (z)$. Mais il est clair que 2 ne divise pas α (les multiples de 2 dans $\mathbb{Z}+\mathbb{Z}\alpha$ ont leurs coefficients en 1 et α qui sont des entiers pairs).

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.
   Si on a $I = xA$ avec $x \neq 0$ alors on a $I \sim A$. Réciproquement, si on a $aI = bA$ avec a, b non nuls, on a $b \in aI \subseteq aA$ et donc $b = ac$ pour un certain $c \in A$, puis $aI = acA$, et comme A est intègre, $I = cA$ est principal.
2. En déduire que A est principal si, et seulement si, on a $|\mathrm{Cl}(A)| = 1$.
   On a toujours $[A] \in \mathrm{Cl}(A)$, et par la question précédente A est principal si et seulement si on a $\mathrm{Cl}(A) = \{[A]\}$.

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 $v \in \mathbb{Z}+\mathbb{Z}it$ avec soit $|z-v| < 1$, soit $|z - v/2| < 1/2$.
   Soit $z \in \mathbb{C}$, on écrit $z = x + ity$ avec x et y des réels. On cherche v de la forme $a + itb$ avec a et b des entiers relatifs. On peut toujours trouver $a \in \{\lfloor x \rfloor, \lfloor x \rfloor + 1\}$ tel que $|x-a| \leq 1/2$. On veut majorer $|y-b|$ plus finement. Supposons qu'on puisse avoir $|y-b| < r$ pour un $r > 0$ que l'on déterminera plus tard. On a alors

$$|z-v|^2 = (x-a)^2 + t^2(y-b)^2 < 1/4 + t^2r^2,$$

ce qui implique $|z-v|<1$ si on prend $r=\sqrt{3}/(2t)$, ce que l'on fait. Si maintenant on ne peut pas trouver un entier b tel que $|y-b|<r$, alors y est loin de $\mathbb{Z}$ donc proche de $1/2+\mathbb{Z}$; en effet on a

$$y \in [\lfloor y\rfloor + r, \lfloor y\rfloor + 1 - r] = [(\lfloor y\rfloor + 1/2) - (1/2-r), (\lfloor y\rfloor + 1/2) + (1/2-r)].$$

Donc on trouve $b = 2\lfloor y\rfloor + 1 \in \mathbb{Z}$ tel que $|y-b/2| < 1/2-r$. Comme plus haut, on trouve aussi $a \in \{2\lfloor x\rfloor, 2(\lfloor x\rfloor+1)\}$ tel que $|x-a/2| \leq 1/2$. On a donc

$$|z-v/2|^2 = (x-a/2)^2 + t^2(y-b/2)^2 < 1/4 + t^2(1/2-r)^2 = (1+(t-\sqrt{3})^2)/4,$$

et on conclut puisque $(t-\sqrt{3})^2 < 3$.

