

# Anneaux et idéaux

## I. Anneaux commutatifs et morphismes d'anneaux

Ce chapitre prolonge l'étude des groupes. En effet, un anneau est un groupe additif muni d'une seconde loi compatible. Dans tout le chapitre, les anneaux sont commutatifs et unitaires. Le but est d'unifier l'arithmétique de  $\mathbb{Z}$  et celle de  $K[X]$  : ces deux anneaux partagent les mêmes théorèmes, et une seule théorie suffit à les démontrer.

### Définition :

Un anneau commutatif est un triplet  $(A, +, \times)$  tel que  $(A, +)$  est un groupe abélien, la loi  $\times$  est associative, commutative, distributive sur  $+$ , et admet un élément neutre noté  $1$ . Un élément  $a$  est inversible s'il existe  $b \in A$  tel que  $ab = 1$ . Les inversibles forment un groupe multiplicatif noté  $A^\times$ . Enfin, un corps est un anneau non nul dans lequel  $A^\times = A \setminus \{0\}$ .

### Exemple :

Les ensembles  $\mathbb{Z}$ ,  $\mathbb{Z}/n\mathbb{Z}$ ,  $K[X]$  pour un corps  $K$ , l'anneau  $\mathcal{C}([0,1], \mathbb{R})$  des fonctions continues et l'anneau  $\mathbb{Z}[i] = \left\{ \begin{smallmatrix} a + ib, \\ a, b \in \mathbb{Z} \end{smallmatrix} \right\}$  sont des anneaux commutatifs. De plus, si  $A$  et  $B$  sont des anneaux, le produit  $A \times B$  est un anneau pour les lois composante par composante. On a par exemple  $\mathbb{Z}^\times = \{-1, 1\}$  et  $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$ .

Un sous-anneau de  $A$  est une partie qui contient  $1$  et qui est stable par différence et par produit. Ensuite, on compare deux anneaux grâce aux morphismes.

### Définition :

Une application  $f : A \rightarrow B$  est un morphisme d'anneaux si, pour tous  $a, b \in A$ ,  $f(a + b) = f(a) + f(b)$ ,  $f(ab) = f(a)f(b)$  et  $f(1_A) = 1_B$ . Son noyau est  $\ker f = f^{-1}(\{0\})$ . Un morphisme bijectif est un isomorphisme.

### Propriété :

Soit  $f : A \rightarrow B$  un morphisme d'anneaux. Alors  $f(A^\times) \subset B^\times$ , l'image  $f(A)$  est un sous-anneau de  $B$ , et  $f$  est injectif si et seulement si  $\ker f = \{0\}$ . Par ailleurs, pour tout anneau  $A$ , il existe un unique morphisme  $\mathbb{Z} \rightarrow A$ , à savoir  $n \rightarrow n \cdot 1_A$ .

### Exemple :

L'évaluation  $\mathbb{R}[X] \rightarrow \mathbb{C}$ ,  $P \rightarrow P(i)$ , est un morphisme d'anneaux. Son image est  $\mathbb{C}$  tout entier, car  $a + bX$  a pour image  $a + ib$ . En revanche, son noyau contient  $X^2 + 1$ , donc elle n'est pas injective.

## II. Idéaux et anneaux quotients

Le noyau d'un morphisme n'est pas un sous-anneau en général, puisqu'il ne contient pas  $1$ . Il possède cependant une propriété d'absorption. Cette propriété définit les idéaux, qui jouent pour les anneaux le rôle des sous-groupes distingués pour les groupes.

### Définition :

Un idéal de  $A$  est un sous-groupe  $I$  de  $(A, +)$  tel que, pour tous  $a \in A$  et  $x \in I$ , on a

$ax \in I$ . L'idéal engendré par  $a_1, \dots, a_n$  est  $(a_1, \dots, a_n) = a_1 A + \dots + a_n A$ . Un idéal de la forme  $(a) = aA$  est dit principal.

### Propriété :

Le noyau d'un morphisme est un idéal. De plus, un idéal  $I$  est égal à  $A$  si et seulement s'il contient  $1$ , si et seulement s'il contient un inversible. Par conséquent, un anneau non nul  $A$  est un corps si et seulement si ses seuls idéaux sont  $\{0\}$  et  $A$ . En particulier, tout morphisme d'un corps vers un anneau non nul est injectif.

### Théorème :

Les idéaux de  $\mathbb{Z}$  sont exactement les  $n\mathbb{Z}$  avec  $n \in \mathbb{N}$ .

### Démonstration :

Soit  $I$  un idéal non nul. Il contient un plus petit entier  $n > 0$ , car  $x \in I$  entraîne  $-x \in I$ . D'abord,  $n\mathbb{Z} \subset I$  par absorption. Ensuite, pour  $x \in I$ , la division euclidienne donne  $x = qn + r$  avec  $0 \leq r < n$ . Or  $r = x - qn \in I$ , donc  $r = 0$  par minimalité de  $n$ . Ainsi  $I = n\mathbb{Z}$ .

