

Anneaux et idéaux

Corrigé de l'exercice 1 : Inversibles, diviseurs de zéro et nilpotents de $\mathbb{Z}/n\mathbb{Z}$

- Si $\text{pgcd}(k, n) = 1$, le théorème de Bézout fournit $u, v \in \mathbb{Z}$ avec $ku + nv = 1$. En réduisant modulo n , on obtient $\bar{k} \bar{u} = \bar{1}$. Réciproquement, si $\bar{k} \bar{u} = \bar{1}$, alors $ku - 1 = nv$ pour un entier v . Ainsi $ku - nv = 1$, et tout diviseur commun de k et n divise 1. **Donc $\bar{k}$ est inversible si et seulement si $\text{pgcd}(k, n) = 1$.**
- Soit $\bar{k} \neq \bar{0}$ non inversible. Alors $d = \text{pgcd}(k, n) > 1$. On pose $m = n/d$, qui vérifie $1 \leq m < n$, donc $\bar{m} \neq \bar{0}$. De plus, $km = (k/d)n$ est multiple de n . Par conséquent, $\bar{k} \bar{m} = \bar{0}$. **Tout élément non nul est donc inversible ou diviseur de zéro.**
- Les entiers de 1 à 11 premiers avec 12 sont 1, 5, 7, 11. **Les inversibles sont $\bar{1}, \bar{5}, \bar{7}, \bar{11}$; les diviseurs de zéro sont $\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{10}$.** Ensuite, $5 \times 5 = 25 = 2 \times 12 + 1$ et $7 \times 7 = 49 = 4 \times 12 + 1$. **Ainsi $\bar{5}^{-1} = \bar{5}$ et $\bar{7}^{-1} = \bar{7}$.**
- On a $\bar{k}^m = \bar{0}$ si et seulement si $12 \mid k^m$. Il faut donc que 2 et 3 divisent k , c'est-à-dire $6 \mid k$. Réciproquement, $\frac{6^2}{12} = 36 \equiv 0$. **Les nilpotents de $\mathbb{Z}/12\mathbb{Z}$ sont $\bar{0}$ et $\bar{6}$.** En général, notons $p_1, \dots, p_r$ les facteurs premiers distincts de n et α le plus grand exposant. Si $n \mid k^m$, chaque p_j divise k par le lemme d'Eucclide. Réciproquement, si $p_1 \dots p_r \mid k$, alors $n \mid k^\alpha$. **Donc $\bar{k}$ est nilpotent si et seulement si $p_1 p_2 \dots p_r$ divise k .**

Point de méthode : dans un anneau fini, la multiplication par un élément non diviseur de zéro est injective, donc bijective ; c'est la raison profonde de la question 2.

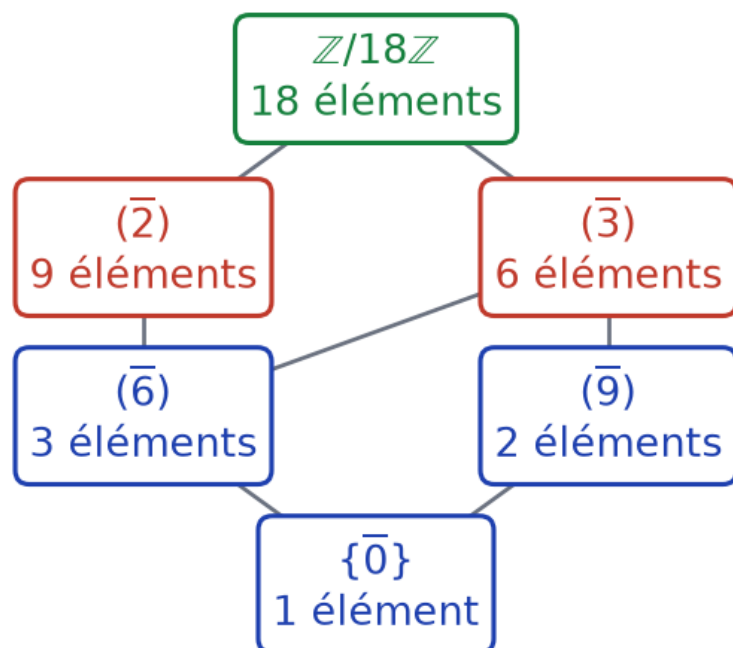
Corrigé de l'exercice 2 : Morphismes d'anneaux issus de $\mathbb{Z}$ et de $\mathbb{Z}[i]$

1. Un morphisme $f: \mathbb{Z} \rightarrow A$ vérifie $f(1) = 1_A$. Comme f est additif, on a $f(n) = n \cdot 1_A$ pour tout $n \in \mathbb{Z}$, d'où l'unicité. Réciproquement, $n \mapsto n \cdot 1_A$ est additif, et $(n \cdot 1_A)(m \cdot 1_A) = nm \cdot 1_A$ par distributivité. **Il existe donc un unique morphisme $\mathbb{Z} \rightarrow A$.**
2. Un morphisme $g: \mathbb{Z}/n\mathbb{Z} \rightarrow A$ composé avec la surjection π donne le morphisme $n \mapsto n \cdot 1_A$, qui doit s'annuler sur $n\mathbb{Z}$. Il faut donc $n \cdot 1_A = 0$, et g est déterminé par $g(\bar{k}) = k \cdot 1_A$. Réciproquement, si $n \cdot 1_A = 0$, le noyau de $\mathbb{Z} \rightarrow A$ contient $n\mathbb{Z}$. Ce morphisme passe alors au quotient. **Un morphisme existe si et seulement si $n \cdot 1_A = 0$, et il est unique.**
3. Dans $\mathbb{Z}/4\mathbb{Z}$, $6 \cdot \bar{1} = \bar{2} \neq \bar{0}$, alors que $12 \cdot \bar{1} = \bar{0}$. Dans $\mathbb{Z}/12\mathbb{Z}$, $4 \cdot \bar{1} = \bar{4} \neq \bar{0}$. **Il y a donc respectivement 0, 1 et 0 morphismes.**
4. Un morphisme $\varphi: \mathbb{Z}[i] \rightarrow \mathbb{Z}/5\mathbb{Z}$ vérifie $\varphi(m + ni) = \bar{m} + \bar{n}a$ avec $a = \varphi(i)$. De plus, $a^2 = \varphi(i^2) = -\bar{1} = \bar{4}$. Or, dans $\mathbb{Z}/5\mathbb{Z}$, les carrés de $\bar{0}, \dots, \bar{4}$ valent $\bar{0}, \bar{1}, \bar{4}, \bar{4}, \bar{1}$. Donc $a \in \{\bar{2}, \bar{3}\}$. Réciproquement, soit a tel que $a^2 = -\bar{1}$ et $\varphi(m + ni) = \bar{m} + \bar{n}a$. Cette application est additive et envoie 1 sur $\bar{1}$. Pour le produit, on a d'une part $(m + ni)(m' + n'i) = mm' - nn' + (mn' + nm')i$. D'autre part, $(\bar{m} + \bar{n}a)(\bar{m}' + \bar{n}'a) = \bar{m}\bar{m}' + \bar{m}\bar{n}'a + \bar{n}\bar{m}'a + \bar{n}\bar{n}'a^2$, et $a^2 = -\bar{1}$. Les deux expressions coïncident. **Il y a exactement deux morphismes, définis par $i \mapsto \bar{2}$ et $i \mapsto \bar{3}$.**
5. Pour $a = \bar{2}$, on a $\varphi(m + ni) = \overline{m + 2n}$. L'image de l'entier m est $\bar{m}$, donc φ est surjectif. Enfin, $\varphi(2 - i) = \overline{2 - 2} = \bar{0}$. **Ainsi φ est surjectif et $2 - i \in \ker \varphi$.**

Corrigé de l'exercice 3 : Idéaux de $\mathbb{Z}/18\mathbb{Z}$

1. D'après le théorème de correspondance, les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $J/n\mathbb{Z}$ avec J idéal de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Or $J = d\mathbb{Z}$ avec $d \geq 0$, et $n\mathbb{Z} \subset d\mathbb{Z}$ équivaut à $d \mid n$. L'idéal $d\mathbb{Z}/n\mathbb{Z}$ est l'idéal $(\bar{d})$. Ses éléments sont $\bar{0}, \bar{d}, \dots, (\overline{n/d} - 1)\bar{d}$. **Les idéaux sont les $(\bar{d})$, $d \mid n$, et $(\bar{d})$ a n/d éléments.**

