Compléments sur les anneaux, polynômes

Définition

Un *anneau* est la donnée d'un triplet $(A, +, \cdot)$ où A est un ensemble et $+ : A \times A \to A$ et $\cdot : A \times A \to A$ sont deux lois de composition interne tels que les propriétés suivantes sont remplies :

- le couple $(A, +)$ est un groupe abélien ;
- la loi $\cdot$ est associative, distributive (à droite et à gauche), par rapport à la loi $+$.

On note 0_A l'élément neutre pour la loi $+$. L'anneau est dit *unitaire* s'il existe un élément neutre 1_A (à droite et à gauche) pour la loi $\cdot$, *commutatif* si la loi $\cdot$ est commutative.
La loi $+$ est appelée *addition* et la loi $\cdot$ *multiplication*.

Exemples

(1) Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
(2) $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}$.
(3) Si K est un corps et V un K-espace vectoriel, $\mathrm{End}_K(V)$, muni de l'addition et de la composition des endomorphismes est un anneau unitaire (non commutatif si $\dim_K(V) > 1$).
(4) Si A est un anneau, l'anneau des polynômes $A[X]$, l'anneau des matrices $\mathrm{M}_n(A)$.
(5) Plein d'exemples en analyse.

Dans ce qui suit, tous les anneaux seront supposés *unitaires*.

Binôme de Newton

Si $a, b \in A$ *commutent* et $n \in \mathbb{N}$, on a

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

⚠ Mise en garde : il est important de supposer que $ab = ba$.

Définition - Anneaux produits

(1) Soient A_1 et A_2 deux anneaux. L'*anneau produit* est le produit cartésien $A_1 \times A_2$ muni des lois étant données par les formules

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$$

L'élément neutre pour l'addition (resp. la multiplication) est $(0_{A_1}, 0_{A_2})$ (resp. $1_{A_1 \times A_2} = (1_{A_1}, 1_{A_2})$).
(2) Soit I un ensemble. On note A^I (resp. $A^{(I)}$) l'ensemble des applications $I \to A$ (resp. des applications $I \to A$ qui sont nulles en dehors d'une partie finie de I). Muni des lois d'addition et de multiplication « composante par composante », A^I est un anneau.

Remarque

Lorsque I est infini, $A^{(I)}$ est un anneau *non unitaire*.

Définition

Soient A un anneau et $a \in A$.
(1) On dit que a est *inversible*, s'il existe $b \in A$ tel que $ab = ba = 1$. L'ensemble des éléments inversibles de A est noté $A^\times$. Muni de la restriction de la multiplication, c'est un groupe, d'élément neutre 1. L'anneau A est un *corps* s'il est non nul et $A^\times = A \setminus \{0\}$.
(2) On dit que a est *diviseur de zéro* s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$ ou $ba = 0$. L'anneau A est dit *intègre* s'il n'a pas de diviseur de zéro autre que 0. L'anneau nul n'est pas intègre.
(3) On dit que a est *nilpotent* s'il existe $n \in \mathbb{N}_{>0}$ tel que $a^n = 0$. L'anneau A est dit *réduit* s'il n'a pas d'élément nilpotent autre que 0.

Exemples

(1) Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps. Il en est de même de $\mathbb{Z}/p\mathbb{Z}$ lorsque p est un entier premier. L'anneau $\mathbb{Z}$ est intègre, mais ce n'est pas un corps.
(2) L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre, parce que $\overline{2}\,\overline{3} = \overline{0}$ alors que $\overline{2} \neq \overline{0}$ et $\overline{3} \neq \overline{0}$. En fait, on a $(\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}, \overline{5}\}$. Par contre, $\mathbb{Z}/6\mathbb{Z}$ est réduit.
(3) L'anneau $\mathbb{Z}/4\mathbb{Z}$ n'est pas réduit, car $\overline{2}^2 = \overline{0}$ mais $\overline{2} \neq \overline{0}$.