Les idéaux se combinent. La somme  $I + J$  et l'intersection  $I \cap J$  sont des idéaux, ainsi que le produit  $IJ$ , engendré par les produits  $xy$ . Par exemple, dans  $\mathbb{Z}$ , on a  $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$  et  $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$  : le PGCD et le PPCM apparaissent naturellement.

## 1. Construction de l'anneau quotient

### Théorème :

Soit  $I$  un idéal de  $A$ . La relation  $a \equiv b \pmod{I} \Leftrightarrow a - b \in I$  est une relation d'équivalence. L'ensemble quotient  $A/I$  est muni d'une unique structure d'anneau telle que la surjection canonique  $\pi : A \rightarrow A/I, a \rightarrow \bar{a}$ , soit un morphisme. Son noyau est  $I$ .

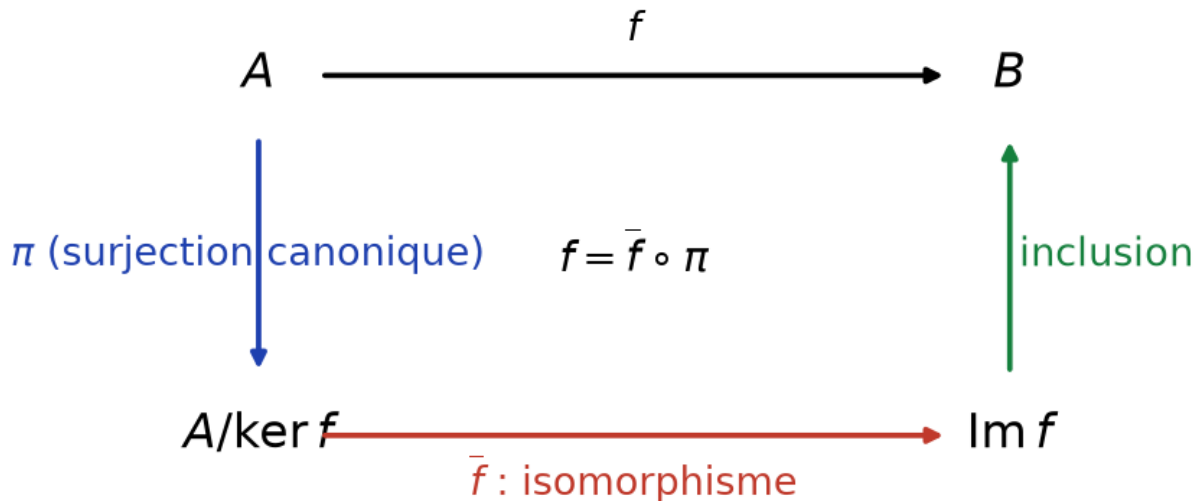
### Démonstration :

Le groupe quotient  $A/I$  existe déjà, car  $I$  est un sous-groupe du groupe abélien  $A$ . Il reste à vérifier que le produit  $\bar{a}\bar{b} = \overline{ab}$  ne dépend pas des représentants. Si  $a' = a + x$  et  $b' = b + y$  avec  $x, y \in I$ , alors  $a'b' - ab = ay + xb + xy$ . Chaque terme appartient à  $I$  par absorption. Les axiomes d'anneau passent ensuite au quotient.

### Théorème :

Théorème de factorisation. Soit  $f : A \rightarrow B$  un morphisme d'anneaux. Alors  $f$  induit un isomorphisme  $\bar{f} : A/\ker f \rightarrow f(A)$ , défini par  $\bar{f}(\bar{a}) = f(a)$ .

Le diagramme ci-dessous résume la situation : tout morphisme se décompose en une surjection canonique, un isomorphisme et une inclusion.



### Méthode :

Pour identifier un quotient  $A/I$ , on cherche un morphisme surjectif  $f: A \rightarrow B$  de noyau exactement  $I$ . Le théorème de factorisation donne alors  $A/I \simeq B$ . En pratique, on vérifie trois points :  $f$  est un morphisme,  $f$  est surjectif, et  $\ker f = I$ . L'inclusion  $I \subset \ker f$  est souvent immédiate ; l'inclusion réciproque demande une division euclidienne.

### Exemple :

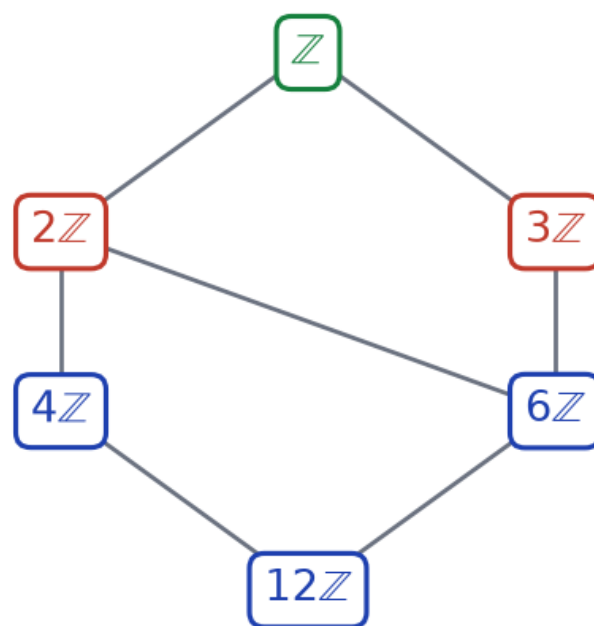
Montrons que  $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$ . L'évaluation  $f: P \rightarrow P(i)$  est surjective. Si  $P(i) = 0$ , on divise :  $P = (X^2 + 1)Q + aX + b$  avec  $a, b$  réels. Alors  $ai + b = 0$ , donc  $a = b = 0$ . Ainsi  $\ker f = (X^2 + 1)$ , et le quotient est isomorphe à  $\mathbb{C}$ .

