المدرسة الوطنية للعلوم التطبيقية
ⵜⵉⵎⵙⵙⵓⵜ ⵜⴰⵏⴰⵎⵓⵔⵜ ⵏ ⵜⵙⴽⵏⵉⵡⵉⵏ ⵜⵉⵜⵜⴰⵡⵉⵏ
Ecole Nationale des Sciences Appliquées de Fès

جامعة سيدي محمد بن عبد الله
ⵜⴰⵙⴷⴰⵡⵜ ⵙⵉⴷⵉ ⵎⵓⵃⴰⵎⵎⴷ ⴱⵏ ⵄⴱⴷⵍⵍⴰⵀ
Université Sidi Mohamed Ben Abdellah

Université Sidi Mohammed Ben Abdelah
École Nationale des Sciences Appliquées - Fès
Filière: Cycle préparatoire 2
Quatrième semestre

Cours d'Algèbre IV

Prof : Z. Mazgouri

Fès, le 7 février 2024

TABLE DES MATIÈRES

CHAPITRE 1.

ANNEAUX, MORPHISMES ET IDÉAUX

1. Anneaux et morphismes d'anneaux

1.1 Anneaux

Définition 1 (Anneau).

Soit A un ensemble muni de deux lois de composition internes " $+$ " et "." :

On dit que $(A, +, .)$, ou simplement que A est un **anneau** si :

- $(A, +)$ est un groupe abélien.
- La loi . est associative, i.e., $\forall a, b, c \in A$, on a : $a(bc) = (ab)c$.
- La loi . est distributive par rapport à $+$, i.e., $\forall a, b, c \in A$, on a : $a(b + c) = ab + ac$.

- Si de plus la loi . est commutative, on dit que l'anneau A est commutatif.

- Si un anneau A possède un élément neutre pour la loi ., on dit que l'anneau A est **unitaire**.

Exemple 1 .

1. $(\mathbb{Z}, +, .), (\mathbb{Q}, +, .), (\mathbb{R}, +, .)$ et $(\mathbb{C}, +, .)$ sont des anneaux commutatifs unitaires.
2. Pour $\mathbb{K} = \mathbb{R}, \mathbb{C}$, l'ensemble $\mathbb{K}[X]$ muni de l'addition et de la multiplication usuelles est un anneau commutatif unitaire d'élément unité le polynôme constant égal à 1.

Dans tout ce qui suit, A est un anneau commutatif et unitaire.

Remarque 1 .

1. L'élément neutre pour l'addition 0_A est noté tout simplement 0 et on a $\forall a \in A, a.0 = 0$.
2. L'élément neutre pour la multiplication 1_A est unique, on le note tout simplement 1.
3. On note $-a$ l'opposé de $a \in A$ pour la loi $+$, et on a, $-a = (-1)a$.
4. Si $a \in A$ et si $n \in \mathbb{N}$, on définit par récurrence a^n, en posant $a^0 = 1$ et $a^n = a(a^{n-1})$.
5. $\forall a \in A$ et $\forall m, n \in \mathbb{N}$, $a^{m+n} = a^m a^n$.
6. $\forall a, b \in A$ et $\forall n \in \mathbb{N}$, on a (formule du binôme de Newton) :

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}.$$

Définition 2 (Sous-anneau).

Soit A un anneau. Une partie $B \subset A$ est dite un **sous-anneau** de A si B contient les éléments 0_A et 1_A et si B est stable par addition, multiplication et stable par opposé.
C'est équivalent à : $1_A \in B, \forall x, y \in B$, on a $x - y \in B$ et $xy \in B$.

Exemple 2 .

1. $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.
2. $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{R}$.
3. L'ensemble des fonctions dérivables sur $I \subset \mathbb{R}$ constitue un sous-anneau de l'ensemble des fonctions continues sur I, qui constitue lui-même un sous-anneau de l'ensemble des fonctions de I dans $\mathbb{R}$.

Remarque 2 .

Soit A un anneau. Tout sous-anneau B de A est aussi un anneau avec $0_B = 0_A$ et $1_B = 1_A$.

Définition 3 (Élément inversible).

Un élément $a \in A$ est dit **inversible** s'il existe $b \in A$ tel que $ab = 1$. Cet élément est unique et appelé l'inverse de a. Il est généralement noté a^{-1}.
L'ensemble des éléments inversibles d'un anneau A est noté $U(A)$ (dit aussi l'ensemble des unités de A).

Proposition 1 .

$(U(A), .)$ est un groupe commutatif.

Preuve

Observons d'abord que la multiplication définit une loi interne. En effet, pour tous $a, b \in U(A)$, on a

$$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (a.1_A)a^{-1} = aa^{-1} = 1_A.$$

Ainsi ab est inversible d'inverse $b^{-1}a^{-1}$. Maintenant, il est clair que 1_A est l'élément neutre pour cette loi et que pour $a \in U(A)$ l'élément a^{-1} est son inverse.
De plus, le groupe $(U(A), .)$ est commutatif car A est commutatif.

Exemple 3 .

1. Il est clair que $U(\mathbb{Z}) = \{-1, 1\}$ et $U(\mathbb{Q}) = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ (pour $\frac{a}{b} \in \mathbb{Q}^*$, on a $(\frac{a}{b})^{-1} = \frac{b}{a}$).
2. Pour $n \in \mathbb{N}^*, U(\mathcal{M}_n(\mathbb{R})) = GL_n(\mathbb{R}) = \{M \in \mathcal{M}_n(\mathbb{R}) : det(M) \neq 0\}$.

Exercice 1 *On considère l'ensemble des complexes suivant :* $\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{Z}\}$.

1. *Montrer que* $(\mathbb{Z}[i], +, .)$ *est un anneau commutatif unitaire.*
2. *Déterminer* $U(\mathbb{Z}[i])$.

Définition 4 (Anneau intègre).

Un élément $a \neq 0$ de A est dit diviseur de zéro, s'il existe un élément $b \in A \setminus \{0\}$ tel que $ab = 0$.
Un anneau A non réduit à $\{0\}$ est dit **intègre** si

$$\forall x, y \in A,\ xy = 0 \Longrightarrow x = 0 \text{ ou } y = 0.$$

C'est donc un anneau sans diviseurs de zéro.

Exemple 4 .

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des anneaux intègres.
2. $(\mathcal{M}_2(\mathbb{R}), +, .)$ est un anneau non intègre.
3. $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre car, par exemple, $\bar{2}.\bar{3} = \bar{0}$ bien que $\bar{2} \neq \bar{0}$ et $\bar{3} \neq \bar{0}$.

Définition 5 (Corps).

L'anneau A non réduit à $\{0\}$ est dit un **corps**, si tout élément non nul de A est inversible (i.e., $U(A) = A^* = A \setminus \{0\}$).

Exemple 5 .

1. $Q, \mathbb{R}$ et $\mathbb{C}$ sont des corps pour leurs opérations usuelles $+$ et $\times$.
2. $(\mathbb{Z}, +, .)$ n'est pas un corps, car pour tout $x \in \mathbb{Z} \setminus \{0\}$, x n'admet pas d'inverse dans $\mathbb{Z}$.

Remarque 3 .

Comme un inversible n'est jamais diviseur de zéro, un corps est intègre ; la réciproque est fausse : $\mathbb{Z}$ est intègre sans être un corps.

1.2 Morphismes d'anneaux

Définition 6 .

Soient A et B deux anneaux. Une application $f : A \to B$ est dite homomorphisme d'anneaux (ou simplement un **morphisme** d'anneaux) si

1. $f(1_A) = 1_B$.
2. $\forall a, b \in A, f(a+b) = f(a) + f(b)$ et $f(ab) = f(a)f(b)$.

Si de plus f est **bijective**, on dit que f est un **isomorphisme** d'anneaux et que A et B sont deux anneaux isomorphes. Dans ce cas on écrit $A \cong B$.

Exemple 6 .

Si B est un sous anneau de A, l'inclusion $i : B \to A$, $x \to x$ est un morphisme d'anneaux, dite injection canonique de B dans A.

Remarque 4 .

