

Anneaux et idéaux

Exercice 1 : Inversibles, diviseurs de zéro et nilpotents de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geq 2$ un entier. Un élément x d'un anneau est un diviseur de zéro s'il est non nul et s'il existe $y \neq 0$ tel que $xy = 0$. Il est nilpotent s'il existe $m \geq 1$ tel que $x^m = 0$.

1. Montrer que $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\text{pgcd}(k, n) = 1$.
2. Montrer que tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est soit inversible, soit diviseur de zéro.
3. Dresser la liste des inversibles et des diviseurs de zéro de $\mathbb{Z}/12\mathbb{Z}$. Donner l'inverse de $\bar{5}$ et celui de $\bar{7}$.
4. Déterminer les éléments nilpotents de $\mathbb{Z}/12\mathbb{Z}$, puis ceux de $\mathbb{Z}/n\mathbb{Z}$ en fonction des facteurs premiers de n .

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

1. Soit A un anneau. Montrer qu'il existe un unique morphisme d'anneaux $\mathbb{Z} \rightarrow A$.
2. En déduire qu'il existe un morphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \rightarrow A$ si et seulement si $n \cdot 1_A = 0$, et qu'il est alors unique.
3. Combien y a-t-il de morphismes d'anneaux de $\mathbb{Z}/6\mathbb{Z}$ vers $\mathbb{Z}/4\mathbb{Z}$? de $\mathbb{Z}/12\mathbb{Z}$ vers $\mathbb{Z}/4\mathbb{Z}$? de $\mathbb{Z}/4\mathbb{Z}$ vers $\mathbb{Z}/12\mathbb{Z}$?
4. Déterminer tous les morphismes d'anneaux $\mathbb{Z}[i] \rightarrow \mathbb{Z}/5\mathbb{Z}$.
5. Pour celui qui envoie i sur $\bar{2}$, vérifier qu'il est surjectif et que $2 - i$ appartient à son noyau.

Exercice 3 : Idéaux de $\mathbb{Z}/18\mathbb{Z}$

1. Soit $n \geq 2$. Montrer que les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $(\bar{d}) = d\mathbb{Z}/n\mathbb{Z}$, où d parcourt les diviseurs positifs de n , et que $(\bar{d})$ a n/d éléments.
2. Dresser la liste des idéaux de $\mathbb{Z}/18\mathbb{Z}$ et les ranger par inclusion.
3. Lesquels sont premiers ? maximaux ? Identifier chaque quotient $(\mathbb{Z}/18\mathbb{Z})/(\bar{d})$.
4. Déterminer les idéaux $(\bar{4})$, $(\bar{15})$, $(\bar{4}) + (\bar{15})$ et $(\bar{2}) \cap (\bar{3})$.