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 $2a = qb+r$.
   On a $3 < 2\sqrt{3}$ et donc $\sqrt{|d|} \leqslant \sqrt{7} < 1+\sqrt{3}$. On pose $z = a/b$. Par la question précédente, il existe $q \in A$ avec soit $\mathrm{N}(a/b-q) < 1$, soit $\mathrm{N}(a/b-q/2) < 1/4$. On a $\mathrm{N}(r) < \mathrm{N}(b)$ avec $r = a-qb$ dans le premier cas, et $r = 2a-qb$ dans le second.
5. Montrer que tout idéal non nul de A est équivalent à un idéal contenant $2A$.
   On choisit $z \in I$ non nul et avec $\mathrm{N}(z) \in \mathbb{N}^*$ minimal. On a $Az \subseteq I$ car I est un idéal. Soit $a \in I$ non nul. Par la question précédente, on peut écrire soit $a = qz+r$, soit $2a = qz+r$, avec $\mathrm{N}(r) < \mathrm{N}(z)$. On a $r \in I$ et donc $r = 0$ dans les deux cas, par choix de z. On a donc $2I \subseteq Az$. On a montré $zA \subseteq I \subseteq \frac{1}{2}zA$. En multipliant ces inclusions par l'élément $\frac{2}{z} \in \mathbb{Q}[\sqrt{d}]^\times$, elles s'écrivent aussi $2A \subseteq I' \subseteq A$ avec $I' = \frac{2}{z}I$, qui est donc un idéal non nul de A. Il vérifie $zI' = 2I$: il est équivalent à I.
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 $d < -4$).
   Soit I un idéal de A contenant $2A$. On a $A = \mathbb{Z} \oplus \mathbb{Z}\alpha$. Le groupe quotient $A/2A \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ a donc pour représentants $0, 1, \alpha, \alpha+1$. Si I contient 1 on a $I = A$. Si I contient α on a $J \subseteq I$, puis $I = J$ ou $I = A$ car J est d'indice 2 . Enfin, si I contient $\alpha+1$, alors I contient aussi $\alpha(\alpha+1) = \alpha^2+\alpha$. Si d est pair on a $\alpha^2 = d \in 2\mathbb{Z} \subseteq I$, donc I contient α, puis $1 = 1+\alpha-\alpha$, et donc $I = A$. De même, si d est impair on a $\alpha^2 = 2\alpha + d - 1$ et donc $\alpha(\alpha+1)+\alpha = 3\alpha + d - 1 \in \alpha + 2A$, et donc $\alpha \in I$ puis encore $1 \in I$ et donc $I = A$.
7. Démontrer $\mathrm{Cl}(A) = \{[A], [J]\}$ et que J est non équivalent à A.
   D'après les deux questions précédentes, tout idéal non nul de A est équivalent à $2A$, J ou A. Comme A et $2A$ sont principaux, on a $\mathrm{Cl}(A) = \{[A], [J]\}$. On en déduit que l'idéal J est équivalent à A si et seulement si A est principal, par la question 2. On sait que J n'est pas principal pour $d < -4$. Pour $d = -3$, on a vu que A est non factoriel en cours, donc non principal, donc J est non équivalent à A aussi dans ce cas.

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 $\mathbb{Z}[\sqrt{-2}]$.
   Il suffit de voir qu'il n'y a pas d'irréductible π divisant $y+\sqrt{-2}$ et $y-\sqrt{-2}$. Mais un tel π diviserait $2\sqrt{-2} = -\sqrt{-2}^3$, et donc $\sqrt{-2}$ (car π est également premier), et donc y. Mais alors $\mathrm{N}(\sqrt{-2}) = 2$ diviserait $\mathrm{N}(y) = y^2$ dans $\mathbb{Z}$: absurde car y est impair (2 n'est pas un cube dans $\mathbb{Z}/4\mathbb{Z}$).
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 $b = d^n u$.
   On décompose a, b et c en irréductibles et on utilise la propriété d'unicité.
3. En déduire les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation $y^2 = x^3 - 2$.
   On déduit de la question précédente et du fait que $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$ l'existence de $z \in \mathbb{Z}[\sqrt{-2}]$ tel que $y+\sqrt{-2} = \pm z^3 = (\pm z)^3$. Posons $\pm z = u + v\sqrt{-2}$ avec $u, v \in \mathbb{Z}$. On a donc

$$y+\sqrt{-2} = (u+v\sqrt{-2})^3 = u^3 - 6uv^2 + \left(3u^2v - 2v^3\right)\sqrt{-2}$$

   En prenant la coordonnée en $\sqrt{-2}$, il vient $1 = v\left(3u^2 - 2v^2\right)$, d'où l'on tire $v = \pm 1$ puis $3u^2 = v + 2$ et donc $v = 1$ et $u = \pm 1$. On a donc $y = u^3 - 6uv^2 = \pm 5$, puis $x^3 = 27$, et donc nécessairement $x = 3$, ce qui conclut ! Les seules solutions $(x, y) \in \mathbb{Z}^2$ de l'équation $y^2 = x^3 - 2$ sont $(3, 5)$ et $(3, -5)$.