## 2. Idéaux d'un quotient

### Proposition :

Les idéaux de  $A/I$  sont en bijection avec les idéaux  $J$  de  $A$  qui contiennent  $I$ , par  $J \rightarrow \pi(J) = J/I$ . Cette bijection respecte l'inclusion, et  $(A/I)/(J/I) \simeq A/J$ .

Par exemple, les idéaux de  $\mathbb{Z}/12\mathbb{Z}$  correspondent aux idéaux  $d\mathbb{Z}$  avec  $d$  diviseur de  $12$ . La figure suivante les range par inclusion ; les plus grands idéaux propres sont en rouge.



en rouge : idéaux maximaux

Remarque :

Si  $I + J = A$ , le lemme chinois affirme que  $A/(I \cap J) \simeq A/I \times A/J$ . Ainsi, pour  $m$  et  $n$  premiers entre eux,  $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ .

### III. Idéaux premiers, idéaux maximaux et intégrité

Dans  $\mathbb{Z}$ , on ne peut pas avoir  $ab = 0$  avec  $a$  et  $b$  non nuls. Cette propriété d'intégrité se perd dans  $\mathbb{Z}/6\mathbb{Z}$ , où  $\bar{2} \times \bar{3} = \bar{0}$ . Les idéaux premiers mesurent précisément ce phénomène.

#### Définition :

Un anneau  $A$  est intègre s'il est non nul et si  $ab = 0$  entraîne  $a = 0$  ou  $b = 0$ . Un idéal  $P \neq A$  est premier si  $ab \in P$  entraîne  $a \in P$  ou  $b \in P$ . Un idéal  $M \neq A$  est maximal si les seuls idéaux contenant  $M$  sont  $M$  et  $A$ .

#### Théorème :

Soit  $I$  un idéal de  $A$ . Alors  $I$  est premier si et seulement si  $A/I$  est intègre, et  $I$  est maximal si et seulement si  $A/I$  est un corps. Par conséquent, tout idéal maximal est premier.

#### Démonstration :

La première équivalence traduit la définition :  $\bar{a}\bar{b} = \bar{0}$  signifie  $ab \in I$ , et  $\bar{a} = \bar{0}$  signifie  $a \in I$ . Pour la seconde, on utilise la correspondance des idéaux. En effet,  $I$  est maximal si et seulement si  $A/I$  n'a que deux idéaux,  $\{0\}$  et lui-même. D'après la partie II, cela équivaut à dire que  $A/I$  est un corps. Enfin, un corps est intègre, donc un idéal maximal est premier.

#### Exemple :

Dans  $\mathbb{Z}$ , les idéaux premiers sont  $\{0\}$  et les  $p\mathbb{Z}$  avec  $p$  premier, car  $\mathbb{Z}/n\mathbb{Z}$  est intègre si et seulement si  $n$  est premier. Les  $p\mathbb{Z}$  sont maximaux, alors que  $\{0\}$  est premier sans être maximal. De même, dans  $\mathbb{Z}[X]$ , l'idéal  $(X)$  est premier, car  $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$ , mais il n'est pas maximal.

### Théorème :

Théorème de Krull (admis). Dans un anneau non nul, tout idéal propre est contenu dans un idéal maximal. La preuve générale repose sur le lemme de Zorn.

## 1. Corps des fractions

Un anneau intègre se plonge dans un corps, exactement comme  $\mathbb{Z}$  se plonge dans  $\mathbb{Q}$ . La construction reprend celle des rationnels.

### Théorème :

Soit  $A$  intègre. Sur  $A \times (A \setminus \{0\})$ , la relation  $(a, b) \sim (c, d) \Leftrightarrow ad = bc$  est une relation d'équivalence. L'ensemble des classes, noté  $\text{Frac}(A)$ , est un corps pour  $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$  et  $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ . De plus,  $a \rightarrow \frac{a}{1}$  est injectif. Enfin, tout morphisme injectif de  $A$  dans un corps  $L$  se prolonge de façon unique en un morphisme  $\text{Frac}(A) \rightarrow L$ .

### Exemple :

On a  $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$  et  $\text{Frac}(K[X]) = K(X)$ , le corps des fractions rationnelles. Par ailleurs,  $\text{Frac}(\mathbb{Z}[i]) \simeq \mathbb{Q}(i) = \left\{ \frac{a+ib}{c+id}, a, b, c, d \in \mathbb{Z} \right\}$ . Par exemple,  $\frac{1}{3+4i} = \frac{3-4i}{25}$ .