Exercice 4 : Idéaux d'un anneau produit

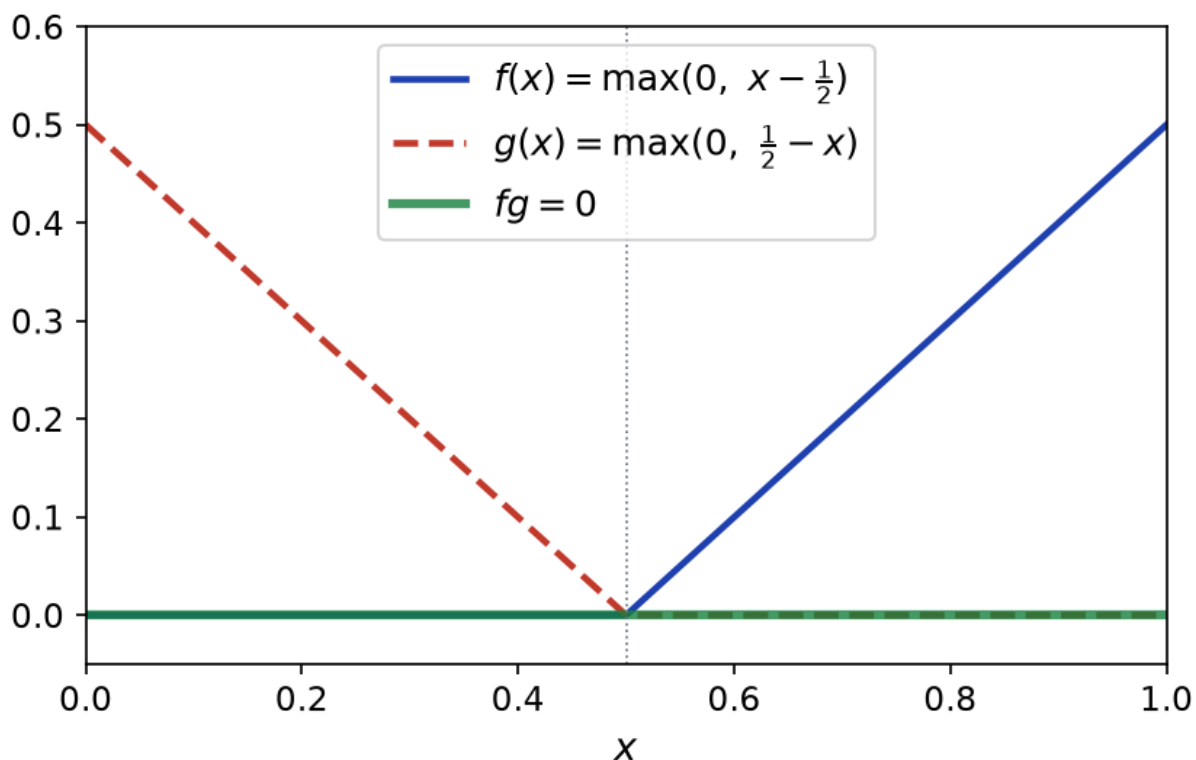
Soient A et B deux anneaux non nuls.

1. Montrer que les idéaux de $A \times B$ sont exactement les $I \times J$, avec I idéal de A et J idéal de B .
2. Montrer que $(A \times B)/(I \times J) \simeq A/I \times B/J$.
3. Montrer que $A \times B$ n'est jamais intègre. En déduire que les idéaux premiers de $A \times B$ sont les $P \times B$ et les $A \times Q$, avec P premier dans A et Q premier dans B .
4. Déterminer les idéaux premiers et les idéaux maximaux de $\mathbb{Z} \times \mathbb{Z}$.

Exercice 5 : Idéaux maximaux des fonctions continues

On note $C = \mathcal{C}([0,1], \mathbb{R})$ l'anneau des fonctions continues, et, pour $a \in [0,1]$,
 $I_a = \left\{ f \in C, \begin{array}{l} f(a) = 0 \end{array} \right\}$. On considère aussi les fonctions $f(x) = \max(0, x - \frac{1}{2})$ et

$g(x) = \max(0, \frac{1}{2} - x)$, représentées ci-dessous.



1. Montrer que $\mathcal{C}$ n'est pas intègre.
2. Montrer que I_a est un idéal maximal de $\mathcal{C}$.
3. Montrer que $J = \left\{ f \in \mathcal{C}, f(0) = f(1) = 0 \right\}$ est un idéal qui n'est pas premier.
4. Soit M un idéal maximal de $\mathcal{C}$. On suppose que $M \neq I_a$ pour tout a . Montrer que pour tout a , il existe $f_a \in M$ avec $f_a(a) \neq 0$.
5. En utilisant la compacité de $[0, 1]$, construire une fonction $h \in M$ strictement positive sur $[0, 1]$. Conclure que les idéaux maximaux de $\mathcal{C}$ sont exactement les I_a .

Exercice 6 : Trois quotients de $R[X]$

1. Montrer que $\mathbb{R}[X]/(X^2 + 1)$ est isomorphe à $\mathbb{C}$.
2. Montrer que dans $\mathbb{R}[X]/(X^2)$, la classe x de X est non nulle et nilpotente. L'idéal (X^2) est-il premier ?
3. Montrer que $\varphi : P \rightarrow (P(1), P(-1))$ induit un isomorphisme $\mathbb{R}[X]/(X^2 - 1) \simeq \mathbb{R} \times \mathbb{R}$.
4. Parmi ces trois quotients, lesquels sont des corps ? lesquels sont intègres ?