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 π un irréductible de $\mathbb{Z}[i]$. Alors $n := \mathrm{N}(\pi) = \pi\overline{\pi}$ est un entier $n > 1$. Comme π est premier, car $\mathbb{Z}[i]$ est principal, il divise donc dans $\mathbb{Z}[i]$ l'un des facteurs premiers de n dans $\mathbb{Z}$. Soit p un tel facteur. On a $p = \pi\eta$ avec $\eta \in \mathbb{Z}[i]$. On en déduit $p^2 = \mathrm{N}(\pi)\mathrm{N}(\eta)$, puis $\mathrm{N}(\pi) = p$ ou p^2. Cela montre que p est uniquement déterminé par π, d'où l'unicité.

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).

   L'irréductibilité de $1+i$ découle de la question 1 de l'exercice 1.

3. Si $p \equiv 3 \bmod 4$, montrer que p est irréductible dans $\mathbb{Z}[i]$ (de norme p^2),

   Supposons $p \equiv 3 \bmod 4$. Si p n'est pas irréductible, on peut écrire $p = \alpha\beta$ avec α, β dans $\mathbb{Z}[i]$ de normes > 1. Comme on a $\mathrm{N}(p) = p^2 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, on a donc $\mathrm{N}(\alpha) = p$. Écrivant $\alpha = a + bi$ avec $a, b \in \mathbb{Z}$ on a alors $p = a^2 + b^2$. Comme p est impair, alors a et b n'ont pas même parité, et donc on a $p \equiv 1 \bmod 4$: contradiction.

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).

   Supposons enfin $p \equiv 1 \bmod 4$. Montrons que p n'est pas irréductible. On va utiliser le fait que -1 est un carré modulo p (en effet, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique donc admet un élément α d'ordre $p-1$; on a dans $\mathbb{Z}/p\mathbb{Z}$ l'égalité $0 = \alpha^{p-1} - 1 = (\alpha^{(p-1)/2} - 1)(\alpha^{(p-1)/2} + 1)$, donc $-1 = \alpha^{(p-1)/2} = \left(\alpha^{(p-1)/4}\right)^2$ est un carré). Il existe donc $n \in \mathbb{Z}$ tel que p divise $n^2 + 1$. On a la décomposition $n^2 + 1 = (n+i)(n-i)$ dans $\mathbb{Z}[i]$. Si p était irréductible dans $\mathbb{Z}[i]$, il serait premier (car $\mathbb{Z}[i]$ est factoriel), et on aurait donc $p \mid n+i$ ou $p \mid n-i$ dans $\mathbb{Z}[i]$. C'est absurde car $p\mathbb{Z}[i]$ est l'ensemble des $a + bi$ avec $a \in p\mathbb{Z}$ et $b \in p\mathbb{Z}$, et $n \pm i$ n'a pas cette propriété. On en déduit $p = \alpha\beta$ avec α, β non inversibles, puis $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = p$ comme à la question précédente. Posons $\pi = \alpha = a + bi$. On a montré $p = \mathrm{N}(\pi) = a^2 + b^2$, et donc que p est somme de deux carrés. En outre π est irréductible car de norme première, et $p = \pi\overline{\pi}$ est donc sa décomposition en irréductibles. Il ne reste qu'à voir que π et $\overline{\pi}$ sont non associés. Mais comme on a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, les associés de $\pi = a + bi$ sont $a + bi, -a - bi, -b + ai$ et $b - ai$. Cette liste contient $\overline{\pi} = a - bi$ si et seulement si $b = 0$, $a = 0$ ou encore $a = \pm b$, et donc $p \in \{a^2, b^2, 2a^2\}$: aucune de ces solutions n'est possible (on a $p > 2$).

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 $\mathbb{Z}[i]$.

   Les irréductibles de $\mathbb{Z}[i]$ sont de norme 2 (pour $1+i$), ou p premier $\equiv 1 \bmod 4$ (pour π et $\overline{\pi}$ dans l'écriture $p = \pi\overline{\pi}$), ou p^2 avec $p \equiv 3 \bmod 4$. On a donc une bonne idée de la factorisation en irréductibles d'un $z \in \mathbb{Z}[i]$ en factorisant d'abord $\mathrm{N}(z)$ dans $\mathbb{Z}$.