Notons quelques conséquences immédiates de cette définition :
Un morphisme d'anneaux $f : A \to B$ vérifie toujours :

$$f(0_A) = 0_B \quad \text{et} \quad f(-a) = -f(a), \ \forall a \in A.$$

En effet, on a :

$$f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A).$$

En ajoutant $-f(0_A)$, on obtient $f(0_A) = 0_B$.
De plus, on a

$$0_B = f(0_A) = f(a - a) = f(a) + f(-a), \ \forall a \in A.$$

L'unicité de l'opposé dans le groupe $(B, +)$ entraîne $f(-a) = -f(a)$.

Proposition 2 .

Soit $f : A \to B$ un morphisme d'anneaux. Si $a \in U(A)$ alors $f(a) \in U(B)$.

Preuve

On a : $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_B$.
Donc $f(a) \in U(B)$ et $(f(a))^{-1} = f(a^{-1})$.

Définition 7 .

Le noyau du morphisme f est $ker(f) := \{a \in A : f(a) = 0_B\}$.
L'image du morphisme f est l'ensemble $Im(f) := f(A) = \{f(a) : a \in A\}$.

Proposition 3 .

Soit $f : A \to B$ un morphisme d'anneaux. Alors, $Im(f)$ est un sous-anneau de B.

Preuve

On a par définition $Im(f) = \{f(a) : a \in A\}$.

- On a $f(1_A) = 1_B$. Donc $1_B \in Im(f)$.
- Soient $x, y \in Im(f)$, $\exists a, b \in A$ tels que $x = f(a)$ et $y = f(b)$. Ainsi :
  $x - y = f(a) - f(b) = f(a - b) \in Im(f)$,
  et $\quad xy = f(a).f(b) = f(ab) \in Im(f)$.
  D'où : $Im(f)$ est un sous-anneau de B.

Proposition 4 .

Un morphisme d'anneaux f de A vers B est injectif si et seulement si $ker(f)$ est réduit à $\{0_A\}$. Il est surjectif si et seulement si $Im(f) = B$.

2. Idéaux d'un anneau

Il se trouve que la notion de sous-anneau n'est pas la plus riche ni la plus intéressante : en particulier, elle ne permet pas de définir des anneaux quotients car la relation d'équivalence $a\mathcal{R}b \Leftrightarrow a - b \in B$ n'est en général pas compatible avec le produit lorsque B est seulement un sous-anneau de A. Pour définir des anneaux quotients, il faut utiliser des idéaux.

2.1 Définition et premières propriétés

Définition 8 .

Soit $(A, +, .)$ un anneau et I un sous-ensemble **non vide** de A.
On dit que I est un **idéal** de A si $(I, +)$ est un sous-groupe de $(A, +)$ et si, pour tout $a \in A$ et tout $x \in I$, $ax \in I$.
Ce qui est équivalent à : $\forall x, y \in I, \forall a \in A$, on a $x - y \in I$ et $ax \in I$.

Remarque 5 .

- Un idéal I de A contient toujours 0. En effet, I est non vide, soit $x \in I$, on a, $0 = 0x \in I$.
- Pour tout $x \in I$, $-x = (-1)x \in I$.

Exemple 7 .

1. $\{0\}$ et A sont des idéaux de A dits idéaux triviaux.
2. Pour tout $x \in A$, l'ensemble des multiples de x :
$$(x) := Ax = \{ax \mid a \in A\}$$
est un idéal de A. Cet idéal est dit l'idéal **principal** de A engendré par x.
3. Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, $(n \in \mathbb{N})$.

Proposition 5 (très utile dans la pratique).

Soit A un anneau et I un idéal de A.

1. Si I contient 1, alors $I = A$.
2. Si I contient un élément de $U(A)$, alors $I = A$.

Preuve

1. Supposons que $1 \in I$. Tout $x \in A$ s'écrit $x = x.1$. Comme $1 \in I$, il en résulte de la définition d'un idéal $x \in I$. On a alors $A \subset I$. Donc $A = I$.
2. Supposons maintenant que I contient un élément x inversible dans A. On a $1 = xx^{-1}$ avec $x \in I$ et $x^{-1} \in A$, donc $1 \in I$, et on applique l'assertion (1) de la proposition pour conclure.

Proposition 6 .

Si I et J sont deux idéaux de A, l'intersection $I \cap J$ est encore un idéal de A. Plus généralement, l'intersection d'une famille non vide d'idéaux est encore un idéal.

Preuve

Remarquons d'abord que $I \cap J$ est non vide. En effet, $0 \in I \cap J$.
Pour tous $x, y \in I \cap J$ et tout $a \in A$, on a $x, y \in I$ et $x, y \in J$. Et puisque I et J sont des idéaux de A, alors, $x - y \in I$, $x - y \in J$, $ax \in I$ et $ax \in J$. Donc, $x - y \in I \cap J$ et $ax \in I \cap J$. Par suite, $I \cap J$ est un idéal de A.

Proposition 7 .

Soient I et J deux idéaux d'un anneau A. La somme de I et J définie par $I + J := \{x + y : x \in I, y \in J\}$ est un idéal de A.

Preuve

Notons que $I + J$ est non vide. En effet, il contient au moins 0.
Soient $x, y \in I + J$ et $a \in A$. Donc, $x = x_1 + x_2$ et $y = y_1 + y_2$ avec $x_1, y_1 \in I$ et $x_2, y_2 \in J$. Ainsi,

$$x - y = \underbrace{(x_1 - y_1)}_{\in I} + \underbrace{(x_2 - y_2)}_{\in J} \in I + J \quad \text{et} \quad ax = \underbrace{ax_1}_{\in I} + \underbrace{ax_2}_{\in J} \in I + J.$$

$I + J$ est donc un idéal de A.

Théorème 1 .

Un anneau intègre A est un corps si, et seulement si, les seuls idéaux de A sont $\{0\}$ et A.

Preuve

Supposons que A est un corps et soit I un idéal non nul de A. Soit $x \neq 0$ un élément de I, alors il existe $y \in A$ tel que $xy = 1_A$. D'où $1_A \in I$ et par suite $I = A$.
Réciproquement, supposons que $\{0\}$ et A sont les seuls idéaux de A. Soit $x \neq 0$ un élément de A, alors (x) est un idéal de A distinct de $\{0\}$. Par suite $(x) = A$. Et puisque $1 \in A$, alors il existe $y \in A$ tel que $xy = 1$. Donc tout élément non nul de A est inversible, i.e., A est un corps.

Proposition 8 .

Soient $f : A \to B$ un morphisme d'anneaux et J un idéal de B. Alors l'image réciproque

$$I = f^{-1}(J) = \{a \in A : f(a) \in J\}$$

est un idéal de A. En particulier, $ker(f)$ est un idéal de A.

Preuve

- On a $f(0_A) = 0_B \in J$. Donc $0_A \in I$. Soient $x, y \in I$ et $a \in A$. Alors, $f(x), f(y) \in J$, et donc $f(x-y) = f(x) - f(y) \in J$ et $f(ax) = f(a)f(x) \in J$. D'où, $x - y \in I$ et $ax \in I$. Par suite, I est un idéal de A.
- Pour $ker(f)$, il suffit d'écrire $ker(f) = \{a \in A : f(a) = 0_B\} = f^{-1}\{0_B\}$.

Remarque 6 .

L'image directe d'un idéal par un morphisme d'anneaux $f : A \to B$ n'est pas forcément un idéal de B. Par exemple, pour le morphisme d'anneaux $f : \mathbb{Z} \to \mathbb{Q}$, $x \to x$ défini par l'injection canonique, l'image de $(2) = 2\mathbb{Z}$ (qui est un idéal de $\mathbb{Z}$) n'est pas un idéal de $\mathbb{Q}$. En effet, $\frac{1}{5}.2 = \frac{2}{5} \notin f(2\mathbb{Z}) = 2\mathbb{Z}$.

2.2 Idéaux et anneaux quotients

Rappels :

On commence par rappeler les deux définitions élémentaires suivantes :

Définition 9 .

Soit X un ensemble. Une **relation d'équivalence** $\mathcal{R}$ sur X est une relation sur X telle que :

- $\mathcal{R}$ est réfléxive : $x\mathcal{R}x$ pour tout $x \in X$;
- $\mathcal{R}$ est symétrique : $x\mathcal{R}y$ implique $y\mathcal{R}x$ pour tous $x, y \in X$;
- $\mathcal{R}$ est transitive : $x\mathcal{R}y$ et $y\mathcal{R}z$ implique $x\mathcal{R}z$ pour tous $x, y, z \in X$.