2. Les diviseurs de 18 sont 1, 2, 3, 6, 9, 18. Il y a donc six idéaux : $\mathbb{Z}/18\mathbb{Z}$, $(\bar{2})$, $(\bar{3})$, $(\bar{6})$, $(\bar{9})$ et $\{\bar{0}\}$. L'inclusion $(\bar{d}) \subset (\bar{d'})$ équivaut à $d' \mid d$. La figure ci-dessous représente ces inclusions.



en rouge : idéaux maximaux

3. On a $(\mathbb{Z}/18\mathbb{Z})/(\bar{d}) \simeq \mathbb{Z}/d\mathbb{Z}$ par la correspondance des quotients. Ce quotient est intègre si et seulement si d est premier, et c'est alors un corps. **Les idéaux premiers sont $(\bar{2})$ et $(\bar{3})$; ils sont maximaux, de quotients $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.** Les autres idéaux propres ne sont pas premiers : par exemple $\bar{2} \times \bar{3} \in (\bar{6})$ alors que ni $\bar{2}$ ni $\bar{3}$ n'y appartient.
4. L'idéal $(\bar{k})$ correspond à $k\mathbb{Z} + 18\mathbb{Z} = \text{pgcd}(k, 18)\mathbb{Z}$. Ainsi $(\bar{4}) = (\bar{2})$, car $\text{pgcd}(4, 18) = 2$, et $(\bar{15}) = (\bar{3})$. Ensuite, $(\bar{2}) + (\bar{3})$ contient $\bar{3} - \bar{2} = \bar{1}$. Enfin, $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$. **Donc $(\bar{4}) + (\bar{15}) = \mathbb{Z}/18\mathbb{Z}$ et $(\bar{2}) \cap (\bar{3}) = (\bar{6})$.**

Corrigé de l'exercice 4 : Idéaux d'un anneau produit

1. Si I et J sont des idéaux, $I \times J$ est un sous-groupe, et $(a, b)(x, y) = (ax, by) \in I \times J$. Réciproquement, soit K un idéal de $A \times B$. On pose

$I = \left\{ \begin{pmatrix} x \\ (x, y) \end{pmatrix} \in K \right\}$ et $J = \left\{ \begin{pmatrix} y \\ (x, y) \end{pmatrix} \in K \right\}$, qui sont des idéaux, images de K par les projections. Évidemment $K \subset I \times J$. Inversement, si $x \in I$, il existe y avec $(x, y) \in K$, donc $(x, 0) = (1, 0)(x, y) \in K$. De même, $(0, y) \in K$ pour $y \in J$. Ainsi $(x, y) = (x, 0) + (0, y) \in K$. **Les idéaux de $A \times B$ sont exactement les $I \times J$.**

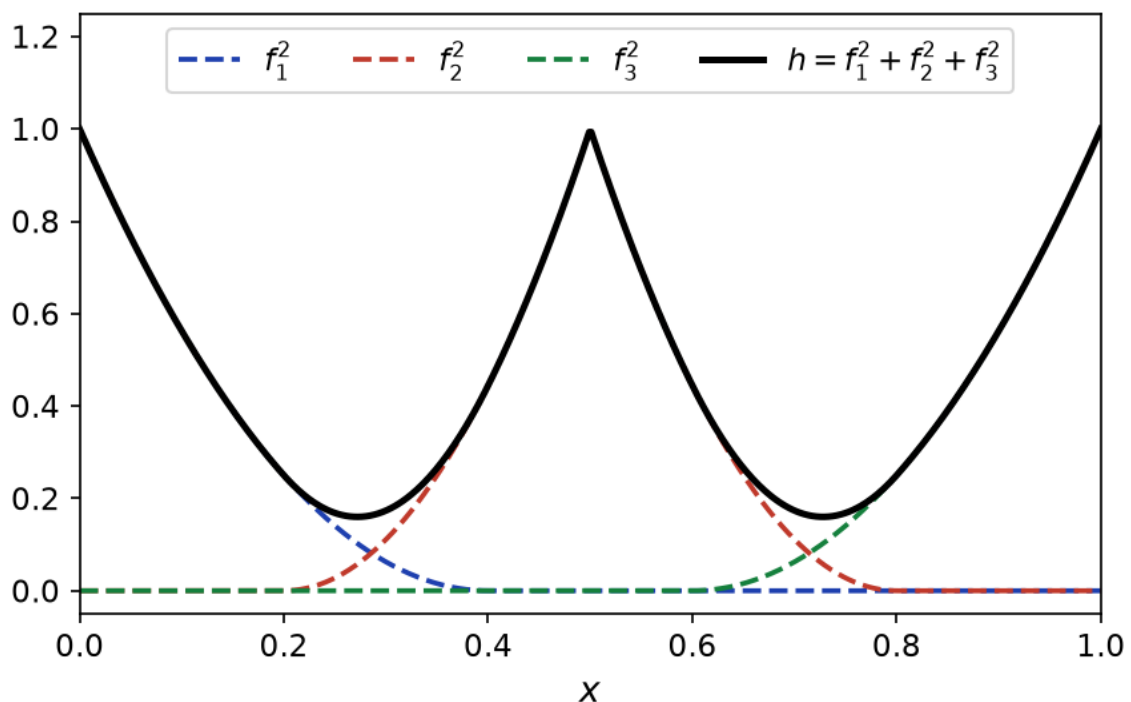
- Le morphisme $A \times B \rightarrow A/I \times B/J$, $(a, b) \rightarrow (\bar{a}, \bar{b})$, est surjectif, et son noyau est $I \times J$. **Par le théorème de factorisation, $(A \times B)/(I \times J) \simeq A/I \times B/J$.**
- On a $(1, 0)(0, 1) = (0, 0)$ avec $(1, 0) \neq 0$ et $(0, 1) \neq 0$, car A et B sont non nuls. Donc $A \times B$ n'est pas intègre. Soit maintenant $I \times J$ premier. D'après la question 2, $A/I \times B/J$ est intègre. Si les deux facteurs étaient non nuls, ce produit ne serait pas intègre. Donc $I = A$ ou $J = B$, mais pas les deux, car un idéal premier est propre. Si $J = B$, le quotient est A/I , qui doit être intègre : I est premier. **Les idéaux premiers sont les $P \times B$ et les $A \times Q$, avec P et Q premiers.** Le même raisonnement, avec « corps » à la place de « intègre », montre que les idéaux maximaux sont les $M \times B$ et $A \times M'$, avec M et M' maximaux.
- Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et les $p\mathbb{Z}$. **Les idéaux premiers de $\mathbb{Z} \times \mathbb{Z}$ sont $\{0\} \times \mathbb{Z}$, $\mathbb{Z} \times \{0\}$, $p\mathbb{Z} \times \mathbb{Z}$ et $\mathbb{Z} \times p\mathbb{Z}$; les maximaux sont $p\mathbb{Z} \times \mathbb{Z}$ et $\mathbb{Z} \times p\mathbb{Z}$, p premier.**

Corrigé de l'exercice 5 : Idéaux maximaux des fonctions continues

- Les fonctions f et g sont continues et non nulles, car $f(1) = g(0) = \frac{1}{2}$. Cependant, pour tout x , l'un des deux facteurs $f(x)$ ou $g(x)$ est nul. **Ainsi $fg = 0$, et C n'est pas intègre.**
- L'évaluation $e_a : C \rightarrow \mathbb{R}$, $f \rightarrow f(a)$, est un morphisme d'anneaux. Elle est surjective, car la fonction constante égale à c a pour image c . Son noyau est I_a . Par le théorème de factorisation, $C/I_a \simeq \mathbb{R}$, qui est un corps. **Donc I_a est un idéal maximal.**
- On a $J = I_0 \cap I_1$, qui est un idéal comme intersection d'idéaux. Posons $u(x) = x$ et $v(x) = 1 - x$. Alors uv s'annule en 0 et en 1, donc $uv \in J$. En revanche, $u(1) = 1$ et $v(0) = 1$, donc $u \notin J$ et $v \notin J$. **L'idéal J n'est pas premier.**
- Soit $a \in [0, 1]$. Si toutes les fonctions de M s'annulaient en a , on aurait $M \subset I_a$. Or

$I_\alpha \neq \mathcal{C}$ et M est maximal, donc $M = I_\alpha$, ce qui est exclu. **Il existe donc** $f_\alpha \in M$ **telle que** $f_\alpha(\alpha) \neq 0$.