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

1. Montrer que $P \rightarrow P(i)$ induit un isomorphisme $\mathbb{Z}[X]/(X^2 + 1) \simeq \mathbb{Z}[i]$.
2. On considère $\psi : \mathbb{Z}[i] \rightarrow \mathbb{Z}/5\mathbb{Z}$, $m + ni \rightarrow \overline{m + 2n}$, dont on admet que c'est un morphisme d'anneaux. Montrer que $\ker \psi = (2 - i)$. En déduire que $\mathbb{Z}[i]/(2 - i) \simeq \mathbb{Z}/5\mathbb{Z}$ et que $2 - i$ est irréductible.
3. Montrer que $\mathbb{Z}[i]/(5)$ n'est pas intègre, en exhibant deux diviseurs de zéro.
4. Montrer que $\mathbb{Z}[i]/(3) \simeq \mathbb{F}_3[X]/(X^2 + 1)$, puis que c'est un corps à 9 éléments.

Exercice 8 : Idéal non principal de $\mathbb{Z}[X]$ et anneaux $A[X]$ principaux

1. Montrer que l'idéal (X) de $\mathbb{Z}[X]$ est premier mais n'est pas maximal.
2. Montrer que $(2, X) = \left\{ P \in \mathbb{Z}[X], \begin{matrix} P(0) \text{ pair} \\ P \text{ pair} \end{matrix} \right\}$ et que c'est un idéal maximal.
3. Montrer que $(2, X)$ n'est pas un idéal principal.
4. Soit A un anneau intègre. Montrer que $A[X]$ est principal si et seulement si A est un corps.
5. En déduire que $\mathbb{Z}[X]$ et $\mathbb{R}[X, Y]$ ne sont pas principaux.

Exercice 9 : Idéaux premiers de $\mathbb{Z}$, $\mathbb{C}[X]$ et $\mathbb{R}[X]$

1. Rappeler les idéaux premiers de $\mathbb{Z}$.
2. Soit K un corps. Montrer que les idéaux premiers de $K[X]$ sont $\{0\}$ et les (P) avec P irréductible, et que les non nuls sont maximaux.
3. Décrire les idéaux premiers de $\mathbb{C}[X]$, puis ceux de $\mathbb{R}[X]$.
4. L'idéal $(X^2 + X + 1)$ est-il maximal dans $\mathbb{R}[X]$? dans $\mathbb{C}[X]$? L'idéal $(X^2 - 2)$ est-il maximal dans $\mathbb{Q}[X]$? dans $\mathbb{R}[X]$?