Définition

Soient A et B deux anneaux. Un *morphisme d'anneaux* de A vers B est un morphisme $f : A \to B$ entre les groupes additifs sous-jacents tel que

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

Remarques

(1) Si $f : A \to B$ et $g : B \to C$ sont deux morphismes d'anneaux, l'application composée $g \circ f$ est encore un morphisme d'anneaux.
(2) L'application $i : A \to A \times A$; $a \mapsto (a, 0)$ n'est pas un morphisme d'anneau, parce que $i(1_A) \neq 1_{A\times A}$.

Exemples

(1) Les inclusions $\mathbb{Z} \to \mathbb{Q}$, $\mathbb{Q} \to \mathbb{R}$, $\mathbb{R} \to \mathbb{C}$. Pour $n \in \mathbb{N}_{>1}$, la réduction modulo n : $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.
(2) Il existe un unique morphisme d'anneaux $c_A \colon \mathbb{Z} \to A$. C'est l'application qui à $z \in \mathbb{N}$ associe $c_A(z) = \underbrace{1_A + \cdots + 1_A}_{z \text{ fois}}$ et telle que $c_A(z) = -c_A(-z)$ si $z \in \mathbb{Z}_{<0}$.

Définition

Soit $f \colon A \to B$ un morphisme d'anneaux. Le noyau $\{a \in A,\ f(a) = 0_B\}$ (resp. l'image $\{f(a)\}_{a \in A}$) du morphisme de groupes sous-jacent s'appelle le *noyau* (resp. l'*image*) de f et est noté $\mathrm{Ker}(f)$ (resp. $\mathrm{Im}(f)$). Rappelons que f est injectif si et seulement si $\mathrm{Ker}(f) = \{0_A\}$.

⚠ $\mathrm{Ker}(f)$ n'est *pas* un sous-anneau de A.

Définition

Soient A et B deux anneaux. On dit que A est un *sous-anneau* de B si $A \subset B$ et si l'inclusion $A \hookrightarrow B$ est un morphisme d'anneaux.

Exemple

$\mathscr{C}^0([0,1],\mathbb{R})$ est un sous-anneau de $\mathscr{B}([0,1],\mathbb{R})$.

Remarque

Pour montrer qu'un ensemble muni de deux lois de composition interne est un anneau, il est souvent judicieux de voir comme un sous-anneau d'un anneau convenable. Par exemple,
$\mathbb{Z}[i] = \{a + ib\,;\ a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$.

Dans tout ce qui suit, A désigne un anneau.

Définition

Un *idéal à gauche* de A est un sous-groupe $I \subset A$ pour la loi $+$ tel que

$$(\forall a \in A)\,(\forall x \in I)\; ax \in I.$$

On définit la notion d'*idéal à droite* de façon analogue. Un *idéal bilatère* est un idéal à gauche qui est aussi un idéal à droite. Un idéal I est dit *strict* si $I \neq A$ (l'anneau A est toujours un idéal, appelé *idéal unité*).

Exemple

Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$ (en particulier ils coïncident avec les sous-groupes).

Proposition

Si $f : A \to B$ est un morphisme d'anneaux, alors $\mathrm{Ker}(f)$ est un idéal bilatère de A.

Remarque

Si $f : A \to B$ est un morphisme d'anneaux et $J \subset B$ un idéal à gauche (resp. à droite), alors $f^{-1}(J)$ est un idéal à gauche (resp. à droite) de A.

⚠Si $I \subset A$ est un idéal à gauche, $f(I)$ n'est pas un idéal à gauche de B en général (c'en est un lorsque f est surjectif).

Définition

Supposons A commutatif.

• Si $X \subset A$, l'idéal *engendré* par X est :

$$\left\{ \sum_{i=1}^{n} a_i x_i,\ n \in \mathbb{N},\ a_1, \ldots, a_n \in A,\ x_1, \ldots, x_n \in X \right\}.$$

Si $X = \{x_1, \ldots, x_r\}$, on note $x_1 A + x_2 A + \cdots + x_r A$ ou $\langle x_1, \ldots, x_r \rangle$.

• Un idéal engendré par un seul élément est dit *principal*, et un anneau *intègre* dont tous les idéaux sont principaux est dit *principal*.