5. Par continuité, f_α ne s'annule pas sur un intervalle ouvert U_α contenant α . Les U_α recouvrent le compact $[0,1]$. D'après la propriété de Borel-Lebesgue, on extrait un sous-recouvrement fini $U_{\alpha_1}, \dots, U_{\alpha_n}$. On pose alors $h = f_{\alpha_1}^2 + \dots + f_{\alpha_n}^2$. Comme M est un idéal, $h \in M$. De plus, tout x appartient à un U_{α_k} , donc $h(x) \geq f_{\alpha_k}(x)^2 > 0$. La figure ci-dessous illustre cette construction avec trois fonctions. Par suite, $1/h$ est continue, et $1 = h \cdot \frac{1}{h} \in M$. C'est absurde, car $M \neq \mathcal{C}$. **Tout idéal maximal de $\mathcal{C}$ est donc de la forme I_α , et ces idéaux sont maximaux d'après la question 2.**



Point de méthode : on utilise des carrés pour éviter les compensations de signe ; la somme de carrés ne s'annule que là où tous s'annulent.

Corrigé de l'exercice 6 : Trois quotients de $\mathbb{R}[X]$

1. L'évaluation $f : \mathbb{R}[X] \rightarrow \mathbb{C}, P \rightarrow P(i)$, est un morphisme. Elle est surjective, car

$a + bX$ a pour image $a + ib$. Soit $P \in \ker f$. La division euclidienne donne $P = (X^2 + 1)Q + aX + b$ avec a, b réels. Alors $0 = P(i) = ai + b$, donc $a = b = 0$. Ainsi $\ker f = (X^2 + 1)$. **Par le théorème de factorisation**, $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$.

- On a $x^2 = \overline{X^2} = 0$. En revanche, $X \notin (X^2)$ pour une raison de degré, donc $x \neq 0$. **Ainsi x est nilpotent non nul, et (X^2) n'est pas premier**, puisque $X \cdot X \in (X^2)$ alors que $X \notin (X^2)$.
- L'application φ est un morphisme, car l'évaluation en un point en est un. Elle est surjective : (α, β) est l'image de $\frac{\alpha - \beta}{2}X + \frac{\alpha + \beta}{2}$. Ensuite, $P \in \ker \varphi$ si et seulement si 1 et -1 sont racines de P , si et seulement si $(X - 1)(X + 1)$ divise P . En effet, $X - 1$ et $X + 1$ sont premiers entre eux. **Donc $\ker \varphi = (X^2 - 1)$ et $\mathbb{R}[X]/(X^2 - 1) \simeq \mathbb{R} \times \mathbb{R}$.**
- Le premier quotient est isomorphe à $\mathbb{C}$, qui est un corps. Le deuxième contient un nilpotent non nul, donc un diviseur de zéro. Le troisième contient $(1, 0)(0, 1) = (0, 0)$. **Seul $\mathbb{R}[X]/(X^2 + 1)$ est intègre, et c'est un corps.** Cela confirme que $K[X]/(P)$ est un corps si et seulement si P est irréductible.

Corrigé de l'exercice 7 : Quotients de l'anneau $\mathbb{Z}[i]$

- L'évaluation $f : \mathbb{Z}[X] \rightarrow \mathbb{Z}[i], P \rightarrow P(i)$, est un morphisme surjectif, car $m + nX \rightarrow m + ni$. Comme $X^2 + 1$ est unitaire, la division euclidienne par ce polynôme reste possible dans $\mathbb{Z}[X]$: $P = (X^2 + 1)Q + aX + b$ avec $a, b \in \mathbb{Z}$. Si $P(i) = 0$, alors $ai + b = 0$, donc $a = b = 0$. **Ainsi $\ker f = (X^2 + 1)$ et $\mathbb{Z}[X]/(X^2 + 1) \simeq \mathbb{Z}[i]$.**
- D'abord, $\psi(2 - i) = \overline{2 - i} = \bar{0}$, donc $(2 - i) \subset \ker \psi$. Réciproquement, soit $z = m + ni \in \ker \psi$. Comme $i = 2 - (2 - i)$, on a $i \equiv 2$ modulo $(2 - i)$. Donc $z \equiv m + 2n$ modulo $(2 - i)$. De plus, $5 = (2 - i)(2 + i)$ appartient à $(2 - i)$. Or $5 \mid m + 2n$, donc $m + 2n \in (2 - i)$, et $z \in (2 - i)$. Enfin, ψ est surjectif, car $\psi(m) = \bar{m}$. **Donc $\mathbb{Z}[i]/(2 - i) \simeq \mathbb{Z}/5\mathbb{Z}$.** Ce quotient est un corps, donc $(2 - i)$ est maximal, donc premier. **Par conséquent $2 - i$ est premier, donc irréductible.**
- Dans $\mathbb{Z}[i]/(5)$, on a $\overline{2 + i} \cdot \overline{2 - i} = \bar{5} = \bar{0}$. Or $2 + i \notin (5)$, car $\frac{2 + i}{5} \notin \mathbb{Z}[i]$, et de même $2 - i \notin (5)$. **Les classes de $2 + i$ et $2 - i$ sont des diviseurs de zéro, donc $\mathbb{Z}[i]/(5)$ n'est pas intègre.**

4. D'après la question 1, $\mathbb{Z}[i]/(3) \simeq \mathbb{Z}[X]/(X^2 + 1, 3)$. Par ailleurs, la réduction modulo 3 des coefficients est un morphisme surjectif $\mathbb{Z}[X] \rightarrow \mathbb{F}_3[X]/(X^2 + 1)$, de noyau $(3, X^2 + 1)$. Ainsi $\mathbb{Z}[i]/(3) \simeq \mathbb{F}_3[X]/(X^2 + 1)$. Or $X^2 + 1$ prend les valeurs 1, 2, 2 en 0, 1, 2 : il n'a pas de racine, et il est de degré 2, donc irréductible. **Le quotient est un corps de dimension 2 sur $\mathbb{F}_3$, donc à 9 éléments.**

Corrigé de l'exercice 8 : Idéal non principal de $\mathbb{Z}[X]$ et anneaux $A[X]$ principaux

- Le morphisme $P \rightarrow P(0)$ de $\mathbb{Z}[X]$ sur $\mathbb{Z}$ est surjectif, de noyau (X) , car $P(0) = 0$ équivaut à $X \mid P$. Ainsi $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$, qui est intègre sans être un corps. **L'idéal (X) est premier mais n'est pas maximal.**
- Considérons $\theta : \mathbb{Z}[X] \rightarrow \mathbb{Z}/2\mathbb{Z}, P \rightarrow \overline{P(0)}$, morphisme surjectif. Son noyau est $\left\{ P, \begin{matrix} P(0) \text{ pair} \end{matrix} \right\}$. Ce noyau contient 2 et X , donc $(2, X)$. Inversement, si $P(0) = 2k$, alors $P = 2k + XQ$ appartient à $(2, X)$. **Donc $(2, X) = \ker \theta$ et $\mathbb{Z}[X]/(2, X) \simeq \mathbb{Z}/2\mathbb{Z}$: l'idéal est maximal.**
- Supposons $(2, X) = (D)$. Alors D divise 2, donc $\deg D = 0$ et $D \in \{\pm 1, \pm 2\}$. Si $D = \pm 1$, l'idéal est $\mathbb{Z}[X]$; or $1 \notin (2, X)$, car 1 est impair en 0. Si $D = \pm 2$, alors $2 \mid X$ dans $\mathbb{Z}[X]$, ce qui est faux. **L'idéal $(2, X)$ n'est pas principal.**
- Si A est un corps, $A[X]$ est euclidien pour le degré, donc principal. Réciproquement, supposons $A[X]$ principal. Comme à la question 1, $A[X]/(X) \simeq A$, qui est intègre. Donc (X) est un idéal premier non nul. Dans un anneau principal, un idéal premier non nul est maximal. Ainsi $A \simeq A[X]/(X)$ est un corps. **Donc $A[X]$ est principal si et seulement si A est un corps.**
- L'anneau $\mathbb{Z}$ n'est pas un corps, et $\mathbb{R}[X]$ non plus, puisque X n'y est pas inversible. Or $\mathbb{R}[X, Y] = \mathbb{R}[X][Y]$. **Par la question 4, $\mathbb{Z}[X]$ et $\mathbb{R}[X, Y]$ ne sont pas principaux,** bien qu'ils soient factoriels.