Définition 10 .

Etant donnée une relation d'équivalence $\mathcal{R}$ sur un ensemble X.

- L'ensemble $\overline{x} = \{y \in X; x\mathcal{R}y\}$ est la **classe d'équivalence** de x ou tout simplement la classe de x.
- L'ensemble $X/\mathcal{R} = \{\overline{x}; x \in X\}$ des classes d'équivalence est appelé **ensemble quotient** de X par $\mathcal{R}$.
- L'application $\pi : X \to X/\mathcal{R}$ définie par $\pi(x) = \overline{x}$ est appelée **l'application canonique** associée. L'application canonique est surjective car une classe d'équivalence n'est jamais vide.

On se place maintenant dans un anneau A et soit I un idéal de A. Alors la relation $\sim$ définie sur A par :

$$\forall x, y \in A,\ x \sim y \Leftrightarrow x - y \in I$$

est une relation d'équivalence. L'ensemble des classes d'équivalences $A/\sim$ est noté A/I et on a :

$$A/I = \{\overline{x}; x \in A\} \text{ où } \overline{x} = \{y \in A : x - y \in I\} = x + I.$$

L'ensemble A/I des classes d'équivalences modulo I peut être muni d'une structure d'anneau pour les deux lois suivantes :

$$\overline{x} + \overline{y} = \overline{x+y} \quad \text{et} \quad \overline{x}.\overline{y} = \overline{xy}$$

En effet, puisque $(A, +)$ est un groupe abélien et I est un sous-groupe de A, l'ensemble $(A/I, +)$ est un groupe abélien.
Dans ce groupe, la multiplication étant définie de la façon suivante : $\forall \bar{x} = x + I, \bar{y} = y + I \in A/I$: $\overline{x}.\overline{y} = \overline{xy} = xy + I$. Cette opération est bien définie ; en effet, soient $x', y' \in A$ tels que $\overline{x'} = \overline{x}$ et $\overline{y'} = \overline{y}$, on a : $x'y' - xy = x'y' - xy' + xy' - xy = (x' - x)y' + x(y' - y) \in I$, car $(x' - x), (y' - y) \in I$ et I est un idéal de A, d'où $\overline{x'y'} = \overline{xy}$, et ainsi la multiplication des classes d'équivalence et indépendante des représentants choisis.

En utilisant les propriétés de l'anneau A, on vérifie facilement que $(A/I, +, .)$ est un anneau, la classe $\overline{0}$ est l'élément zéro de A/I et la classe $\overline{1}$ est l'unité de A/I.

Définition 11 (Anneau quotient-surjection canonique).

Soit A un anneau et I un idéal de A. L'anneau $(A/I, +, .)$ est appelé **l'anneau quotient** de l'anneau A par l'déal I.
L'application $s : A \to A/I$ définie par $s(x) = \overline{x}$ est un morphisme d'anneaux surjectif appelé **surjection canonique**.

Exemple 8 .

Sur l'anneau $\mathbb{Z}$, on définit la relation d'équivalence suivante :

$$\forall x, y \in \mathbb{Z}, x \equiv y[n] \Leftrightarrow x - y \in n\mathbb{Z}.$$

Cette relation s'appelle la relation de **congruence** modulo n. L'anneau quotient associé n'est autre que l'anneau quotient de $\mathbb{Z}$ par son idéal $n\mathbb{Z}$, i.e.,

$$(\mathbb{Z}/\equiv) = \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}.$$

Théorème 2 (1^{er} théorème d'isomorphisme).

Soit $f : A \to B$ un morphisme d'anneaux. Alors,

$$A/ker(f) \cong Im(f).$$

Preuve

On considère l'application $\overline{f} : A/ker(f) \to Im(f)$ définie par $\overline{f}(\overline{x}) = f(x)$. Cette application est bien définie. En effet, si $\overline{x} = \overline{y}$ alors $x - y \in ker(f)$ et donc $f(x) - f(y) = f(x - y) = 0$. Ainsi $f(x) = f(y)$, i.e., $\overline{f}(\overline{x}) = \overline{f}(\overline{y})$.
Maintentant, il est facile de vérifier que f est un morphisme d'anneaux. En plus,

$$\overline{f}(\overline{x}) = 0 \Leftrightarrow f(x) = 0 \Leftrightarrow x \in ker(f) \Leftrightarrow \overline{x} = \overline{0}.$$

Par suite, $\overline{f}$ est injective.
Aussi, pour tout $f(x) \in Im(f)$, on a $f(x) = \overline{f}(\overline{x})$, et donc $\overline{f}$ est surjective. Enfin, $\overline{f}$ est bijective.

Exercice 2 *On considère l'anneau $\mathbb{R}[X]$ des polynômes à coefficients dans $\mathbb{R}$.*

1. *Montrer que l'application $\varphi : \mathbb{R}[X] \to \mathbb{R} \times \mathbb{R}$ définie par $\varphi(P) = (P(0), P(1))$ est un morphisme d'anneaux surjectif.*
2. *Montrer que $ker(\varphi) = (X^2 - X)$ (l'idéal principal engendré par $X^2 - X$).*
3. *En déduire que $\mathbb{R}[X]/(X^2 - X) \cong \mathbb{R} \times \mathbb{R}$.*
4. *L'anneau $\mathbb{R}[X]/(X^2 - X)$ est-il intègre ? Expliquer.*

Proposition 9 .

Soient A un anneau et I un idéal de A. Les idéaux de A/I sont exactement les ensembles $J/I = \{\overline{x}; x \in J\}$ avec J un idéal de A contenant I.

Preuve

Soit K un idéal de A/I. Posons $J = \{x \in A; \overline{x} \in K\}$.
Montrons d'abord que $I \subseteq J$.
Soit $x \in I$, donc $\overline{x} = \overline{0} \in K$. Par suite $x \in J$. Ainsi, $I \subseteq J$.
En plus, pour tous $x, y \in J$ et $a \in A$, on a :
$\overline{x + y} = \overline{x} + \overline{y} \in K$ et $\overline{ax} = \overline{a}.\overline{x} \in K$. Donc, $x + y \in J$ et $ax \in J$.
Ainsi, J est un idéal de A contenant I et $J/I = K$.
Inversement, si J est un idéal de A contenant I, alors il est facile de voir que J/I est un idéal de A/I.

Exercice 3 *Donner la liste des idéaux de $\mathbb{Z}/12\mathbb{Z}$.*

Théorème 3 ($2^{\text{ème}}$ théorème d'isomorphisme).

Soient $I \subseteq J$ deux idéaux d'un anneau A. Alors,

$$\frac{A/I}{J/I} \cong A/J.$$

Preuve

On considère l'application $f : A/I \to A/J$ définie par $f(\overline{x}) = \hat{x}$. Cette application est bien définie. En effet, $\overline{x} = \overline{y}$ implique que $x - y \in I \subseteq J$ et donc $\hat{x} = \hat{y}$. Par suite, $f(\overline{x}) = f(\overline{y})$. Il est trivial de vérifier que f est un morphisme d'anneaux. Ensuite,

$$ker(f) = \{\overline{x} \in A/I \mid \hat{x} = \hat{0}\} = \{\overline{x} \in A/I \mid x \in J\} = J/I.$$

et

$$Im(f) = A/J.$$

D'après le premier théorème d'isomorphisme, on a le résultat.

2.3 Idéaux premiers et idéaux maximaux

Définition 12 (Idéal premier).

Un idéal P d'un anneau A est dit **premier** si $P \neq A$ et pour tous $x, y \in A$, on a $xy \in P$ entraîne $x \in P$ ou $y \in P$.

Exemple 9 .

1. $\{0\}$ est un idéal premier de $\mathbb{Z}$.
2. Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et $p\mathbb{Z}$ où p est un entier premier.

Proposition 10 .

Un anneau A est intègre si et seulement si $\{0\}$ est un idéal premier de A.

Preuve

Découle des définitions des idéaux premiers et des anneaux intègres.

Proposition 11 .

Un idéal P d'un anneau A est premier si et seulement si A/P est intègre.