## IV. Anneaux euclidiens, principaux et factoriels

## 1. Divisibilité dans un anneau intègre

Soit  $A$  un anneau intègre. On dit que  $a$  divise  $b$  s'il existe  $c$  tel que  $b = ac$ , ce qui équivaut à  $(b) \subset (a)$ . Ainsi, la divisibilité se lit sur les idéaux.

### Définition :

Deux éléments  $a$  et  $b$  sont associés si  $a = ub$  avec  $u \in A^\times$ , ce qui équivaut à  $(a) = (b)$ . Un élément  $p$  non nul et non inversible est irréductible si  $p = ab$  entraîne  $a$  ou  $b$  inversible. Il est premier si  $p \mid ab$  entraîne  $p \mid a$  ou  $p \mid b$ , autrement dit si  $(p)$  est un idéal premier.

### Propriété :

Dans un anneau intègre, tout élément premier est irréductible. En effet, si  $p = ab$ , alors  $p$  divise  $a$  ou  $b$ ; disons  $a = pc$ . Alors  $p = pcb$ , donc  $cb = 1$  par intégrité, et  $b$  est inversible.

## 2. Anneaux euclidiens et principaux

### Définition :

Un anneau intègre  $A$  est principal si tous ses idéaux sont principaux. Il est euclidien s'il existe une application  $v : A \setminus \{0\} \rightarrow \mathbb{N}$ , appelée stathme, telle que pour tous  $a$  et  $b \neq 0$ , il existe  $q, r$  avec  $a = bq + r$  et ( $r = 0$  ou  $v(r) < v(b)$ ).

### Théorème :

Tout anneau euclidien est principal.

### Démonstration :

Soit  $I$  un idéal non nul. On choisit  $b \in I$  non nul de stathme minimal. D'abord,  $(b) \subset I$ . Ensuite, pour  $a \in I$ , on écrit  $a = bq + r$ . Or  $r = a - bq \in I$ , donc  $r = 0$  par minimalité de  $v(b)$ . Ainsi  $I = (b)$ . La preuve reprend donc exactement celle donnée pour  $\mathbb{Z}$ .

### Méthode :

Pour montrer qu'un anneau est euclidien, on propose un stathme naturel : la valeur absolue dans  $\mathbb{Z}$ , le degré dans  $K[X]$ , la norme  $N(a + ib) = a^2 + b^2$  dans  $\mathbb{Z}[i]$ . Ensuite, on construit le quotient par une approximation : on calcule le quotient exact dans le corps des fractions, puis on l'arrondit. Il reste à contrôler l'erreur d'arrondi. À l'inverse, pour montrer qu'un anneau n'est pas principal, on exhibe un idéal à deux générateurs qui n'est pas principal, comme  $(2, X)$  dans  $\mathbb{Z}[X]$ .

### Théorème :

Soit  $A$  principal. Pour  $a, b \in A$ , on a  $(a) + (b) = (d)$ , et  $d$  est un PGCD de  $a$  et  $b$  : c'est la relation de Bézout  $d = au + bv$ . De plus, pour  $p \neq 0$ , les conditions suivantes sont équivalentes :  $p$  est irréductible ;  $p$  est premier ; l'idéal  $(p)$  est maximal. Enfin, tout idéal premier non nul est maximal.

### Démonstration :

Supposons  $p$  irréductible et soit  $(p) \subset (c)$ . Alors  $p = cd$ , donc  $c$  est inversible, auquel cas  $(c) = A$ , ou  $d$  est inversible, auquel cas  $(c) = (p)$ . Ainsi  $(p)$  est maximal, donc premier. Réciproquement, un élément premier est irréductible. Enfin, un idéal premier non nul  $(p)$  a un

générateur premier, donc irréductible, donc  $(p)$  est maximal.

### 3. Anneaux factoriels

#### Définition :

Un anneau intègre  $A$  est factoriel si tout élément non nul et non inversible s'écrit comme produit d'irréductibles, et si cette écriture est unique à l'ordre des facteurs et aux inversibles près.

#### Théorème :

Tout anneau principal est factoriel (admis ici ; l'existence repose sur le fait qu'une suite croissante d'idéaux d'un anneau principal est stationnaire). Dans un anneau factoriel, un élément est irréductible si et seulement s'il est premier : c'est le lemme d'Euclide. Deux éléments y ont toujours un PGCD, lu sur les décompositions.

#### Attention :

Un anneau factoriel n'est pas forcément principal :  $\mathbb{Z}[X]$  est factoriel sans être principal. À l'inverse, certains anneaux intègres ne sont pas factoriels. Dans  $\mathbb{Z}[i\sqrt{5}]$ , on a  $6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ , et ces quatre facteurs sont irréductibles et deux à deux non associés.

Comme le montre la figure ci-dessous, ces classes d'anneaux sont emboîtées. Chaque inclusion est stricte ; l'anneau  $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$  est un exemple classique d'anneau principal non euclidien, dont la preuve dépasse ce cours.