Point de méthode : pour montrer qu'un idéal (a, b) n'est pas principal, on suppose $(a, b) = (d)$; alors d divise a et b , ce qui laisse très peu de candidats à éliminer.

Corrigé de l'exercice 9 : Idéaux premiers de $\mathbb{Z}$, $\mathbb{C}[X]$ et $\mathbb{R}[X]$

1. Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et les $p\mathbb{Z}$ avec p premier, car $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $n = 0$ ou n est premier.
2. L'anneau $K[X]$ est principal. L'idéal $\{0\}$ est premier, car $K[X]$ est intègre. Un idéal non nul (P) est premier si et seulement si P est un élément premier, c'est-à-dire irréductible, puisque $K[X]$ est principal. Dans un anneau principal, P irréductible entraîne (P) maximal. **Les idéaux premiers sont $\{0\}$ et les (P) , P irréductible ; les non nuls sont maximaux.**
3. Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1. **Les idéaux premiers de $\mathbb{C}[X]$ sont $\{0\}$ et les $(X - a)$, $a \in \mathbb{C}$. Ceux de $\mathbb{R}[X]$ sont $\{0\}$, les $(X - a)$, $a \in \mathbb{R}$, et les $(X^2 + bX + c)$ avec $b^2 - 4c < 0$.**
4. Le discriminant de $X^2 + X + 1$ vaut $-3 < 0$, donc ce polynôme est irréductible sur $\mathbb{R}$. En revanche, sur $\mathbb{C}$, on a $X^2 + X + 1 = (X - j)(X - \bar{j})$ avec $j = e^{2i\pi/3}$. Ensuite, $X^2 - 2$ est de degré 2 sans racine rationnelle, car $\sqrt{2}$ est irrationnel ; mais $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ sur $\mathbb{R}$. **$(X^2 + X + 1)$ est maximal dans $\mathbb{R}[X]$, pas dans $\mathbb{C}[X]$; $(X^2 - 2)$ est maximal dans $\mathbb{Q}[X]$, pas dans $\mathbb{R}[X]$.**

Corrigé de l'exercice 10 : Corps des fractions d'anneaux quadratiques

1. L'ensemble $\mathbb{Q}(i)$ contient 1 et est stable par différence et par produit, car $(a + ib)(c + id) = ac - bd + i(ad + bc)$. Pour $z = a + ib \neq 0$, on a $\frac{1}{z} = \frac{a - ib}{a^2 + b^2}$, qui appartient à $\mathbb{Q}(i)$. C'est donc un sous-corps. **En particulier,** $\frac{1}{3 + 4i} = \frac{3 - 4i}{25}$.
2. Soit $z = \frac{p}{r} + i\frac{s}{r}$, écrit avec un dénominateur commun $r \in \mathbb{N}^*$. Alors $z = \frac{p + is}{r}$, quotient de deux éléments de $\mathbb{Z}[i]$. L'inclusion $\mathbb{Z}[i] \rightarrow \mathbb{Q}(i)$ est injective. Par la propriété universelle, elle se prolonge en un morphisme de corps $\text{Frac}(\mathbb{Z}[i]) \rightarrow \mathbb{Q}(i)$, $\frac{u}{v} \rightarrow uv^{-1}$. Ce morphisme est injectif, comme tout morphisme de corps, et surjectif par ce qui précède. **Donc $\text{Frac}(\mathbb{Z}[i]) \simeq \mathbb{Q}(i)$.**

3. Le même argument s'applique. D'une part, $\mathbb{Q}(\sqrt{2}) = \left\{ \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \mid a, b, c, d \in \mathbb{Q} \right\}$ est un corps, car $\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$. Le dénominateur ne s'annule pas pour $(a, b) \neq (0, 0)$, puisque $\sqrt{2}$ est irrationnel. D'autre part, tout élément s'écrit $\frac{p + s\sqrt{2}}{r}$. Ainsi $\text{Frac}(\mathbb{Z}[\sqrt{2}]) \simeq \mathbb{Q}(\sqrt{2})$.
4. On a $(1 + \sqrt{2})(\sqrt{2} - 1) = 2 - 1 = 1$, donc $\frac{1}{1 + \sqrt{2}} = \sqrt{2} - 1$. Ensuite, $(3 + \sqrt{2})(3 - \sqrt{2}) = 7$, donc $\frac{1}{3 + \sqrt{2}} = \frac{3 - \sqrt{2}}{7}$. Seul $1 + \sqrt{2}$ est inversible dans $\mathbb{Z}[\sqrt{2}]$; l'inverse de $3 + \sqrt{2}$ a des coefficients non entiers.

Corrigé de l'exercice 11 : Un anneau quadratique euclidien

1. L'ensemble A contient 1, est stable par différence, et $(a + ib\sqrt{2})(c + id\sqrt{2}) = ac - 2bd + i(ad + bc)\sqrt{2}$. C'est donc un sous-anneau de $\mathbb{C}$, intègre. La norme $N(z) = |z|^2$ est multiplicative comme le module. Si $uv = 1$, alors $N(u)N(v) = 1$ avec des entiers naturels, donc $N(u) = a^2 + 2b^2 = 1$. Ceci impose $b = 0$ et $a = \pm 1$. Ainsi $A^\times = \{-1, 1\}$.
2. On choisit m et n entiers les plus proches de x et y , de sorte que $|x - m| \leq \frac{1}{2}$ et $|y - n| \leq \frac{1}{2}$. Pour $q = m + in\sqrt{2}$, on obtient $|z - q|^2 = (x - m)^2 + 2(y - n)^2 \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4}$. Donc $|z - q|^2 \leq \frac{3}{4}$. Géométriquement, le pire cas est le centre d'une maille du réseau.
3. Soient $a, b \in A$, $b \neq 0$. Le quotient $z = a/b$ s'écrit $x + iy\sqrt{2}$ avec x, y rationnels, car $\frac{a}{b} = \frac{a\bar{b}}{N(b)}$. On prend q comme à la question 2 et $r = a - bq \in A$. Alors $N(r) = N(b)|z - q|^2 \leq \frac{3}{4}N(b) < N(b)$. L'anneau A est euclidien, donc principal.
4. On calcule $\frac{5 + i\sqrt{2}}{1 + i\sqrt{2}} = \frac{(5 + i\sqrt{2})(1 - i\sqrt{2})}{3} = \frac{5 - 5i\sqrt{2} + i\sqrt{2} + 2}{3} = \frac{7 - 4i\sqrt{2}}{3}$. On arrondit $\frac{7}{3}$ en 2 et $-\frac{4}{3}$ en -1, d'où $q = 2 - i\sqrt{2}$. Ensuite, $(1 + i\sqrt{2})(2 - i\sqrt{2}) = 2 - i\sqrt{2} + 2i\sqrt{2} + 2 = 4 + i\sqrt{2}$. Ainsi $5 + i\sqrt{2} = (1 + i\sqrt{2})(2 - i\sqrt{2}) + 1$, et $N(1) = 1 < 3$. Le reste est inversible, donc l'algorithme s'arrête à l'étape suivante avec un PGCD égal à 1. Les deux éléments sont premiers entre eux.
5. On a $3 = (1 + i\sqrt{2})(1 - i\sqrt{2})$ et $11 = (3 + i\sqrt{2})(3 - i\sqrt{2})$. Les normes des facteurs valent 3 et 11, qui sont premiers. Si l'un d'eux s'écrivait uv , on aurait $N(u) = 1$ ou

$N(v) = 1$, donc u ou v inversible. **Ce sont donc des décompositions en produits d'irréductibles.**