Preuve

Supposons que P est premier. Soient $x, y \in A$ tels que $\overline{x}.\overline{y} = \overline{xy} = \overline{0}$. Donc, $xy \in P$. Ainsi, $x \in P$ ou $y \in P$. Par suite, $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Par conséquent, A/P est intègre.
Réciproquement, supposons que A/P est intègre. Soient $x, y \in A$ tels que $xy \in P$. Donc, $\overline{xy} = \overline{x}.\overline{y} = \overline{0}$. Comme A/P est intègre, $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Par suite, $x \in P$ ou $y \in P$. Ainsi P est premier.

Définition 13 (Idéal maximal).

Un idéal I d'un anneau A est dit **maximal** s'il est propre ($I \neq A$) et si les seuls idéaux de A contenant I sont I et A.
Cela est équivalent à : pour tout idéal J de A tel que $I \subset J$, on a $J = I$ ou $J = A$.

Exemple 10 .

Dans l'anneau $\mathbb{Z}$, si p est un nombre premier, alors (p) est un idéal maximal.

Théorème 4 (Admis).

1. Tout anneau non nul possède au moins un idéal maximal.
2. Dans un anneau non nul, tout idéal propre est contenu dans un idéal maximal (Théorème de Krull).

Proposition 12 .

Un idéal M d'un anneau A est maximal si et seulement si l'anneau A/M est un corps.

Preuve

Supposons que M est maximal. Soit $x \in A$ tel que $\overline{x} \neq \overline{0}$. Donc, $x \notin M$. Par suite, $M \subsetneq M + (x)$. Ainsi, $M + (x) = A$. Alors, il existe $m \in M$ et $a \in A$ tels que $m + ax = 1$. D'où, $\overline{ax} = \overline{1}$. Ainsi, $\overline{x}$ est inversible. Par suite A/M est un corps.
Réciproquement, supposons que A/M est un corps. Soit I un ideal de A tel que $M \subset I$. Donc, I/M est un idéal de A/M qu'est un corps. Alors, $I/M = \{\overline{0}\}$ ou $I/M = A/M$. Par suite, $I = M$ ou $I = A$. Par conséquent, M est maximal.

Proposition 13 .

Tout idéal maximal est premier (la réciproque est en général fausse).

Preuve

Soit M un idéal maximal d'un anneau A. Alors, A/M est un corps, et donc intègre. Par suite, M est premier.
La réciproque n'est pas vraie en général. Dans l'anneau $\mathbb{Z}$, l'idéal (0) est premier puisque $\mathbb{Z}$ est intègre mais non maximal puisque $\mathbb{Z}$ n'est pas un corps.

Proposition 14 (Admise).

Soient A un anneau et I un idéal de A. Les idéaux premiers (resp. maximaux) de A/I sont les idéaux de la forme P/I où P un idéal premier (resp. maximal) de A contenant I.

Exercice 4 *Donner tous les idéaux premiers de l'anneau* $\mathbb{Z}/12\mathbb{Z}$.

3. Anneaux de polynômes à une indéterminée

Définition 14 .

Soit A un anneau et X une indéterminée. On appelle P un polynôme à une indéterminée X et à coefficients dans A toute somme finie de la forme

$$P := P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n = \sum_{k=0}^{n} a_kX^k$$

avec $a_0, ..., a_n \in A$. Les scalaires $a_0, ..., a_n$ sont appelés les coefficients de P.
On note $A[X]$ l'ensemble des polynômes à une indéterminée et à coeffcients dans A.

Remarque 7 .

1. Le polynôme nul $P = 0$ est le polynôme dont tous les coefficients sont nuls.
2. Deux polynômes P et Q sont dits égaux si et seulement si les coefficients de même ordre dans P et dans Q sont égaux.
3. L'ensemble $A[X]$ muni de l'addition et de la multiplication usuelles est un anneau commutatif unitaire.

3. Anneaux de polynômes à une indéterminée

Définition 15 (Degré d'un polynôme).

Soit A un anneau et $P = \sum_{k=0}^{n} a_k X^k \in A[X]$. On définit le degré de P, noté $deg(P)$, par :

- Si $P = 0$, on pose $deg(P) = -\infty$.
- Si $P \neq 0$, alors $deg(P) = \max\{k \in \mathbb{N} : a_k \neq 0\}$.

Exemple 11 .

1. $P(X) = 2X^4 + 2X^3 - X + 1 \in \mathbb{Z}[X]$ est un polynôme de degré 4.
2. $Q(X) = \bar{4}X^3 + \bar{2}X^2 + X + \bar{3} \in \mathbb{Z}/5\mathbb{Z}[X]$ et $deg(Q) = 3$ car $\bar{4} \neq \bar{0}$ dans $\mathbb{Z}/5\mathbb{Z}$.

Proposition 15 .

Soient $P, Q \in A[X]$ non nuls. Alors

1. $deg(P+Q) \leq \max\{deg(P), deg(Q)\}$. L'inégalité est stricte si et seulement si $deg(P) = deg(Q)$ et si les coefficients dominants de P et Q sont opposés.
2. $deg(PQ) \leq deg(P) + deg(Q)$. En particulier, si A est intègre alors $deg(PQ) = deg(P) + deg(Q)$.

Preuve

On pose $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k$ avec $deg(P) = n$ et $deg(Q) = m$ (donc $a_n \neq 0$ et $b_m \neq 0$).

1) - Si $n = m$, il est clair que $P+Q = \sum_{k=0}^{n}(a_k+b_k)X^k$. Donc, $deg(P+Q) \leq n$ avec égalité si $a_n+b_n \neq 0$.

- Si $n > m$, on a :

$$P + Q = a_n X^n + ... + a_{m+1} X^{m+1} + \sum_{k=0}^{m}(a_k + b_k)X^k.$$

Ainsi, $deg(P + Q) = n = \max\{n, m\}$.
- De même, si $m > n, deg(P + Q) = m = \max\{n, m\}$.

2) Il suffit de remarquer que

$$PQ = \sum_{k=0}^{n+m} c_k X^k, \text{ où } \forall k \;\; c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j.$$

Dans le cas où A est intègre, on a $c_{n+m} = a_n b_m \neq 0$ car $a_n \neq 0$ et $b_m \neq 0$.

Proposition 16 .

Soit A un anneau intègre. Alors $U(A[X]) = U(A)$.
(En particulier, si $A = K$ est un corps, alors $U(K[X]) = K^* = K \setminus \{0\}$).

Preuve

L'inclusion $U(A) \subseteq U(A[X])$ est évidente. Prenons maintenant $P \in U(A[X])$, il existe $Q \in A[X]$ tel que $PQ = 1$. Donc, $0 = deg(PQ) = deg(P) + deg(Q)$. Ainsi, $deg(P) = deg(Q) = 0$. Par suite $P, Q \in A$ et donc $P \in U(A)$. D'où $U(A[X]) \subseteq U(A)$.

Exemple 12 .

1. $U(\mathbb{Z}[X]) = U(\mathbb{Z}) = \{-1; 1\}$.
2. $U(\mathbb{Z}/2\mathbb{Z}[X]) = (\mathbb{Z}/2\mathbb{Z})^* = \{\bar{1}\}$ (car $\mathbb{Z}/2\mathbb{Z}$ est un corps).

Proposition 17 .

Si A est intègre alors $A[X]$ est intègre. (En particulier, si $A = K$ est un corps, alors $K[X]$ est intègre).

Preuve

Soient $P, Q \in A[X]$ tels que $PQ = 0$. On veut montrer que $P = 0$ ou $Q = 0$.
Supposons par l'absurde que $P \neq 0$ et $Q \neq 0$. On a $PQ = 0$, donc $deg(PQ) = -\infty$. Mais, puisque A est intègre, alors $deg(PQ) = deg(P) + deg(Q) \geq 0$. Ce qui est absurde.
Il en résulte que $P = 0$ ou $Q = 0$. Ainsi, $A[X]$ est intègre.

4. Exercices

Exercice 1

Soit A un anneau unitaire tel que pour tout $x \in A$, on a $x^2 = x$.

1. Montrer que $\forall x \in A$, on a $x + x = 0$ et que A est commutatif.
2. Soit $(x, y) \in A^2$. Calculer $xy(x + y)$.
   En déduire que si A contient plus de deux éléments alors A n'est pas intègre.