## Anneaux intègres

ex. :  $\mathbb{Z}[i\sqrt{5}]$

### Anneaux factoriels

ex. :  $\mathbb{Z}[X], K[X, Y]$

### Anneaux principaux

ex. :  $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$

### Anneaux euclidiens

ex. :  $\mathbb{Z}, \mathbb{Z}[i], K[X]$

### Corps

ex. :  $\mathbb{Q}, \mathbb{R}, \mathbb{Z}/p\mathbb{Z}$

## V. L'anneau des polynômes $K[X]$ et l'irréductibilité

Soit  $K$  un corps. La division euclidienne des polynômes fait de  $K[X]$  un anneau euclidien pour le degré. Par conséquent,  $K[X]$  est principal et factoriel. Tout idéal non nul s'écrit  $(P)$  avec  $P$  unitaire, et ce générateur est unique.

### Théorème :

Soit  $P \in K[X]$  de degré  $n \geq 1$ . Alors  $K[X]/(P)$  est un  $K$ -espace vectoriel de dimension  $n$ , de base  $\overline{1}, \overline{X}, \dots, \overline{X}^{n-1}$ . C'est un corps si et seulement si  $P$  est irréductible.

### Propriété :

Un polynôme de degré 2 ou 3 est irréductible sur  $K$  si et seulement s'il n'a pas de racine dans  $K$ . Les irréductibles de  $\mathbb{C}[X]$  sont les polynômes de degré 1. Ceux de  $\mathbb{R}[X]$  sont les polynômes de degré 1 et ceux de degré 2 à discriminant strictement négatif.

### Attention :

Le critère des racines est faux en degré 4. Par exemple,  $X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2)$  n'a aucune racine réelle, mais il est réductible sur  $\mathbb{Q}$ .

### Exemple :

Sur le corps  $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ , le polynôme  $X^2 + X + 1$  n'a pas de racine, car il vaut 1 en 0 et en 1. Il est donc irréductible. Ainsi  $\mathbb{F}_2[X]/(X^2 + X + 1)$  est un corps à quatre éléments  $0, 1, \alpha, \alpha + 1$ , avec  $\alpha^2 = \alpha + 1$ .

## VI. Polynômes sur un anneau factoriel : lemme de Gauss

Sur  $\mathbb{Q}$ , la question de l'irréductibilité se ramène à  $\mathbb{Z}$ . Pour cela, on sépare dans un polynôme à coefficients entiers une partie numérique et une partie primitive. Dans cette partie,  $A$  est factoriel et  $K = \text{Frac}(A)$ .

### Définition :

Le contenu  $c(P)$  d'un polynôme non nul  $P \in A[X]$  est un PGCD de ses coefficients, défini à un

inversible près. Le polynôme  $P$  est primitif si  $c(P)$  est inversible. Par exemple, dans  $\mathbb{Z}[X]$ ,  $c(6X^2 + 9X - 15) = 3$ .

### Lemme :

Lemme de Gauss. Le produit de deux polynômes primitifs est primitif. Plus généralement,  $c(PQ) = c(P)c(Q)$  à un inversible près.

### Démonstration :

Soient  $P = \sum a_k X^k$  et  $Q = \sum b_k X^k$  primitifs. Supposons qu'un irréductible  $p$  divise tous les coefficients de  $PQ$ . Comme  $p$  est premier,  $A/(p)$  est intègre, donc  $(A/(p))[X]$  aussi. Or la réduction modulo  $p$  donne  $\overline{P}\overline{Q} = \overline{PQ} = 0$ . Par conséquent,  $\overline{P} = 0$  ou  $\overline{Q} = 0$ , ce qui contredit la primitivité. Le cas général s'en déduit en écrivant  $P = c(P)P_1$  et  $Q = c(Q)Q_1$ .

### Corollaire :

Un polynôme  $P \in A[X]$  de degré au moins 1 est irréductible dans  $A[X]$  si et seulement s'il est primitif et irréductible dans  $K[X]$ . De plus, si  $A$  est factoriel, alors  $A[X]$  est factoriel. Ainsi  $\mathbb{Z}[X]$  et  $K[X, Y] = K[X][Y]$  sont factoriels, sans être principaux.

### Théorème :

Critère d'Eisenstein. Soit  $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$  et  $p$  un nombre premier. Si  $p \nmid a_n$ , si  $p \mid a_k$  pour  $k < n$  et si  $p^2 \nmid a_0$ , alors  $P$  est irréductible dans  $\mathbb{Q}[X]$ .

### Démonstration :

Supposons  $P = QR$  dans  $\mathbb{Q}[X]$  avec  $\deg Q, \deg R \geq 1$ . D'après le lemme de Gauss, on peut prendre  $Q, R \in \mathbb{Z}[X]$ . Modulo  $p$ , on obtient  $\overline{a_n} X^n = \overline{Q} \overline{R}$  dans  $\mathbb{F}_p[X]$ . Par factoriabilité de  $\mathbb{F}_p[X]$ , on a  $\overline{Q} = \lambda X^k$  et  $\overline{R} = \mu X^{n-k}$ , avec  $k = \deg Q$  et  $n - k = \deg R$ , car  $p$  ne divise pas les coefficients dominants. Ainsi  $p$  divise les termes constants de  $Q$  et de  $R$ , donc  $p^2$  divise  $a_0$ . C'est absurde.