Corrigé de l'exercice 12 : Un anneau quadratique non factoriel

1. Si $uv = 1$, alors $N(u) = a^2 + 5b^2 = 1$, donc $b = 0$ et $a = \pm 1$. Ensuite, $a^2 + 5b^2 \in \{2, 3\}$ impose $b = 0$, puis $a^2 \in \{2, 3\}$, ce qui est impossible. **Donc $B^\times = \{\pm 1\}$, et aucun élément n'a pour norme 2 ou 3.**
2. Les normes valent $N(2) = 4$, $N(3) = 9$ et $N(1 \pm i\sqrt{5}) = 6$. Si l'un de ces éléments s'écrit uv avec u, v non inversibles, alors $N(u) > 1$ et $N(v) > 1$ divisent 4, 9 ou 6. Dans chaque cas, l'un des deux vaut 2 ou 3, ce qui est impossible. Ces éléments sont donc irréductibles. Enfin, deux éléments associés ont même norme, car les inversibles sont ± 1 . Seuls $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ ont même norme, et $1 - i\sqrt{5} \neq \pm(1 + i\sqrt{5})$. **Les quatre éléments sont irréductibles et deux à deux non associés.**
3. On a $6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, puisque $1 + 5 = 6$. **Ce sont deux décompositions en irréductibles non équivalentes, donc B n'est pas factoriel.**
4. L'élément 2 divise $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6$. Cependant, $\frac{1 \pm i\sqrt{5}}{2}$ n'appartient pas à B , donc 2 ne divise aucun des deux facteurs. **Ainsi 2 est irréductible sans être premier.**
5. Soit $z = 2(p + iq\sqrt{5}) + (1 + i\sqrt{5})(s + it\sqrt{5})$ un élément de I . Son premier terme vaut $2p + 2q i\sqrt{5}$. Le second vaut $(s - 5t) + (s + t) i\sqrt{5}$. La somme des deux coordonnées est donc $2p + 2q + 2s - 4t$, qui est paire. Or 1 a des coordonnées de somme 1, donc $1 \notin I$. Supposons maintenant $I = (d)$. Alors $N(d)$ divise $N(2) = 4$ et $N(1 + i\sqrt{5}) = 6$, donc $N(d) \in \{1, 2\}$. Le cas 2 est exclu par la question 1. Donc $N(d) = 1$, $d = \pm 1$ et $I = B$, ce qui contredit $1 \notin I$. **L'idéal I n'est pas principal.**

Point de méthode : la norme multiplicative est l'outil clé des anneaux quadratiques ; elle transforme toute question de divisibilité en question sur des entiers.

Corrigé de l'exercice 13 : Anneaux intègres finis

1. Soit A intègre fini et $a \neq 0$. L'application $x \rightarrow ax$ est injective, car $ax = ay$ entraîne $a(x - y) = 0$, donc $x = y$. Comme A est fini, elle est bijective. Il existe donc x avec $ax = 1$. **Tout élément non nul est inversible : A est un corps.**
2. Si P est premier dans un anneau fini A , alors A/P est intègre et fini. **C'est donc un corps, et P est maximal.**
3. Si n est premier, $n\mathbb{Z}$ est premier, donc $\mathbb{Z}/n\mathbb{Z}$ est intègre et fini : c'est un corps. Si $n = ab$ avec $1 < a, b < n$, alors $\bar{a}\bar{b} = \bar{0}$ avec deux facteurs non nuls. **Donc $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.**
4. Dans F , on a $x^2 = -x - 1 = x + 1$. On en déduit $x(x + 1) = x^2 + x = 2x + 1 = 1$ et $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1 = x$. **La table est : $1 \cdot y = y$, $x \cdot x = x + 1$, $x(x + 1) = 1$, $(x + 1)^2 = x$.** Tout élément non nul a donc un inverse : $1^{-1} = 1$, $x^{-1} = x + 1$ et $(x + 1)^{-1} = x$. **Ainsi F est un corps à quatre éléments.**

Corrigé de l'exercice 14 : Polynômes irréductibles sur le corps à deux éléments

1. Les polynômes de degré 1 sont X et $X + 1$, tous irréductibles. En degré 2, un polynôme est irréductible si et seulement s'il n'a pas de racine. Il faut donc un terme constant égal à 1, pour que 0 ne soit pas racine, et un nombre impair de termes, pour que 1 ne soit pas racine. **Le seul irréductible de degré 2 est $X^2 + X + 1$.**
2. Le même critère vaut en degré 3. Les candidats de terme constant 1 sont $X^3 + 1$, $X^3 + X + 1$, $X^3 + X^2 + 1$ et $X^3 + X^2 + X + 1$. Les premier et dernier s'annulent en 1. **Les irréductibles unitaires de degré 3 sont $X^3 + X + 1$ et $X^3 + X^2 + 1$.**
3. Soit $P = X^4 + X + 1$. On a $P(0) = 1$ et $P(1) = 1$, donc P n'a pas de facteur de degré 1. S'il était réductible, il serait produit de deux irréductibles de degré 2, c'est-à-dire $(X^2 + X + 1)^2 = X^4 + X^2 + 1$, car les termes croisés doubles s'annulent. Or ce polynôme diffère de P . **Donc $X^4 + X + 1$ est irréductible.**

4. Le polynôme $X^3 + X + 1$ est irréductible, donc K est un corps. C'est un $\mathbb{F}_2$ -espace de dimension 3, donc $|K| = 2^3 = 8$. La relation $\alpha^3 = \alpha + 1$ donne $\alpha(\alpha^2 + 1) = \alpha^3 + \alpha = 1$. Ainsi $\alpha^{-1} = \alpha^2 + 1$. Ensuite, on calcule successivement $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$. De même, $\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1$ et $\alpha^7 = \alpha^3 + \alpha = 1$. Les puissances $\alpha^0, \dots, \alpha^6$ sont les sept éléments non nuls : $K^\times$ est cyclique d'ordre 7, engendré par α .

Corrigé de l'exercice 15 : Critère d'Eisenstein

- On prend $p = 3$. Le coefficient dominant 1 n'est pas divisible par 3. Les autres coefficients 0, -6, 0, 12, 3 le sont, et 9 ne divise pas 3. **Par le critère d'Eisenstein, $X^5 - 6X^3 + 12X + 3$ est irréductible sur $\mathbb{Q}$.**
- Pour $n \geq 1$, on applique le critère avec $p = 2$: 2 ne divise pas 1, divise -2 et les coefficients nuls, et 4 ne divise pas -2. Donc $X^n - 2$ est irréductible sur $\mathbb{Q}$. Si $\sqrt[n]{2}$ était rationnel pour $n \geq 2$, $X - \sqrt[n]{2}$ serait un facteur de degré 1 de $X^n - 2$ dans $\mathbb{Q}[X]$. **Donc $\sqrt[n]{2}$ est irrationnel pour tout $n \geq 2$.**
- L'application $\sigma : P \rightarrow P(X+1)$ est un automorphisme de l'anneau $\mathbb{Q}[X]$, d'inverse $P \rightarrow P(X-1)$. Elle conserve le degré. Ainsi $P = QR$ équivaut à $\sigma(P) = \sigma(Q)\sigma(R)$ avec les mêmes degrés. Par conséquent, P est irréductible si et seulement si $P(X+1)$ l'est. Or $(X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$. Le critère s'applique avec $p = 2$: 4, 6, 4, 2 sont pairs et 4 $\nmid 2$. **Donc $X^4 + 1$ est irréductible sur $\mathbb{Q}$.**
- On a $\Phi_p = \frac{X^p - 1}{X - 1}$, donc $\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{k=1}^p \binom{p}{k} X^{k-1}$. Le coefficient dominant vaut $\binom{p}{p} = 1$ et le terme constant vaut $\binom{p}{1} = p$. Pour $1 \leq k \leq p-1$, p divise $p! = \binom{p}{k} k! (p-k)!$ sans diviser $k! (p-k)!$, donc $p \mid \binom{p}{k}$. Enfin, $p^2 \nmid p$. **Par Eisenstein et la question 3, Φ_p est irréductible sur $\mathbb{Q}$.**