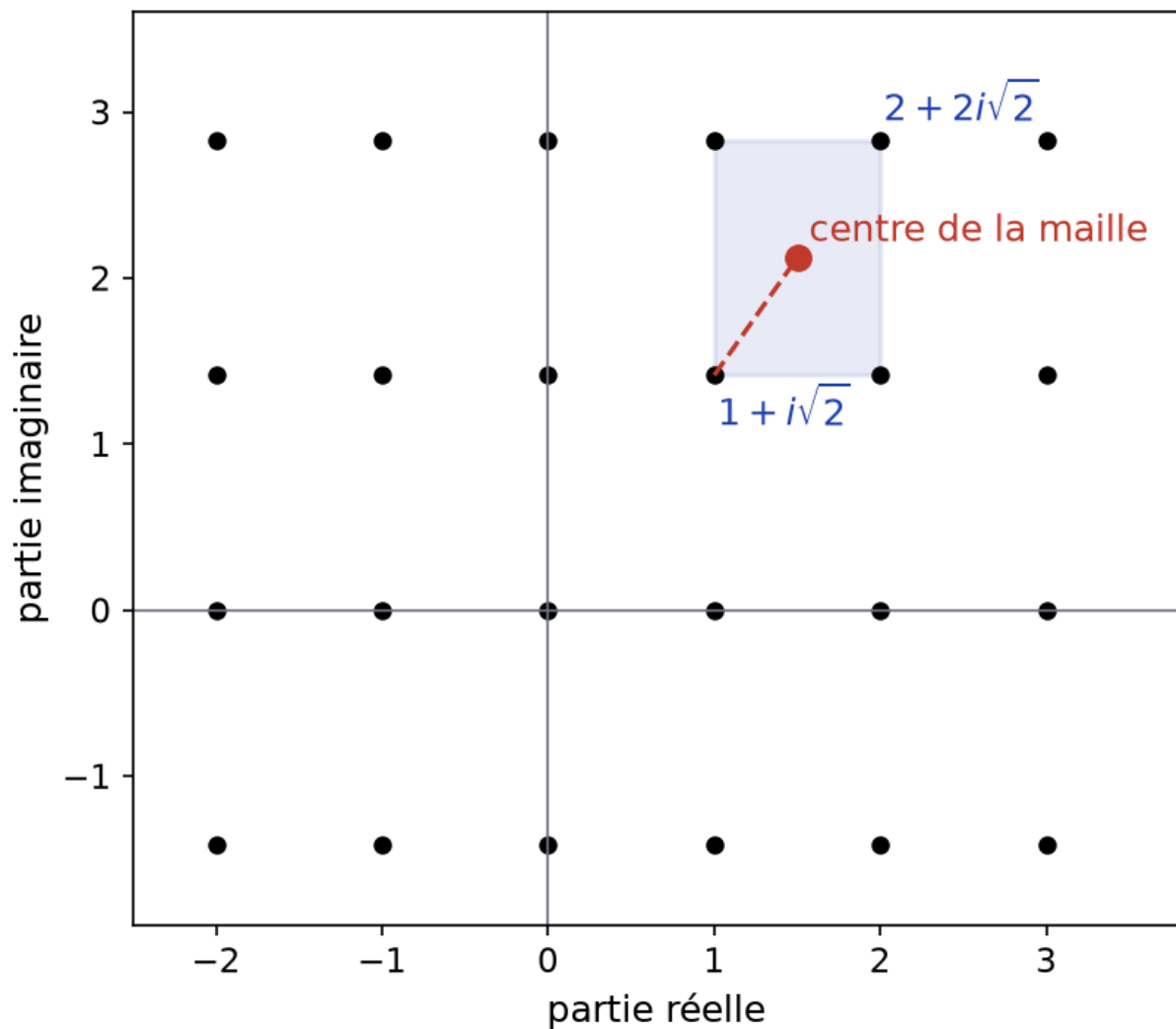
Exercice 10 : Corps des fractions d'anneaux quadratiques

1. Montrer que $\mathbb{Q}(i) = \left\{ \frac{a+ib}{a+b\sqrt{2}} \mid a, b \in \mathbb{Q} \right\}$ est un sous-corps de $\mathbb{C}$. Calculer l'inverse de $3 + 4i$.
2. Montrer que tout élément de $\mathbb{Q}(i)$ est un quotient de deux éléments de $\mathbb{Z}[i]$. En déduire que $\text{Frac}(\mathbb{Z}[i]) \simeq \mathbb{Q}(i)$.
3. On pose $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Montrer de même que $\text{Frac}(\mathbb{Z}[\sqrt{2}]) \simeq \mathbb{Q}(\sqrt{2})$.
4. Calculer l'inverse de $1 + \sqrt{2}$ et celui de $3 + \sqrt{2}$ dans $\mathbb{Q}(\sqrt{2})$. Lequel est inversible dans $\mathbb{Z}[\sqrt{2}]$?

Exercice 11 : Un anneau quadratique euclidien

On note $A = \mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2} \mid a, b \in \mathbb{Z}\}$ et $N(z) = |z|^2$, de sorte que

$N(a + ib\sqrt{2}) = a^2 + 2b^2$. La figure montre le réseau des points de A : ses mailles sont des rectangles de côtés 1 et $\sqrt{2}$.