### Méthode :

Pour prouver qu'un polynôme de  $\mathbb{Z}[X]$  est irréductible sur  $\mathbb{Q}$ , on essaie dans l'ordre : l'absence de racine rationnelle en degré 2 ou 3 ; le critère d'Eisenstein, éventuellement après la substitution  $X \rightarrow X + a$ , qui préserve l'irréductibilité ; la réduction modulo un premier  $p$  ne divisant pas le coefficient dominant. En effet, si  $\overline{P}$  est irréductible dans  $\mathbb{F}_p[X]$  et de même degré que  $P$ , alors  $P$  est irréductible sur  $\mathbb{Q}$ .

### Exemple :

Pour  $p$  premier,  $\Phi_p = X^{p-1} + \dots + X + 1$  est irréductible sur  $\mathbb{Q}$ . En effet, 
$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{k=1}^p \binom{p}{k} X^{k-1}.$$
 Or  $p$  divise  $\binom{p}{k}$  pour  $1 \leq k \leq p-1$ , et le terme constant vaut  $p$ . Le critère d'Eisenstein s'applique donc.

## VII. L'anneau des entiers de Gauss

L'anneau  $\mathbb{Z}[i]$  illustre toute la théorie. D'abord, on y dispose d'une division euclidienne. Ensuite, sa factorisation répond à une question d'arithmétique classique : quels entiers sont sommes de deux carrés ?

### Définition :

La norme de  $z = a + ib \in \mathbb{Z}[i]$  est  $N(z) = z\bar{z} = a^2 + b^2 \in \mathbb{N}$ . Elle est multiplicative :  $N(zw) = N(z)N(w)$ . Par conséquent,  $z$  est inversible si et seulement si  $N(z) = 1$ , d'où  $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$ .

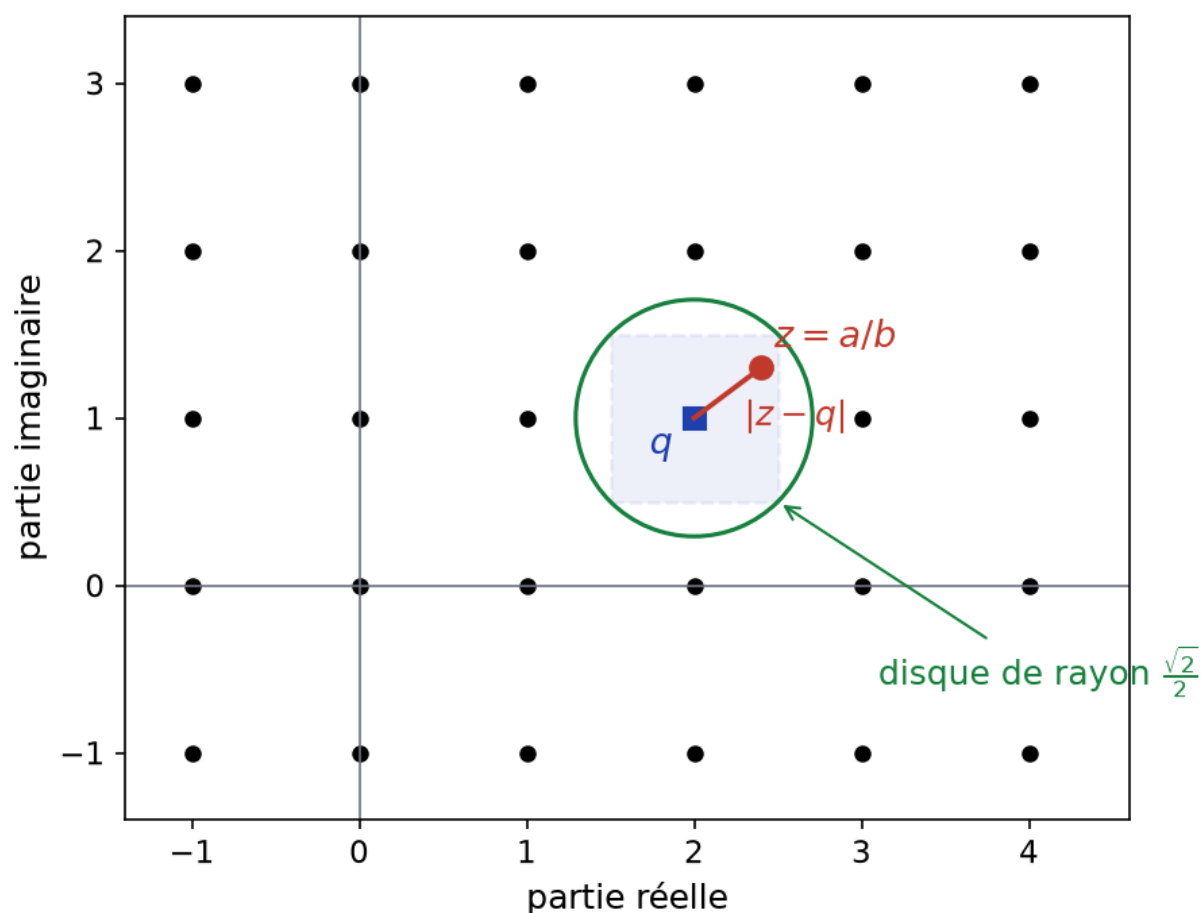
### Théorème :

L'anneau  $\mathbb{Z}[i]$  est euclidien pour la norme  $N$ . Il est donc principal et factoriel.