Exercice 2

Soit $A = \mathbb{Z}/9\mathbb{Z}$.

1. Déterminer les éléments inversibles de A.
2. Déterminer les éléments nilpotents de A.
3. Déterminer les diviseurs de zéro dans A.

Exercice 3

Soient A un anneau commutatif et I et J deux idéaux de A. On considère l'ensemble

$$I : J = \{x \in A : xJ \subset I\}.$$

1. Montrer que $I : J$ est un idéal.
2. Calculer dans $\mathbb{Z}$, les idéaux suivants : $12\mathbb{Z} : 2\mathbb{Z}$, $12\mathbb{Z} : 4\mathbb{Z}$, $12\mathbb{Z} : 8\mathbb{Z}$ et $12\mathbb{Z} : 5\mathbb{Z}$.

Exercice 4

Soit $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, .)$ est un anneau.
2. i) Montrer que $U(\mathbb{Z}[\sqrt{2}]) = \{a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] : a^2 - 2b^2 = \pm 1\}$.
   ii) Est ce que $\mathbb{Z}[\sqrt{2}]$ est un corps ?

Exercice 5

On considère l'ensemble des matrices suivant : $\mathcal{A} = \{\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C}\}$.

Montrer que $(\mathcal{A}, +, .)$ est corps non commutatif.

Exercice 6

Soit A un anneau commutatif unitaire.

1. On suppose que A est intègre et qu'il n'admet qu'un nombre fini d'idéaux. Démontrer que A est un corps.
2. En déduire que tout anneau commutatif unitaire intègre fini est un corps.

Exercice 7

On considère l'anneau $\mathbb{R}[X]$ des polynômes à coefficients dans $\mathbb{R}$.

1. Montrer que l'application $\varphi : \mathbb{R}[X] \to \mathbb{C}$ définie par $\varphi(P) = P(i)$ est un morphisme d'anneaux surjectif.
2. Montrer que $ker(\varphi) = (X^2 + 1)$ (l'idéal principal engendré par $X^2 + 1$).
3. En déduire que $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.
4. Que peut-on dire de l'idéal $(X^2 + 1)$.

Exercice 8 (Examen normal 2020-2021)

On considère l'anneau $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.
Soit $I = (\sqrt{2})$ l'idéal principal de $\mathbb{Z}[\sqrt{2}]$ engendré par $\sqrt{2}$.

1. Vérifier que $I = \{a + b\sqrt{2} \mid a \in 2\mathbb{Z}\ et\ b \in \mathbb{Z}\}$.
2. Montrer que l'application $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}/2\mathbb{Z}$ définie par $f(a+b\sqrt{2}) = \bar{a}$ est un morphisme d'anneaux surjectif.
3. Montrer que $ker(f) = I$.
4. En déduire que I est un idéal maximal de $\mathbb{Z}[\sqrt{2}]$.

Exercice 9 (Facultatif)

On considère l'anneau $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ et l'ensemble $I = \{a + ib : a, b \in \mathbb{Z}\ et\ a \equiv b[2]\}$.

1. Montrer que l'application $\varphi : \mathbb{Z}[i] \to \mathbb{Z}/2\mathbb{Z}$ définie par $\varphi(a+ib) = \overline{a - b}$ est un morphisme d'anneaux surjectif.
2. Montrer que $ker(\varphi) = I$.
3. En déduire que I est un idéal maximal de $\mathbb{Z}[i]$.

Exercice 10 (Extrait du rattrapage 2022-2023)

1. Déterminer $\mathcal{U}(\mathbb{Z}[X])$ et $\mathcal{U}((\mathbb{Z}/2\mathbb{Z})[X])$. ($\mathcal{U}$ désigne l'ensemble des éléments inversibles).
2. On considère le morphisme d'anneaux surjectif

$$\begin{array}{rccc} \varphi : & \mathbb{Z}[X] & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})[X] \\ & P = \sum_{i=0}^{n} a_i X^i & \longmapsto & \varphi(P) = \sum_{i=0}^{n} \overline{a_i} X^i, \end{array}$$

où $\bar{a_i}$ désigne la classe de a_i modulo 2.

(a) Montrer que $\ker(\varphi) = (2) = 2\mathbb{Z}[X]$ (l'idéal principal de $\mathbb{Z}[X]$ engendré par 2).

(b) Que peut-on dire de (2) dans $\mathbb{Z}[X]$?

Exercice 11 (Extrait de l'examen normal 2022-2023)

Soit l'ensemble $\mathcal{B} = \{\frac{a}{b} \in \mathbb{Q} : a \in \mathbb{Z}, b \in \mathbb{N}^* \text{ et } b \text{ est impair}\}$.

1. Vérifier que $\mathcal{B}$ est un anneau intègre.
2. Vérifier que $\mathcal{U}(\mathcal{B}) = \{\frac{a}{b} \in \mathcal{B} : a \in \mathbb{Z}, b \in \mathbb{N}^*,\ a \text{ et } b \text{ impairs}\}$. $\mathcal{B}$ est-il un corps ?
3. On considère l'application $\varphi : \mathcal{B} \to \mathbb{Z}/2\mathbb{Z}$ définie par $\varphi(\frac{a}{b}) = \overline{a}$.

a) Vérifier que φ est bien définie et qu'elle est un morphisme d'anneaux surjectif.

b) Montrer que $\mathcal{B}/(2) \cong \mathbb{Z}/2\mathbb{Z}$.

c) Que peut-on dire de l'idéal (2) dans $\mathcal{B}$?

Exercice 12 (Facultatif)

On considère l'anneau $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ et l'ensemble $I = \{a + ib : a, b \in \mathbb{Z} \; et \; a \equiv b[2]\}$.

1. Montrer que l'application $\varphi : \mathbb{Z}[i] \to \mathbb{Z}/2\mathbb{Z}$ définie par $\varphi(a+ib) = \overline{a-b}$ est un morphisme d'anneaux surjectif.
2. Montrer que $ker(\varphi) = I$.
3. En déduire que I est un idéal maximal de $\mathbb{Z}[i]$.

Exercice 13 (Facultatif)

On se place dans l'anneau $\mathbb{R}[X]$ des polynômes à une indéterminée à coefficients réels.
Soient $P = X^3 + X^2 + X + 1$ et $Q = X^3 - X^2 + X - 1$.

1. Montrer que $(P) + (Q) = (X^2 + 1)$ (indication : vérifier que $pgcd(P, Q) = X^2 + 1$).
2. On note $j = e^{\frac{2i\pi}{3}} = \dfrac{-1}{2} + \dfrac{\sqrt{3}}{2}i$. On rappelle que $j^2 + j + 1 = 0$.
   a) Montrer que l'application :

$$\begin{array}{rccc} \varphi : & \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ & P & \longmapsto & \varphi(P) = P(j). \end{array}$$

   est un morphisme d'anneaux.
   b) Montrer que φ est surjectif (remarquer que $i = \dfrac{1}{\sqrt{3}} + \dfrac{2}{\sqrt{3}}j$).
3. Montrer que $\ker(\varphi) = (X^2+X+1)$ (considérer la division euclidienne de $P \in \ker(\varphi)$ par X^2+X+1).
4. En déduire que $\mathbb{R}[X]/(X^2 + X + 1) \cong \mathbb{C}$.
5. Que peut-on dire de l'idéal $(X^2 + X + 1)$ de $\mathbb{R}[X]$?

Exercice 14 (Facultatif)

Dans cet exercice, on se propose de caractériser les sous-anneaux de $\mathbb{Z}^2$.
On considère l'anneau produit $A = \mathbb{Z} \times \mathbb{Z}$. On rappelle que l'élément neutre de la loi multiplicative de A est $(1, 1)$.