1. Montrer que $\mathcal{A}$ est un sous-anneau de $\mathbb{C}$, que N est multiplicative et que $\mathcal{A}^\times = \{-1, 1\}$.
2. Montrer que pour tout $z \in \mathbb{C}$ de la forme $x + iy\sqrt{2}$ avec x, y réels, il existe $q \in \mathcal{A}$ tel que $|z - q|^2 \leq \frac{3}{4}$.
3. En déduire que $\mathcal{A}$ est euclidien pour N , donc principal.
4. Effectuer la division euclidienne de $5 + i\sqrt{2}$ par $1 + i\sqrt{2}$. Que peut-on dire du PGCD de ces deux éléments ?
5. Décomposer 3 et 11 en produit d'irréductibles de $\mathcal{A}$.

Exercice 12 : Un anneau quadratique non factoriel

On note $B = \mathbb{Z}[i\sqrt{5}] = \left\{ \begin{matrix} a + ib\sqrt{5}, \\ a, b \in \mathbb{Z} \end{matrix} \right\}$ et $N(a + ib\sqrt{5}) = a^2 + 5b^2$, qui est multiplicative.

1. Montrer que $B^\times = \{-1, 1\}$ et qu'aucun élément de B n'a pour norme 2 ou 3.
2. Montrer que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles et deux à deux non associés.
3. En déduire que B n'est pas factoriel.
4. Montrer que 2 est irréductible mais n'est pas premier dans B .
5. Montrer que l'idéal $I = (2, 1 + i\sqrt{5})$ n'est pas principal. On pourra établir que tout élément $a + ib\sqrt{5}$ de I vérifie $a + b$ pair.

Exercice 13 : Anneaux intègres finis

1. Montrer qu'un anneau intègre fini est un corps.
2. En déduire que dans un anneau fini, tout idéal premier est maximal.
3. Retrouver que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
4. On pose $F = \mathbb{F}_2[X]/(X^2 + X + 1)$ et x la classe de X . Écrire la table de multiplication de $F = \{0, 1, x, x + 1\}$ et vérifier que F est un corps.

Exercice 14 : Polynômes irréductibles sur le corps à deux éléments

On travaille dans $\mathbb{F}_2[X]$, où $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

1. Déterminer les polynômes irréductibles de degré 1 et 2.
2. Déterminer les polynômes irréductibles unitaires de degré 3.
3. Montrer que $X^4 + X + 1$ est irréductible.
4. On pose $K = \mathbb{F}_2[X]/(X^3 + X + 1)$ et α la classe de X . Justifier que K est un corps à 8 éléments. Calculer α^{-1} , puis les puissances α^k pour $3 \leq k \leq 7$. Que peut-on dire du groupe $K^\times$?

Exercice 15 : Critère d'Eisenstein

1. Montrer que $X^5 - 6X^3 + 12X + 3$ est irréductible dans $\mathbb{Q}[X]$.
2. Montrer que $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$ pour tout $n \geq 1$. En déduire que $\sqrt[n]{2}$ est irrationnel pour $n \geq 2$.
3. Montrer que P est irréductible dans $\mathbb{Q}[X]$ si et seulement si $P(X+1)$ l'est. En déduire que $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$.
4. Soit p premier. Montrer que $\Phi_p = X^{p-1} + X^{p-2} + \dots + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 16 : Irréductibilité par réduction modulo p

1. Soit $P \in \mathbb{Z}[X]$ de degré $n \geq 1$ et p un premier qui ne divise pas le coefficient dominant de P . Montrer que si la réduction $\bar{P} \in \mathbb{F}_p[X]$ est irréductible, alors P est irréductible dans $\mathbb{Q}[X]$.
2. Montrer que $X^3 + 4X^2 + 3X + 5$ est irréductible dans $\mathbb{Q}[X]$. Retrouver ce résultat en cherchant ses racines rationnelles.
3. Montrer que $X^4 + 5X + 7$ est irréductible dans $\mathbb{Q}[X]$ (on pourra utiliser l'exercice 14).
4. Montrer que la réciproque de la question 1 est fautive : factoriser $X^4 + 1$ dans $\mathbb{F}_2[X]$ et dans $\mathbb{F}_3[X]$, alors qu'il est irréductible sur $\mathbb{Q}$.