   On a $-3 + 15i = 3(-1 + 5i)$ et 3 est irréductible dans $\mathbb{Z}[i]$ donc on se ramène à décomposer $-1 + 5i$ en irréductibles. On a $\mathrm{N}(-1 + 5i) = 1 + 25 = 26 = 2 \cdot 13$. On sait que $1 + i$ doit diviser $-1 + 5i$, et c'est bien le cas

   $$\frac{-1+5i}{1+i} = \frac{1}{2}(-1+5i)(1-i) = \frac{1}{2}(4+6i) = 2+3i.$$

   De plus $2 + 3i$ est irréductible (de norme 13), on a donc la décomposition en irréductibles $-3 + 15i = 3(1+i)(2-3i)$.

   De même, on a $\mathrm{N}(4 + 7i) = 16 + 49 = 65 = 5 \cdot 13$. On a $5 = 1^2 + 2^2 = (1+2i)(1-2i)$, et les deux irréductibles de $\mathbb{Z}[i]$ de norme 5 sont donc les associés de $1 \pm 2i$. Un seul des deux divise $4 + 7i$. On a en effet

   $$\frac{4+7i}{1+2i} = \frac{1}{5}(4+7i)(1-2i) = \frac{1}{5}(18-i), \text{ et}$$
   $$\frac{4+7i}{1-2i} = \frac{1}{5}(4+7i)(1+2i) = \frac{1}{5}(-10+15i) = -2+3i.$$

   On a donc la décomposition en irréductibles $4 + 7i = (1-2i)(-2+3i)$ dans $\mathbb{Z}[i]$. On aurait pu éviter tout calcul en observant que l'on a $4 + 7i \equiv -1 + 2i \bmod 5\mathbb{Z}[i]$, et donc c'est $1 - 2i$ qui divise $4 + 7i$ (car il divise 5).

6. Trouver tous les $(x, y) \in \mathbb{Z}^2$ avec $y^2 = x^3 - 1$.

   On va montrer que la seule solution est $(x, y) = (1, 0)$. Soit $(x, y) \in \mathbb{Z}^2$ avec $y^2 = x^3 - 1$. On a dans $\mathbb{Z}[i]$ la relation $x^3 = y^2 + 1 = (y-i)(y+i)$. Vérifions que $y - i$ et $y + i$ sont premiers entre eux dans $\mathbb{Z}[i]$.

   Sinon, il existe un irréductible π de $\mathbb{Z}[i]$ divisant $y + i$ et $y - i$. On a alors $\pi \mid (y+i) - (y-i) = 2i$, donc π divise 2, puis $\pi \sim 1 + i$ (car on a $2 = -i(1+i)^2$) et $\mathrm{N}(\pi) = 2$. Mais comme π divise $y^2 + 1 = x^3$, on a que $2 = \mathrm{N}(\pi)$ divise x^6, et donc x est pair. C'est absurde car alors on a $y^2 \equiv -1 \bmod 4$.

Comme $\mathbb{Z}[i]$ est factoriel, on en déduit comme à l'exercice 5 que l'on a $y+i = uz^3$ avec $z \in \mathbb{Z}[i]$ et $u \in \mathbb{Z}[i]^\times$. On a $u^4 = 1$, donc $y+i = (u^{-1}z)^3$. Écrivons $u^{-1}z = a+bi$ avec $a, b \in \mathbb{Z}$. On a donc

$$y+i = (a+bi)^3 = \left(a^3 - 3ab^2\right) + \left(3ba^2 - b^3\right) i$$

puis $1 = b\left(3a^2 - b^2\right)$. Cela entraîne $b = \pm 1$, puis $3a^2 = 1+b$, $b = -1$, $a = 0$, $y = 0$ puis $x = 1$.

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 $a, b \in \mathbb{N}$.