Corrigé de l'exercice 16 : Irréductibilité par réduction modulo p

- Supposons $P = QR$ dans $\mathbb{Q}[X]$ avec $\deg Q, \deg R \geq 1$. D'après le lemme de Gauss, on peut choisir $Q, R \in \mathbb{Z}[X]$; en effet, si $c = c(P)$, alors $P/c = Q_1 R_1$ avec Q_1, R_1 primitifs, et $P = (cQ_1) R_1$. Le produit des coefficients dominants de Q et R vaut celui de P , non divisible par p . Donc $\deg \bar{Q} = \deg Q \geq 1$ et $\deg \bar{R} = \deg R \geq 1$. Alors $\bar{P} = \bar{Q} \bar{R}$ est réductible, ce qui est exclu. **Donc P est irréductible dans $\mathbb{Q}[X]$.**
- Modulo 2, $X^3 + 4X^2 + 3X + 5$ devient $X^3 + X + 1$, irréductible sur $\mathbb{F}_2$ car sans racine. Le coefficient dominant 1 est impair. **Le polynôme est donc irréductible sur $\mathbb{Q}$.**
Vérifions-le autrement : une racine rationnelle serait entière, d'après l'exercice 17, et diviserait 5. Or $P(1) = 13$, $P(-1) = 5$, $P(5) = 245$ et $P(-5) = -35$. Sans racine rationnelle, un polynôme de degré 3 est irréductible sur $\mathbb{Q}$.
- Modulo 2, $X^4 + 5X + 7$ devient $X^4 + X + 1$, irréductible d'après l'exercice 14. **Donc $X^4 + 5X + 7$ est irréductible sur $\mathbb{Q}$.**
- Dans $\mathbb{F}_2[X]$, $(X+1)^4 = X^4 + 1$, car les coefficients binomiaux 4 et 6 sont pairs. Dans $\mathbb{F}_3[X]$, on développe $(X^2 + X + 2)(X^2 + 2X + 2) = X^4 + 3X^3 + 6X^2 + 6X + 4$, qui vaut $X^4 + 1$ modulo 3. **Ainsi $X^4 + 1$ est réductible modulo 2 et modulo 3, bien qu'irréductible sur $\mathbb{Q}$: la réciproque est fausse.**

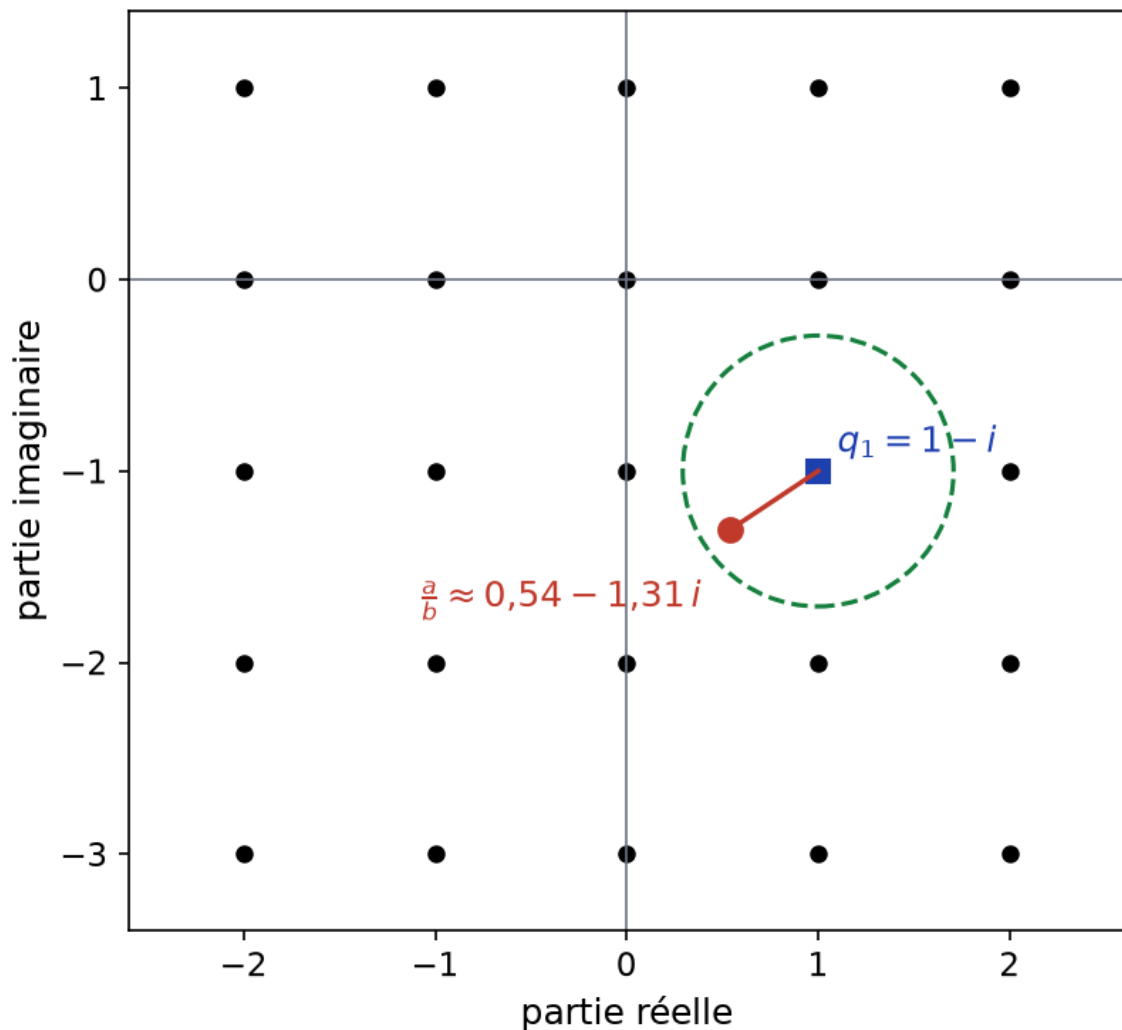
Corrigé de l'exercice 17 : Contenu et lemme de Gauss

- On a $c(P) = \text{pgcd}(6, 9, 15) = 3$ et $c(Q) = \text{pgcd}(10, 4) = 2$. Ensuite, $PQ = 60X^5 + 90X^4 - 24X^3 - 186X^2 + 60$. En effet, le terme en X^2 vaut $-150 - 36 = -186$. Or $\text{pgcd}(60, 90) = 30$, puis $\text{pgcd}(30, 24) = 6$, et 6 divise $186 = 6 \times 31$. **Ainsi $c(PQ) = 6 = c(P)c(Q)$.**
- Soient P, Q primitifs et supposons qu'un premier p divise tous les coefficients de PQ . La réduction modulo p est un morphisme $\mathbb{Z}[X] \rightarrow \mathbb{F}_p[X]$. Donc $\bar{P}\bar{Q} = \overline{PQ} = 0$. Or $\mathbb{F}_p$ est un corps, donc $\mathbb{F}_p[X]$ est intègre. Ainsi $\bar{P} = 0$ ou $\bar{Q} = 0$, c'est-à-dire que p divise tous les coefficients de P ou de Q . C'est contraire à la primitivité. **Donc PQ est primitif.**

3. On écrit $Q = \alpha Q_1$ et $R = \beta R_1$ avec $\alpha, \beta \in \mathbb{Q}_{>0}$ et $Q_1, R_1 \in \mathbb{Z}[X]$ primitifs, en chassant les dénominateurs puis en divisant par le contenu. Alors $P = \alpha\beta Q_1 R_1$, où P est primitif car unitaire, et $Q_1 R_1$ est primitif par la question 2. Écrivons $\alpha\beta = \frac{r}{s}$ irréductible avec $s > 0$. Alors $sP = r Q_1 R_1$, et en prenant les contenus, $s = r$, d'où $\alpha\beta = 1$. Les coefficients dominants q_1 et r_1 de Q_1 et R_1 vérifient $q_1 r_1 = 1$, donc $q_1 = \pm 1$. Comme Q est unitaire, $\alpha q_1 = 1$. **Ainsi $Q = \pm Q_1 \in \mathbb{Z}[X]$, et de même $R \in \mathbb{Z}[X]$.**
4. Si $r \in \mathbb{Q}$ est racine de P unitaire, alors $P = (X - r)S$ avec S unitaire dans $\mathbb{Q}[X]$. D'après la question 3, $X - r \in \mathbb{Z}[X]$, donc $r \in \mathbb{Z}$. **Une racine rationnelle est entière.** Or aucun entier n'a pour carré 2 ni pour cube 5. **Donc $\sqrt{2}$ et $\sqrt[3]{5}$ sont irrationnels.**
5. Dans $\mathbb{Q}[X]$, $2X + 2$ est de degré 1, donc irréductible. Dans $\mathbb{Z}[X]$, en revanche, $2X + 2 = 2(X + 1)$ où 2 n'est pas inversible. **Il est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{Z}[X]$.** Enfin, $6X^2 + 12X + 6 = 6(X + 1)^2$. Les irréductibles de $\mathbb{Z}[X]$ sont les premiers $\pm p$ et les primitifs irréductibles sur $\mathbb{Q}$. **Donc $6X^2 + 12X + 6 = 2 \times 3 \times (X + 1)^2$.**

Corrigé de l'exercice 18 : Division euclidienne et Bézout dans $\mathbb{Z}[i]$

1. **On a $N(a) = 121 + 9 = 130$ et $N(b) = 1 + 64 = 65$.**
2. Première division : $\frac{a}{b} = \frac{(11 + 3i)(1 - 8i)}{65} = \frac{11 - 88i + 3i + 24}{65} = \frac{35 - 85i}{65}$, soit environ $0,54 - 1,31i$. Comme le montre la figure ci-dessous, le point du réseau le plus proche est $q_1 = 1 - i$. On calcule $bq_1 = (1 + 8i)(1 - i) = 9 + 7i$, d'où $r_1 = a - bq_1 = 2 - 4i$, de norme $20 < 65$.