### Démonstration :

Soient  $a, b \in \mathbb{Z}[i]$  avec  $b \neq 0$ . Le quotient exact  $z = a/b$  est dans  $\mathbb{Q}(i)$ . On choisit  $q \in \mathbb{Z}[i]$  en arrondissant la partie réelle et la partie imaginaire de  $z$  à l'entier le plus proche. Alors  $|z - q|^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$ . On pose  $r = a - bq \in \mathbb{Z}[i]$ . Ainsi  $N(r) = |b|^2 |z - q|^2 \leq \frac{1}{2} N(b) < N(b)$ .

La figure suivante illustre cet arrondi : tout point du plan est à distance au plus  $\frac{\sqrt{2}}{2}$  d'un point du réseau  $\mathbb{Z}[i]$ , c'est-à-dire du centre de sa maille carrée.



### Exemple :

Divisons  $a = 7 + 2i$  par  $b = 2 - i$ . On a

$$\frac{a}{b} = \frac{(7 + 2i)(2 + i)}{5} = \frac{12 + 11i}{5} = 2,4 + 2,2i. \text{ On arrondit en } q = 2 + 2i. \text{ Alors}$$

$$r = a - bq = 7 + 2i - (6 + 2i) = 1, \text{ et } N(r) = 1 < 5 = N(b).$$

### Théorème :

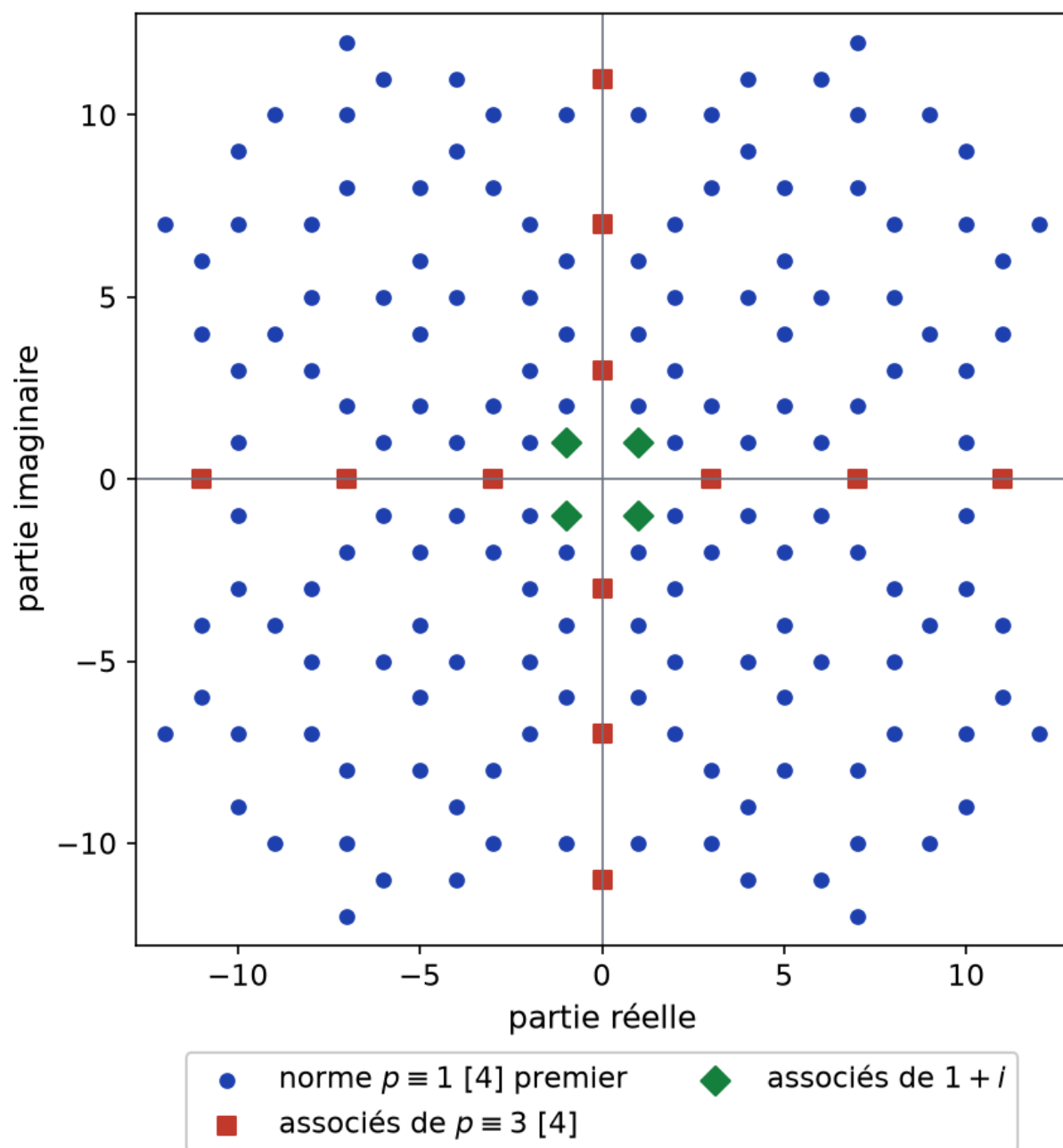
Les irréductibles de  $\mathbb{Z}[i]$  sont, à association près :  $1 + i$  ; les nombres premiers  $p \equiv 3 \pmod{4}$  ; les

$a + ib$  tels que  $a^2 + b^2 = p$  soit un nombre premier  $p \equiv 1 \pmod{4}$ . Par conséquent, un nombre premier  $p$  est somme de deux carrés si et seulement si  $p = 2$  ou  $p \equiv 1 \pmod{4}$ .