1. Déterminer les éléments inversibles de A. Cet anneau est t-il intègre ?
   Dans la suite, on se propose de déterminer les sous-anneaux de A. Pour tout $m \in \mathbb{N}$, on pose

$$A_m = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x - y \in m\mathbb{Z}\}.$$

2. Montrer que A_m est un sous-anneau de A.
3. Expliciter A_0 et A_1.
4. Montrer que $A_m \subset A_n \Leftrightarrow n \mid m$.
5. Réciproquement, soit B un sous-anneau de A. On pose $H = \{a \in Z : (a, 0) \in B\}$.
6. a) Montrer que H est un sous-groupe de $\mathbb{Z}$.
   b) En déduire qu'il existe $m \in \mathbb{N}$ tel que $B = A_m$ (Indication : utiliser la caractérisation des sous-groupes de $\mathbb{Z}$).

CHAPITRE 2.

ANNEAUX : PRINCIPAUX, NOETHÉRIENS, EUCLIDIENS ET FACTORIELS

1. Propriétés arithmétiques

On entend par propriétés arithmétiques des anneaux celles relatives à la divisibilité.
Dans tout ce qui suit, les anneaux considérés sont des anneaux commutatifs.

1.1 Divisibilité dans les anneaux intègres

Soient A un anneau intègre (unitaire et non trivial) et a, b deux éléments de A. On dit que a divise b (ou b est un multiple de a) et on note $a \mid b$, s'il existe $c \in A$ tel que $b = ac$. Cette relation de divisibilité est une relation de préordre (i.e., réflexive et transitive) mais, non symétrique.
Les diviseurs de 1 sont les unités de l'anneau (i.e., $U(A)$).

Proposition 1 .

Soient a et b deux éléments d'un anneau A. On a : $a \mid b \Leftrightarrow (b) \subset (a)$.

Preuve

- Si $a \mid b$, il existe $c \in A$ tel que $b = ac$. Ce qui entraîne $b \in (a)$. Par suite $(b) \subset (a)$.
- Réciproquement, Si $(b) \subset (a)$, alors $b \in (a)$, ce qui implique $\exists c \in A, b = ac$.

Définition 1 .

Soient A un anneau intègre et a, b deux éléments de A. On dit que a est **associé** à b, et on note $a \sim b$, si $a \mid b$ et $b \mid a$. Ce qui est équivalent à $(a) = (b)$, ou $\exists u \in U(A)$ tel que $a = ub$.
Notons que la relation " x est associé à y" est une relation d'équivalence sur A.

Exemple 1 .

1. Dans $\mathbb{Z}$, $m \sim n$ si, et seulement si, $m = \pm n$.
2. Dans $\mathbb{K}[X]$, où $\mathbb{K}$ est un corps commutatif, P et Q sont associés, si et seulement si, $\exists \lambda \in \mathbb{K}$, $\lambda \neq 0$ tel que $Q = \lambda P$.
3. Soit A un anneau intègre, alors $u \in U(A)$ si, et seulement si, $u \sim 1_A$.

1.2 Éléments irréductibles et éléments premiers

Définition 2 .

Soient A un anneau intègre et a un élément non nul de A.
a) L'élément a est dit **irréductible** s'il n'est pas inversible et si l'égalité $a = bc, (b, c) \in A \times A$, implique que $b \in U(A)$ ou $c \in U(A)$.
b) L'élément a est dit **premier** si l'idéal (a) est premier.

Remarque 1 .

1. D'après la définition d'un idéal premier, un élément $a \in A$ est premier s'il est non nul et non inversible et vérifie
$$a \mid bc \Longrightarrow a \mid b \text{ ou } a \mid c.$$
2. Un élément associé à un élément premier (resp. irréductible) est aussi premier (resp. irréductible). Par conséquent, on considérera les éléments premiers (resp. irréductibles) d'un anneau, "aux inversibles près".

Exemple 2 .

Les éléments premiers de $\mathbb{Z}$ sont les nombres premiers.

Proposition 2 .

Soient A un anneau intègre et q un élément de A. Alors, q est irréductible si et seulement si (q) est un idéal maximal dans l'ensemble des idéaux principaux de A différents de A.

Preuve

Supposons que q est irréductible. Soit $x \in A$ tel que $(q) \subset (x) \subsetneq A$. Montrons que $(q) = (x)$ (c'est à dire que x et q sont associés). Le fait que $(x) \subsetneq A$ veut dire que $x \notin U(A)$. Aussi, $q \in (x)$ et donc il existe $y \in A$ tel que $q = xy$. Comme q est irréductible, on déduit que $y \in U(A)$, et donc x et q sont associés. Inversement, supposons que (q) est un idéal maximal dans l'ensemble des idéaux principaux de A différents de A. Posons $q = xy$ avec $x, y \in A$ et $x \notin U(A)$. On a $(q) \subset (x) \subsetneq A$, et donc $(q) = (x)$. Par suite, q et x sont associés. Alors, il existe $u \in U(A)$ tel que $q = ux$. Comme A est intègre et $x \neq 0$, on déduit que $y = u$. D'où q est irréductible.

Proposition 3 .

Soit A un anneau intègre. Tout élément premier de A est irréductible.

Preuve

Soit p un élément premier de A. Alors, p est non nul et non inversible. Soient $a, b \in A$ tels que $p = ab$. D'où $p \mid ab$ et ainsi $p \mid a$ ou $p \mid b$. Si $p \mid a$, alors $\exists c \in A$ tel que $a = pc$, par suite $p = pcb$. On obtient ainsi $cb = 1$ (car A est intègre), et donc $b \in U(A)$. De même si $p \mid b$, on obtient $a \in U(A)$. Par suite, p est irréductible.

Remarque 2 .

L'exemple suivant montre qu'en général, un élément irréductible n'est pas nécessairement premier.
Soit $A = \mathbb{Z}[i\sqrt{3}] := \{a + ib\sqrt{3} : a, b \in \mathbb{Z}\}$. Commençons par déterminer $U(A)$. Soit $x = a + ib\sqrt{3} \in U(A)$, donc $\exists y = c + id\sqrt{3} \in A$ tel que $xy = 1$. En passant aux modules des complexes, on obtient $(a^2 + 3b^2)(c^2 + 3d^2) = 1$, on aura necéssairement $a^2 + 3b^2 = 1$. Si $b \neq 0$, on aura $a^2 + 3b^2 > 1$. Donc $b = 0$, et par suite $a^2 = 1$. Ainsi $x = \pm 1$. D'où $U(A) \subset \{1; -1\}$.
D'autre part, on a $\{1; -1\} \subset U(A)$. Ainsi $U(A) = \{1; -1\}$.
2 est un élément irréductible de A, en effet, on a $2 \notin U(A)$. Soient $x = a + ib\sqrt{3}, y = c + id\sqrt{3} \in A$ tels que $2 = xy$. En passant aux modules des complexes, on obtient $4 = (a^2 + 3b^2)(c^2 + 3d^2)$. Comme $a^2 + 3b^2$ est toujours différent de 2, alors $a^2 + 3b^2 = 1$ ou $c^2 + 3d^2 = 1$. D'où $x = \pm 1 \in U(A)$ ou $y = \pm 1 \in U(A)$. Il en résulte que 2 est irréductible dans A.
Cependant, 2 n'est pas premier dans A. En effet, 2 divise $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ et 2 ne divise ni $1 + i\sqrt{3}$ ni $1 - i\sqrt{3}$ (car si 2 divise $1 + i\sqrt{3}$, alors 2 divise 1 dans $\mathbb{Z}$, ce qui est faux ; de même 2 ne divise pas $1 - i\sqrt{3}$).

1.3 pgcd et ppcm

Définition 3 .

Soient A un anneau intègre et $a, b \in A$.

1. Un élément d de A est dit plus grand commun diviseur (pgcd) de a et b, si : d divise a et b et tout diviseur commun à a et b divise d.
2. Un élément m de A est dit plus petit commun multiple (ppcm) de a et b, si m est un multiple de a et b et tout multiple de a et b est divisible par m.
3. Deux éléments a et b sont dits premiers entre eux si les seuls diviseurs communs à a et à b sont les unités de A (i.e., éléments inversibles).

Remarque 3 .