Deuxième division : $\frac{b}{r_1} = \frac{(1+8i)(2+4i)}{20} = \frac{-30+20i}{20} = -1,5 + i$. On choisit $q_2 = -1 + i$. Alors $r_1 q_2 = (2-4i)(-1+i) = 2+6i$, et $r_2 = b - r_1 q_2 = -1+2i$, de norme $5 < 20$. Troisième division : $\frac{r_1}{r_2} = \frac{(2-4i)(-1-2i)}{5} = \frac{-10}{5} = -2$. Le reste est nul. **Un PGCD est $d = -1+2i$, associé à $2+i$, car $-i(-1+2i) = 2+i$.**

3. On remonte l'algorithme. D'abord $r_2 = b - r_1 q_2$ et $r_1 = a - b q_1$. Donc $r_2 = b - (a - b q_1) q_2 = -q_2 a + (1 + q_1 q_2) b$. Or $q_1 q_2 = (1-i)(-1+i) = 2i$. **Ainsi $d = (1-i)a + (1+2i)b$.** Vérification : $(1-i)(11+3i) = 14-8i$ et $(1+2i)(1+8i) = -15+10i$, de somme $-1+2i$. Par conséquent, $d \in (a, b)$, et d divise a et b . **Donc $(a, b) = (2+i)$.**

4. On trouve $a = (3+2i)(3-i)$, car $(3+2i)(3-i) = 9-3i+6i+2 = 11+3i$. De plus, $3-i = -i(1+3i)$ et $1+3i = (1+i)(2+i)$. Ensuite, $b = (3-2i)(-1+2i)$, car ce produit vaut $-3+6i+2i+4 = 1+8i$. Les normes 13, 2 et 5 sont premières, donc ces facteurs sont irréductibles. Par ailleurs, $3+2i$ et $3-2i$ ne sont pas associés : leurs associés sont $\pm(3+2i)$ et $\pm(-2+3i)$. **Le seul**

irréductible commun est $2 + i$, à association près, ce qui confirme le PGCD.

Point de méthode : dans $\mathbb{Z}[i]$, on divise en multipliant par le conjugué du diviseur, puis on arrondit chaque coordonnée ; en cas d'égalité, comme $-1,5$, les deux arrondis conviennent.

Corrigé de l'exercice 19 : Factorisation en irréductibles dans $\mathbb{Z}[i]$

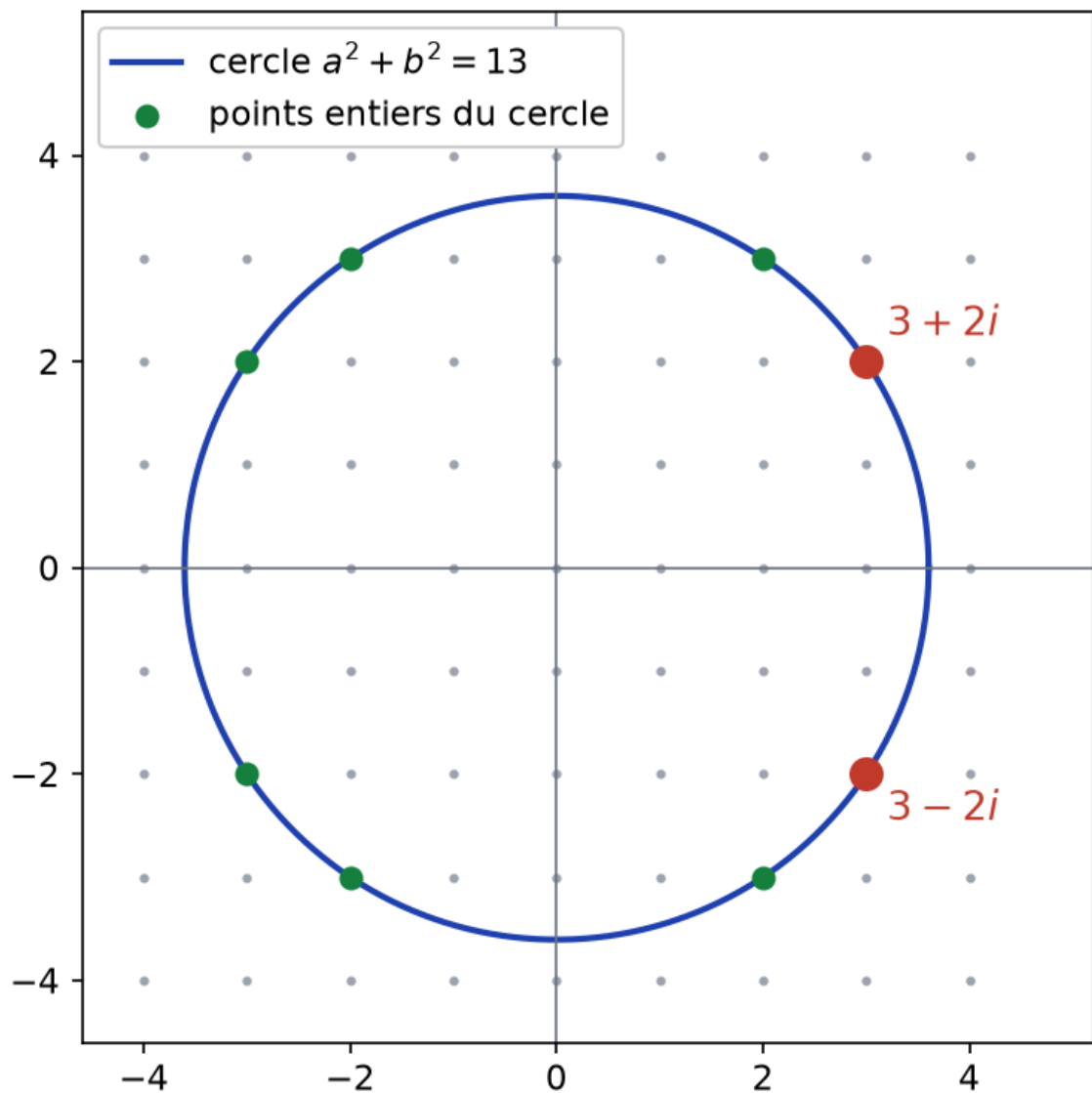
1. Si $z = uv$, alors $N(z) = N(u)N(v)$. Comme $N(z)$ est premier, $N(u) = 1$ ou $N(v) = 1$, donc u ou v est inversible. De plus, z n'est pas inversible, car $N(z) \neq 1$.
Donc z est irréductible.
2. On a $(1 + i)^2 = 2i$, donc $2 = -i(1 + i)^2$. Ensuite, $5 = (2 + i)(2 - i)$ et $13 = (3 + 2i)(3 - 2i)$, d'où $65 = (2 + i)(2 - i)(3 + 2i)(3 - 2i)$. Tous ces facteurs ont une norme première, 2 , 5 ou 13 , donc sont irréductibles par la question 1. **Ce sont les décompositions cherchées.** Notons que $2 - i$ n'est pas associé à $2 + i$, car $i(2 + i) = -1 + 2i$.
3. Soit $p \equiv 3 \pmod{4}$ premier. Si $p = uv$ avec u, v non inversibles, alors $N(u)N(v) = p^2$ avec $N(u), N(v) > 1$. Donc $N(u) = p$, c'est-à-dire $p = a^2 + b^2$. Or un carré est congru à 0 ou 1 modulo 4 , donc $a^2 + b^2 \not\equiv 3 \pmod{4}$. **Ainsi p est irréductible dans $\mathbb{Z}[i]$.**
4. On a $N(7 + i) = 50 = 2 \times 5^2$. Donc $1 + i$ divise $7 + i$:
$$\frac{7 + i}{1 + i} = \frac{(7 + i)(1 - i)}{2} = \frac{8 - 6i}{2} = 4 - 3i$$
. Ensuite, $N(4 - 3i) = 25$, et $(2 + i)^2 = 3 + 4i$. Or $-i(3 + 4i) = 4 - 3i$. **Ainsi $7 + i = -i(1 + i)(2 + i)^2$.**
Vérification : $(1 + i)(3 + 4i) = -1 + 7i$, puis $-i(-1 + 7i) = 7 + i$.
5. Les solutions correspondent aux $z = x + iy$ de norme 65 . Par factorialité, un tel z s'écrit $u \cdot \pi_5 \cdot \pi_{13}$, avec u parmi les quatre inversibles, $\pi_5 \in \{2 + i, 2 - i\}$ et $\pi_{13} \in \{3 + 2i, 3 - 2i\}$. Ces $4 \times 2 \times 2 = 16$ produits sont distincts, par unicité de la décomposition. **Il y a donc 16 couples :** les $(\pm 1, \pm 8)$, $(\pm 8, \pm 1)$, $(\pm 4, \pm 7)$ et $(\pm 7, \pm 4)$, puisque $65 = 1 + 64 = 16 + 49$.