### Démonstration :

Soit  $\pi$  irréductible. Il divise  $N(\pi) = \pi \bar{\pi}$ , donc il divise un nombre premier  $p$ , car  $\pi$  est premier dans l'anneau factoriel  $\mathbb{Z}[i]$ . Alors  $N(\pi)$  divise  $N(p) = p^2$ . Si  $N(\pi) = p$ , on a  $p = a^2 + b^2$ . Sinon  $N(\pi) = p^2$ ,  $\pi$  est associé à  $p$ , et  $p$  est irréductible. Or un carré vaut 0 ou 1 modulo 4, donc  $p \equiv 3 \pmod{4}$  n'est jamais somme de deux carrés. Enfin, le cas  $p \equiv 1 \pmod{4}$  se traite grâce au théorème de Wilson, qui fournit  $x$  avec  $p \mid x^2 + 1$ .

La figure ci-dessous représente les irréductibles de norme modérée. On y voit leur symétrie : si  $\pi$  est irréductible, ses associés  $i\pi$ ,  $-\pi$ ,  $-i\pi$  et son conjugué  $\bar{\pi}$  le sont aussi.



### Méthode :

Pour résoudre un problème arithmétique dans  $\mathbb{Z}[i]$ , on passe par la norme. Elle transforme une égalité dans  $\mathbb{Z}[i]$  en égalité d'entiers, ce qui borne les diviseurs possibles. Ensuite, on utilise la factoriabilité : on décompose en irréductibles et on compare les exposants. Par exemple,  $5 = (2 + i)(2 - i)$  et  $2 = -i(1 + i)^2$ .

## Ce qu'il faut retenir

---

- Un idéal est un sous-groupe additif absorbant ; les noyaux de morphismes sont exactement les idéaux.
- Pour identifier  $A/I$ , on construit un morphisme surjectif de noyau  $I$  et on applique le théorème de factorisation.
- $I$  est premier si et seulement si  $A/I$  est intègre ;  $I$  est maximal si et seulement si  $A/I$  est un corps.
- Tout anneau intègre possède un corps des fractions, le plus petit corps qui le contient.
- Euclidien entraîne principal, qui entraîne factoriel ; les réciproques sont fausses.
- Dans un anneau principal, irréductible, premier et « engendre un idéal maximal » sont équivalents, et la relation de Bézout est vraie.
- $K[X]/(P)$  est un corps si et seulement si  $P$  est irréductible sur  $K$ .
- Le lemme de Gauss ramène l'irréductibilité sur  $\mathbb{Q}$  à celle sur  $\mathbb{Z}$  ; Eisenstein et la réduction modulo  $p$  la prouvent.
- $\mathbb{Z}[i]$  est euclidien pour la norme  $a^2 + b^2$ , et ses irréductibles décrivent les sommes de deux carrés.

## Questions fréquentes sur anneaux et idéaux

---

Quelle est la différence entre un élément irréductible et un élément premier ?

Un irréductible ne se décompose pas en produit de deux non-inversibles ; un premier  $p$  vérifie :  $p \mid ab$  entraîne  $p \mid a$  ou  $p \mid b$ . Dans un anneau intègre, premier entraîne irréductible. La réciproque est vraie dans un anneau factoriel, mais fausse en général : dans  $\mathbb{Z}[\sqrt{5}]$ ,  $2$  est irréductible sans être premier.

Comment savoir si un idéal est maximal sans connaître tous les idéaux ?

On calcule le quotient. L'idéal  $I$  est maximal si et seulement si  $A/I$  est un corps, et premier si et

seulement si  $A/I$  est intègre. Pour identifier  $A/I$ , on construit un morphisme surjectif de noyau  $I$ .

Un anneau factoriel est-il toujours principal ?

Non. L'anneau  $\mathbb{Z}[X]$  est factoriel d'après le lemme de Gauss, mais l'idéal  $(2, X)$  n'y est pas principal. Plus généralement,  $A[X]$  est principal si et seulement si  $A$  est un corps.

Le critère d'Eisenstein suffit-il pour tous les polynômes ?

Non, c'est seulement une condition suffisante. Il faut souvent l'appliquer après une substitution  $X \rightarrow X + a$ , comme pour  $X^4 + 1$ . Sinon, on essaie la recherche de racines rationnelles en degré 2 ou 3, ou la réduction modulo un nombre premier bien choisi.

## Pour aller plus loin 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](#)