Exercice 17 : Contenu et lemme de Gauss

1. Calculer le contenu de $P = 6X^3 + 9X^2 - 15$ et de $Q = 10X^2 - 4$, puis celui de PQ . Vérifier la relation $c(PQ) = c(P)c(Q)$.
2. Démontrer le lemme de Gauss dans $\mathbb{Z}[X]$: le produit de deux polynômes primitifs est primitif.
3. Soit $P \in \mathbb{Z}[X]$ unitaire. On suppose $P = QR$ avec $Q, R \in \mathbb{Q}[X]$ unitaires. Montrer que $Q, R \in \mathbb{Z}[X]$.
4. En déduire qu'une racine rationnelle d'un polynôme unitaire à coefficients entiers est un entier. Application : $\sqrt{2}$ et $\sqrt[3]{5}$ sont irrationnels.
5. Le polynôme $2X^2 + 2$ est-il irréductible dans $\mathbb{Q}[X]$? dans $\mathbb{Z}[X]$? Décomposer $6X^2 + 12X + 6$ en produit d'irréductibles de $\mathbb{Z}[X]$.

Exercice 18 : Division euclidienne et Bézout dans $\mathbb{Z}[i]$

On pose $a = 11 + 3i$ et $b = 1 + 8i$.

1. Calculer $N(a)$ et $N(b)$.
2. Appliquer l'algorithme d'Euclide dans $\mathbb{Z}[i]$ à a et b . En déduire un PGCD d de a et b .
3. Trouver $u, v \in \mathbb{Z}[i]$ tels que $au + bv = d$, et en déduire l'idéal (a, b) .
4. Décomposer a et b en produit d'irréductibles et retrouver le résultat.

Exercice 19 : Factorisation en irréductibles dans $\mathbb{Z}[i]$

1. Montrer que si $N(z)$ est un nombre premier, alors z est irréductible dans $\mathbb{Z}[i]$.

- Décomposer 2 , 5 , 13 et 65 en produit d'irréductibles de $\mathbb{Z}[i]$.
- Montrer qu'un nombre premier $p \equiv 3 \pmod{4}$ est irréductible dans $\mathbb{Z}[i]$.
- Décomposer $7 + i$ en produit d'irréductibles.
- Déterminer le nombre de couples $(x, y) \in \mathbb{Z}^2$ tels que $x^2 + y^2 = 65$.

Exercice 20 : Théorème des deux carrés

Soit p un nombre premier tel que $p \equiv 1 \pmod{4}$.

- Montrer le théorème de Wilson : $(p-1)! \equiv -1 \pmod{p}$.
- On pose $x = \left(\frac{p-1}{2}\right)!$. Montrer que $x^2 \equiv -1 \pmod{p}$.
- Montrer que p n'est pas premier dans $\mathbb{Z}[i]$, puis qu'il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.
- Cas $p = 13$: calculer x modulo 13 , puis un PGCD de 13 et $x + i$ par l'algorithme d'Euclide. En déduire une écriture $13 = a^2 + b^2$.
- Cas $p = 29$: sachant que $12^2 \equiv -1 \pmod{29}$, écrire 29 comme somme de deux carrés par la même méthode.

Exercice 21 : Problème : une équation diophantienne dans $\mathbb{Z}[i]$

On cherche les couples $(x, y) \in \mathbb{Z}^2$ tels que $x^2 + 1 = y^3$.

1. Montrer que tout inversible de $\mathbb{Z}[i]$ est un cube dans $\mathbb{Z}[i]$.
2. Soit (x, y) une solution. Montrer que x est pair et y impair.
3. Montrer que $x + i$ et $x - i$ sont premiers entre eux dans $\mathbb{Z}[i]$.
4. Soit R un anneau factoriel et $u, v, w \in R$ non nuls avec $uv = w^3$, u et v premiers entre eux. Montrer que u est le produit d'un inversible et d'un cube.
5. En déduire qu'il existe $a, b \in \mathbb{Z}$ tels que $x + i = (a + ib)^3$, puis résoudre l'équation.

Le corrigé des exercices

Chaque exercice est corrigé en détail, question par question, sur la page suivante.



Pour aller plus loin en L3

- Le cours : [anneaux et idéaux, cours de maths en L3](#)
- 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](#)