1. Si a divise b alors a est un pgcd de a et b.
2. Si a et b (éléments d'un anneau intègre A) admettent un pgcd, alors ce pgcd est unique à facteurs inversibles près. En effet,
   - Si d est un pgcd de a et b et $d' \in A$ tel que $d \sim d'$ alors d' est aussi un pgcd de a et b ($d' \mid a$ et $d' \mid b$ car $d' \mid d$ et $d \mid a$ et $d \mid b$; si $\delta \mid a$ et $\delta \mid b$, alors $\delta \mid d'$ car $\delta \mid d$ et $d \mid d'$).
   - D'autre part, si d et d' sont des pgcd de a et b, alors d et d' sont associés (car $d \mid d'$ et $d' \mid d$).
3. En général, deux éléments d'un anneau intègre n'ont pas nécessairement un pgcd.
   Dans l'anneau $A = \mathbb{Z}[i\sqrt{5}]$ les éléments $z_1 = 2(1 + i\sqrt{5})$ et $z_2 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ n'ont pas de pgcd. En effet, supposons que d soit un pgcd de ces deux éléments. Comme d divise z_1 et z_2, alors $|d|^2$ divise $|z_1|^2 = 24$ et $|z_2|^2 = 36$. D'autre part, comme 2 et $(1 + i\sqrt{5})$ sont des diviseurs communs, $|d|^2$ est divisible par 4 et 6. On en déduit facilement que $|d|^2 = 12$. Ceci est impossible car l'équation $a^2 + 5b^2 = 12$ n'a pas de solution dans $\mathbb{Z}$.

Proposition 4 .

Soit A un anneau intègre. Alors, tout élément irréductible de A est premier avec tout élément qu'il ne divise pas.

Preuve

Soit q un élément irréductible de A et soit $a \in A$ tel que q ne divise pas a. Soit aussi d un diviseur en commun de q et a. Donc, $d \in U(A)$ ou d est associé à q. Dans le second cas, $a \in (d) = (q)$, et donc q divise a, ce qui est absurde. Donc, $d \in U(A)$, et q et a sont premiers entre eux.

2. Anneaux principaux

Définition 4 (Anneau principal).

Un anneau intègre A est dit **principal** si tout idéal de A est principal ; i.e., pour tout idéal I de A, il existe $x \in A$ tel que $I = Ax = \{ax \mid a \in A\}$.

Exemple 3 .

1. Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$, l'anneau $\mathbb{Z}$ est donc principal.
2. Tout corps est un anneau principal.

Remarque 4 .

1. Il est crucial de ne pas oublier "intègre" dans la définition d'un anneau principal. Par exemple, l'anneau $\mathbb{Z}_4 := \mathbb{Z}/4\mathbb{Z}$ a tous ses idéaux ($\{\bar{0}\}$, $2\mathbb{Z}_4$ et $\mathbb{Z}_4$) principaux. Cependant l'anneau $\mathbb{Z}_4$ n'est pas principal car il n'est pas intègre.
2. Il existe des anneaux intègres non principaux. Par exemple, $\mathbb{Z}[X]$ est un anneau intègre non principal. En effet, l'idéal $(2, X)$ engendré par 2 et X n'est pas principal (voir TD 2).

Proposition 5 .

Dans un anneau principal, tout idéal premier non nul est maximal.

Preuve

Soit A un anneau principal et $I = Ax$ ($x \neq 0$) un idéal premier de A. On suppose que $I \subseteq J = Ay$. Donc, $x = ay$ avec $a \in A$. Et comme I est premier, alors $a \in I$ ou $y \in I$. Si $y \in I$, alors $J = Ay \subseteq I$. D'où, $J = I$. Si maintenant $a \in I$, alors $a = bx$ avec $b \in A$. Donc, $x = xby$, ce qui implique que $1 = by$ (car A intègre et $x \neq 0$), et donc y est inversible. Par suite $J = A$. En conclusion, I est maximal.

Proposition 6 .

Soit A un anneau principal. Alors, tout élément irréductible de A est premier.

Preuve

Soit q un élément irréductible de A. On sait que (q) est un idéal maximal dans l'ensemble des idéaux principaux de A (différents de A). Mais comme A est principal, tout idéal est principal, et donc (q) est un idéal maximal. Par suite, (q) est un idéal premier, et donc q est premier.

Remarque 5 .

Dans un anneau principal, les notions d'éléments premiers et d'éléments irréductibles coincident.

Proposition 7 .

Dans un anneau principal, toute suite croissante d'idéaux est stationnaire.

Preuve

Soit A un anneau principal. Supposons par l'absurde qu'il existe une suite strictement croissante $(a_1) \subset (a_2) \subset ...$ d'idéaux de A non stationnaire. On pose $J = \cup_{i\geq 1}(a_i)$. Montrons que J est un idéal. Il est clairement non vide. Si $x, y \in J$ alors il existe $i, j \geq 1$ tel que $x \in (a_i)$ et $y \in (a_j)$. Si par exemple $i \leq j$, alors $x \in (a_i) \subset (a_j)$ et donc $x - y \in (a_j) \subset J$. En plus, pour tout $a \in A, ax \in (a_i) \subset J$. Par suite, J est un idéal de A, et donc principal. On pose $J = (a)$. Alors, il existe $i \geq 1$ tel que $a \in (a_i)$, et donc pour tout $j \geq i, J \subset (a_i) \subset (a_j) \subset J$. Par conséquent, $(a_i) = (a_j)$ ce qui est absurde. D'où le résultat.

3. Anneaux noethériens

Définition 5 (Idéal de type fini).

Un idéal I d'un anneau A est dit **de type fini** s'il est engendré par un nombre fini d'éléments, i.e., $\exists x_1, ..., x_n \in A$ tels que

$$I = (x_1, ..., x_n) = \{a_1x_1 + ... + a_nx_n \mid a_1, ..., a_n \in A\}.$$

En particulier, l'idéal principal (x) avec $x \in A$ est un idéal de type fini engendré par x.

Proposition 8 (Admise).

Soit A un anneau. Les assertions suivantes sont équivalentes :

1) Tout idéal de A est de type fini.
2) Toute suite croissante $I_1 \subset I_2 \subset ...$ d'idéaux de A est stationnaire.
   (i.e., $\exists k \in \mathbb{N}$ tel que $\forall i \geq k,\ I_i = I_k$).
3) Toute famille non vide d'idéaux de A a un élément maximal pour l'inclusion (i.e., qui n'est strictement inclus dans aucun autre élément de la famille).

Définition 6 (Anneau noethérien).

Un anneau qui vérifie 1), 2) ou 3) est dit **noethérien**.

Exemple 4 .

Un anneau principal est un anneau noethérien. En particulier, $\mathbb{Z}$ est noethérien.

Proposition 9 .

Si A est noethérien alors $A[X]$ est noethérien.

Exemple 5 .

$\mathbb{Z}[X]$ est noethérien car $\mathbb{Z}$ l'est.

4. Anneaux enclidiens

Définition 7 (Anneau enclidien).

Un anneau A est dit **euclidien** lorsque :

1. A est intègre.
2. A est muni d'une division euclidienne : $\exists v : A \setminus \{0\} \to \mathbb{N}$ telle que
   $\forall a, b \in A, b \neq 0, \exists q, r \in A$ tels que $a = bq + r$, avec $r = 0$ ou $v(r) < v(b)$.

Exemple 6 .

1. $\mathbb{Z}$ est un anneau euclidien, $v : \mathbb{Z}^* \to \mathbb{N};\ v(n) = |n|$.
2. $\mathbb{Z}[i] := \{a + ib; a, b \in \mathbb{Z}\}$ est un anneau euclidien, $v : (\mathbb{Z}[i])^* \to \mathbb{N};\ v(z) = |z|^2$.
3. $A = \mathbb{R}[X]$ est un anneau euclidien, $v(P) = deg(P)$.

Théorème 1 .

Tout anneau euclidien est principal.

Preuve

Soit A un anneau euclidien muni d'une division euclidienne v, et soit $(0) \subsetneq I \subsetneq A$ un idéal de A. On considère l'ensemble $F = \{v(x) : x \in I\}$. L'ensemble $F \subseteq \mathbb{N}$ est non vide, et donc admet un plus petit élément $v(a)$. Soit $x \in I, \exists q, r \in A$ tels que $x = aq + r$ avec $r = 0$ ou $v(r) < v(a)$. En plus, $r = x - aq \in I$, et donc, si $r \neq 0$, on a $v(r) \geq v(a)$, ce qu'est impossible car $v(r) < v(a)$. Ainsi, $r = 0$, et par suite, $x \in Aa$. Par conséquent, $I \subseteq Aa \subseteq I$. D'où, I est principal.