   Soit p premier $\equiv 1 \bmod 4$. On a vu que la décomposition en irréductibles de p dans $\mathbb{Z}[i]$ est $p = \pi\overline{\pi}$, avec π et $\bar{\pi}$ des irréductibles (non associés). En particulier, posant $\pi = a+bi$, on a $p = a^2 + b^2$.

   Supposons maintenant que l'on a $x, y \in \mathbb{Z}$ avec $x^2 + y^2 = p$. L'élément $z = x + iy$ vérifie donc $\mathrm{N}(z) = p = z\overline{z}$. C'est donc un facteur irréductible (car de norme première) de p dans $\mathbb{Z}[i]$. Par factorialité de $\mathbb{Z}[i]$, les seules possibilités sont donc $z \sim \pi$ ou $z \sim \overline{\pi}$. Mais on a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, de sorte que les 4 associés de π sont $a+bi, -a-bi, -b+ai$ et $b-ai$, et ceux de $\overline{\pi}$ sont $a-bi, -a+bi, -b-ai$, et $b+ai$. Au final, on a bien $(x, y) = (\pm a, \pm b)$ ou $(\pm b, \pm a)$.

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 $\mathbb{Z}[i]$.

   Comme 1 et i forment une $\mathbb{Z}$-base de $\mathbb{Z}[i]$, le groupe abélien sous-jacent à $(2+2i)$ est engendré par $2+2i$ et par $i(2+2i) = -2+2i$, ou ce qui revient au même par 4 et $2+2i$. Ces deux éléments sont $\mathbb{R}$-linéairement indépendants, donc $\mathbb{Z}$-libres.

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 $a+bi \equiv 3 \bmod 2+2i$?

   Comme 1 et $1+i$ forment une $\mathbb{Z}$-base de $\mathbb{Z}[i]$, et comme $c + d(1+i)$ est dans $(2+2i)$ si, et seulement si, on a $c \equiv 0 \bmod 4$ et $d \equiv 0 \bmod 2$ par la question précédente, on en déduit que le morphisme de groupes additifs $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}[i]/(2+2i)$, $(\overline{a}, \overline{b}) \mapsto \overline{c+d(1+i)}$, qui est bien défini et surjectif, est un isomorphisme. Pour la condition demandée dans l'énoncé, on écrit $a+bi = a-b+b(1+i)$ et on a donc $b \equiv 0 \bmod 2$ et $a-b \equiv 3 \bmod 4$.

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.

    On note $f : \mathbb{Z}[i] \to A$ la projection canonique (un morphisme d'anneaux). Posons $\varepsilon = f(1+i)$. On a $i(2+2i) = (1+i)^3$ dans $\mathbb{Z}[i]$, et donc $\varepsilon^3 = 0$ en appliquant f. On a aussi $(1+i)\mathbb{Z}[i] = 2\mathbb{Z} + (1+i)\mathbb{Z}$, et donc εA est l'ensemble des classes des $c + d(1+i)$ avec c pair. Il y a 4 tels éléments, tous non inversibles car $\varepsilon^3 = 0$. Les 4 éléments restants sont ± 1 et $\pm 1 + \varepsilon \equiv \pm i$.

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.

    Soit π un irréductible de $\mathbb{Z}[i]$ non associé à $1+i$. On sait alors qu'il est premier à $1+i$, et donc par Bézout qu'il existe $u, v \in \mathbb{Z}[i]$ avec $u\pi + v(1+i) = 1$. En appliquant f on en déduit que $f(u)f(\pi) + \varepsilon f(v) = 1$. Comme on a vu à la question précédente que $A^\times = A - \varepsilon A$ avec ε la classe de $1+i$ dans A, on a donc $f(u)f(\pi) \in A^\times$ et donc $f(\pi)$ est inversible dans A. D'après la question précédente, il existe ainsi une unique unité w de $\mathbb{Z}[i]$ tel que $f(w\pi) = f(w)f(\pi) \equiv -1 \bmod (2+2i)$ (noter que l'on a $3 \equiv -1$ dans A). Ainsi, $w\pi$ est l'unique associé de π qui est congru à 3 modulo $(2+2i)$.