Corrigé de l'exercice 20 : Théorème des deux carrés

- Dans le corps $\mathbb{F}_p$, l'équation $x^2 = 1$ a pour seules solutions ± 1 , car $(x-1)(x+1) = 0$. Les autres éléments de $\{2, \dots, p-2\}$ se regroupent donc en paires $\{x, x^{-1}\}$ avec $x \neq x^{-1}$. Chaque paire a un produit égal à 1. Par conséquent, $(p-1)! \equiv 1 \times (p-1) \equiv -1 \pmod{p}$. **C'est le théorème de Wilson.**
- On regroupe k et $p-k$ pour $1 \leq k \leq \frac{p-1}{2}$:

$$(p-1)! = \prod_{k=1}^{(p-1)/2} k(p-k) \equiv \prod_{k=1}^{(p-1)/2} (-k^2) \pmod{p}.$$

Ce produit vaut $(-1)^{(p-1)/2} x^2$. Or $\frac{p-1}{2}$ est pair, car $p \equiv 1 \pmod{4}$. **Donc** $x^2 \equiv -1 \pmod{p}$.
- D'après la question 2, p divise $x^2 + 1 = (x+i)(x-i)$. Cependant, p ne divise pas $x+i$, car $\frac{x}{p} + \frac{i}{p} \notin \mathbb{Z}[i]$, et de même pour $x-i$. Donc p n'est pas premier. Comme $\mathbb{Z}[i]$ est principal, p n'est pas irréductible : $p = zw$ avec $N(z), N(w) > 1$. Or $N(z)N(w) = p^2$, donc $N(z) = p$. **En écrivant** $z = a + ib$, **on obtient** $p = a^2 + b^2$.
- On a $6! = 720 = 55 \times 13 + 5$, donc $x \equiv 5 \pmod{13}$. On vérifie $5^2 = 25 \equiv -1 \pmod{13}$. Première division : $\frac{13}{5+i} = \frac{13(5-i)}{26} = 2,5 - 0,5i$. On choisit $q = 2$, d'où le reste $13 - 2(5+i) = 3 - 2i$, de norme $13 < 26$. Ensuite, $\frac{5+i}{3-2i} = \frac{(5+i)(3+2i)}{13} = \frac{13+13i}{13} = 1+i$. La division est exacte. **Un PGCD est** $3 - 2i$, **et** $13 = 3^2 + 2^2$. La figure représente les huit points entiers du cercle de rayon $\sqrt{13}$, qui correspondent aux associés de $3 + 2i$ et de $3 - 2i$.



5. Première division : $\frac{29}{12+i} = \frac{29(12-i)}{145} = \frac{12-i}{5} = 2,4 - 0,2i$. On choisit $q = 2$, d'où le reste $29 - 2(12+i) = 5 - 2i$, de norme $29 < 145$. Ensuite,
 $\frac{12+i}{5-2i} = \frac{(12+i)(5+2i)}{29} = \frac{58+29i}{29} = 2+i$. La division est exacte. **Un PGCD est $5 - 2i$, et $29 = 5^2 + 2^2$.**

Point de méthode : le PGCD de p et $x+i$ est un facteur de p de norme p ; l'algorithme d'Euclide le fournit sans aucun tâtonnement.

Corrigé de l'exercice 21 : Problème : une équation diophantienne dans $\mathbb{Z}[i]$

1. On a $1 = 1^3$, $-1 = (-1)^3$, $i = (-i)^3$ et $-i = i^3$. **Tout inversible de $\mathbb{Z}[i]$ est donc un cube.**
2. Si x est impair, alors $x^2 \equiv 1 \pmod{4}$, donc $y^3 = x^2 + 1 \equiv 2 \pmod{4}$. Dans ce cas, y est pair, donc $8 \mid y^3$, et $y^3 \equiv 0 \pmod{4}$. C'est une contradiction. **Donc x est pair, puis $y^3 = x^2 + 1$ est impair, et y aussi.**
3. Soit δ un diviseur commun de $x + i$ et $x - i$. Il divise leur différence $2i$, donc $N(\delta)$ divise $N(2i) = 4$. Il divise aussi $x + i$, donc $N(\delta)$ divise $N(x + i) = x^2 + 1$, qui est impair. Ainsi $N(\delta)$ divise $\text{pgcd}(4, x^2 + 1) = 1$. **Donc δ est inversible : $x + i$ et $x - i$ sont premiers entre eux.**
4. Si w est inversible, alors u l'est aussi, et $u = u \cdot 1^3$. Sinon, on écrit $w = \varepsilon p_1^{e_1} \dots p_r^{e_r}$, avec des irréductibles p_j deux à deux non associés. Alors $uv = \varepsilon^3 p_1^{3e_1} \dots p_r^{3e_r}$. Chaque p_j divise u ou v , mais pas les deux, car u et v sont premiers entre eux. Par unicité de la décomposition, l'exposant de p_j dans u vaut donc $3e_j$ ou 0 . Ainsi $u = \eta \prod_{j \in S} p_j^{3e_j} = \eta \left(\prod_{j \in S} p_j^{e_j} \right)^3$ avec η inversible. **Donc u est le produit d'un inversible et d'un cube.**
5. D'abord, $y \neq 0$, sinon $x^2 = -1$. On applique la question 4 dans l'anneau factoriel $\mathbb{Z}[i]$ avec $u = x + i$, $v = x - i$ et $w = y$. Ainsi $x + i = \eta c^3$, et η est un cube par la question 1. **Il existe donc $a, b \in \mathbb{Z}$ tels que $x + i = (a + ib)^3$.** Or $(a + ib)^3 = a^3 - 3ab^2 + i(3a^2b - b^3)$. En identifiant les parties imaginaires, $b(3a^2 - b^2) = 1$. Donc $b = \pm 1$. Si $b = 1$, alors $3a^2 = 2$, ce qui est impossible. Si $b = -1$, alors $-(3a^2 - 1) = 1$, donc $a = 0$. Ainsi $x + i = (-i)^3 = i$, soit $x = 0$, puis $y^3 = 1$, donc $y = 1$. **La seule solution est $(x, y) = (0, 1)$.**

Point de méthode : on factorise l'équation dans un anneau factoriel plus grand, on montre que les facteurs sont premiers entre eux, puis on identifie chaque facteur à une puissance.

Pour aller plus loin en L3

- Le cours : [anneaux et idéaux, cours de maths en L3](#)
- Les énoncés : [exercices de maths en L3 sur anneaux et idéaux](#)
- À maîtriser avant : [Groupes : quotients et actions de groupes](#)
- Chapitre précédent : [Groupes : quotients et actions de groupes](#)
- Chapitre suivant : [Corps, extensions et corps finis](#)
- Tester vos connaissances : [QCM de maths en L3 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L3](#) et la [licence de maths de L1 à L3](#)