Remarque 6 .

1. La réciproque du théorème précédent est fausse. En effet, l'anneau $\mathbb{Z}[\frac{1+\sqrt{19}i}{2}]$ est principal mais non euclidien.
2. A principal $\not\Rightarrow A[X]$ principal et A euclidien $\not\Rightarrow A[X]$ euclidien. En effet, un simple contre-exemple est donné par $\mathbb{Z}$ qu'est euclidien (donc principal), mais $\mathbb{Z}[X]$ n'est pas principal (donc n'est pas euclidien).

Proposition 10 .

Soit A un anneau. Alors, $A[X]$ euclidien $\Leftrightarrow$ $A[X]$ principal $\Leftrightarrow$ A corps.

Preuve

Il suffit de montrer que si $A[X]$ est principal alors A est un corps. Les autres implications sont claires. Considérons l'application $f : A[X] \to A$ définie par $f(P) = P(0)$. f est un morphisme d'anneaux surjectif et $ker(f) = \{P \in A[X] : P(0) = 0\} = XA[X] = (X)$. D'après le premier théorème d'isomorphisme, on a $A \cong A[X]/(X)$. L'anneau $A[X]$ est supposé principal, donc intègre et par suite A l'est aussi. Donc $A[X]/(X)$ est intègre et par suite (X) est premier dans $A[X]$ (qui est supposé principal) et donc maximal. Il en résulte que A est un corps.

5. Anneaux factoriels

Définition 8 (Anneau factoriel).

Un anneau A est dit **factoriel** lorsque :

1. A est intègre.
2. $\forall a \in A$ tq $a \neq 0$, on a, $a = up_1...p_r, u \in U(A)$, p_i irréductible.
3. Si $a = up_1...p_r = vq_1...q_s$, alors $r = s$ et $\exists \sigma \in S_r$ tq $p_{\sigma(i)}$ est associé à q_i (i.e., la décomposition de a en produit de facteurs irréductibles est unique à permutation près et à éléments inversibles près).

Exemple 7 .

$\mathbb{Z}$ est un anneau factoriel.

Dans $\mathbb{Z}$ on a : $20 = 1.2^2.5 = 1.2.2.5 = (-1).2.2.(-5) = (-1).(-5).(-2).(-2)$.

5. Anneaux factoriels

Proposition 11 .

Dans un anneau factoriel A, on a :

1. Tout élément irréductible est premier.
2. Si $a = u\prod_{i\in I} p_i^{\alpha_i}$ et $b = v\prod_{i\in I} p_i^{\beta_i}$, alors $a \mid b \Leftrightarrow \alpha_i \leq \beta_i, \forall i \in I$.
3. On a le lemme de Gauss, si $a \mid bc$ et a et premier avec b, alors $a \mid c$.
4. Deux éléments quelconques possèdent un pgcd et un ppcm. Plus précisément, si $a = u\prod_{i\in I} p_i^{\alpha_i}$ et $b = v\prod_{i\in I} p_i^{\beta_i}$ alors, $d = \prod_{i\in I} p_i^{\min(\alpha_i,\beta_i)}$ est un pgcd de a et b et $m = \prod_{i\in I} p_i^{\max(\alpha_i,\beta_i)}$ est un ppcm de a et b.

Théorème 2 .

Tout anneau principal est factoriel.

Preuve

Soit A un anneau principal. Par l'absurde, supposons qu'il existe un élément non nul et non inversible de A qui n'est pas produit d'éléments irréductibles. Notons $\mathcal{F}$ l'ensemble des idéaux propres dont les générateurs ne sont pas produit d'éléments irréductibles. On a $\mathcal{F} \neq \emptyset$. Puisque A est principal, alors il est noethérien et donc $\mathcal{F}$ contient un élément maximal pour l'inclusion $J = (a)$. On a a n'est pas inversible. Soit p un élément premier divisant a. Alors $a = pb$. Par conséquent, $(a) \subsetneq (b)$. D'où $b \notin \mathcal{F}$. Il en résulte que b est ou bien inversible, ou bien un produit d'éléments premiers. Par suite, a est produit d'éléments premiers. Une contradiction.

Théorème 3 (Théorème de transfert de Gauss).

Si A est un anneau factoriel, alors $A[X]$ est un anneau factoriel.

Exemple 8 .

$\mathbb{Z}[X]$ est un anneau factoriel car $\mathbb{Z}$ est factoriel.

6. Exercices

Exercice 1

On se place dans l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}$.
On note $(2, X) := 2\mathbb{Z}[X] + X\mathbb{Z}[X]$ l'idéal de $\mathbb{Z}[X]$ engendré par 2 et X.

1. Montrer que $(2, X)$ n'est pas principal.
2. Montrer que l'application $f : \mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z}$ définie par $f(P) = \overline{P(0)}$ est un morphisme d'anneaux surjectif.
3. Montrer que $ker(f) = (2, X)$.
4. En déduire que $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$.
5. Que peut-on dire de l'idéal $(2, X)$.

Exercice 2

Soit l'application $f : \mathbb{Z}[i] \to \mathbb{Z}/10\mathbb{Z}$ définie par $f(a + ib) = \overline{a + 7b}$.

1. Montrer que f est un morphisme d'anneaux surjectif.
2. Soit $(3 + i)$ l'idéal principal de $\mathbb{Z}[i]$ engendré par $3 + i$.
   Montrer que $10 \in (3 + i)$ et que $ker(f) = (3 + i)$.
3. En déduire que $\mathbb{Z}[i]/(3 + i) \cong \mathbb{Z}/10\mathbb{Z}$.
4. $3 + i$ est-il premier dans $\mathbb{Z}[i]$? Justifier.

Exercice 3

En utilisant la définition d'un idéal maximal, montrer que l'idéal (X) est un idéal maximal de $\mathbb{R}[X]$.

Exercice 4

Dans $\mathbb{R}[X]$, on considère l'idéal $(X^2 + 1)$ (l'idéal principal engendré par $X^2 + 1$).

1. Montrer que $(X^2 + 1)$ est un idéal premier de $\mathbb{R}[X]$.
2. L'idéal $(X^2 + 1)$ est-il maximal ? Justifier.

Exercice 5 (Examen normal 2021-2022)

On note $\mathbb{Z}[i\sqrt{5}]$ l'ensemble des complexes suivant : $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} : a, b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[i\sqrt{5}], +, .)$ est un anneau commutatif et unitaire.
2. On considère l'application $N : \mathbb{Z}[i\sqrt{5}] \longrightarrow \mathbb{N}$ définie par $N(a + ib\sqrt{5}) = a^2 + 5b^2$.
   Vérifier que $\forall z, z' \in \mathbb{Z}[i\sqrt{5}]$, on a $N(zz') = N(z)N(z')$.
3. Déterminer les éléments inversibles de $\mathbb{Z}[i\sqrt{5}]$.
4. Montrer que les éléments $2; 3; 1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles dans $\mathbb{Z}[i\sqrt{5}]$.
5. En déduire que l'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

Exercice 6

On considère l'anneau des entiers de Gauss $\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{Z}\}$.
On désigne par $Fr(\mathbb{Z}[i]) := \{\frac{u}{v} : u, v \in \mathbb{Z}[i], v \neq 0\}$ le corps des fractions de $\mathbb{Z}[i]$.

1. Montrer que $Fr(\mathbb{Z}[i]) = \mathbb{Q}[i] = \{z = x + iy : x, y \in \mathbb{Q}\}$.
2. Montrer que pour tout $x \in \mathbb{Q}$, il existe $a \in \mathbb{Z}$, tel que $|x - a| \leq \frac{1}{2}$.
3. Montrer que pour tout $u \in \mathbb{Q}[i]$ il existe $z \in \mathbb{Z}[i]$, tel que $|u - z|^2 < 1$.
4. En déduire que $\mathbb{Z}[i]$ est euclidien.

Exercice 7

Dans l'anneau $\mathbb{Z}[i\sqrt{5}]$ on considère les éléments :

$$z_1 = 2(1 + i\sqrt{5}) \text{ et } z_2 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

1. Montrer que z_1 et z_2 n'ont pas de pgcd.
2. En déduire que $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.