Exemple

$\mathbb{Z}$ et $\mathbb{Q}[X]$ sont principaux, mais pas $\mathbb{Q}[X, Y]$ et $\mathbb{Z}[X]$.

Opérations sur les idéaux

Soient A un anneau commutatif et $\{I_\lambda\}_{\lambda\in\Lambda}$ une famille d'idéaux de A. L'intersection $\bigcap_{\lambda\in\Lambda} I_\lambda$ et $\sum_{\lambda\in\Lambda} I_\lambda$ sont des idéaux de A (rappelons que $\sum_{\lambda\in\Lambda} I_\lambda$ désigne l'ensemble des sommes *finies* $x_1 + \cdots + x_r$ avec $x_i \in I_{\lambda_i}$, et $\lambda_i \in \Lambda$).
Si $\Lambda = \{1, \ldots, n\}$ est *fini*, on note $I_1 I_2 \cdots I_n$ l'idéal engendré par l'ensemble des produits $x_1 x_2 \cdots x_n$ avec $x_j \in I_j$ pour $1 \leq j \leq n$.

Exemple

Dans $\mathbb{Z}$, on a $6\,\mathbb{Z} \cap 10\,\mathbb{Z} = 30\,\mathbb{Z}$, $6\,\mathbb{Z} + 10\,\mathbb{Z} = 2\,\mathbb{Z}$ et $(6\,\mathbb{Z})(10\,\mathbb{Z}) = 60\,\mathbb{Z}$.

Définition

Il existe un unique morphisme unitaire $c_A : \mathbb{Z} \to A$. Le noyau de ce morphisme est un idéal de $\mathbb{Z}$: il est de la forme $\mathrm{car}(A)\,\mathbb{Z}$ avec $n \in \mathbb{N}$. L'entier $\mathrm{car}(A)$ s'appelle la *caractéristique* de l'anneau A.

Exemple

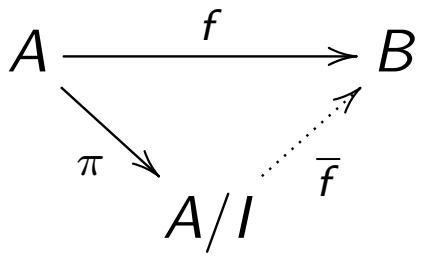
Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique 0, tout comme l'anneau $\mathbb{Z}$. Pour $n \in \mathbb{N}_{>1}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n.

Idéaux et quotients

Soit $I \subset A$ un idéal bilatère. On dispose du groupe quotient A/I et de la *projection canonique* $\pi : A \to A/I$.

Proposition - Définition

Le groupe A/I est naturellement muni d'une structure d'anneau pour laquelle la projection canonique π est un morphisme d'anneaux. L'anneau ainsi obtenu s'appelle l'*anneau quotient* de A modulo I. Le couple $(A/I, \pi)$ a la propriété universelle suivante : si $f : A \to B$ est un morphisme d'anneaux tel que $I \subset \mathrm{Ker}(f)$, alors il existe un unique morphisme d'anneaux $\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ \pi$.



Remarques

(1) Si A est commutatif, il en est de même de A/I.
(2) On a $I = \mathrm{Ker}(\pi : A \to A/I)$: tout idéal bilatère peut être vu comme le noyau d'un morphisme d'anneaux.
(3) Si $f : A \to B$ est un morphisme d'anneaux, on dispose de la factorisation canonique $f = \overline{f} \circ \pi$ où $\overline{f} : A/\mathrm{Ker}(f) \to B$ est un morphisme *injectif* d'anneaux (cela s'appelle « passer au quotient »). Si le morphisme f de départ est surjectif, le morphisme obtenu est alors un *isomorphisme*.

Désormais, les anneaux seront tous supposés *commutatifs*.

Idéaux et quotients

Soient A un anneau et $I \subset A$ un idéal. Notons $\pi : A \to A/I$ la surjection canonique. Si $J \subset A$ est un idéal contenant I, on dispose de $\pi(J) = J/I$: c'est un idéal de A/I. Réciproquement, si $\bar{J} \subset A/I$ est un idéal, alors $\pi^{-1}(\bar{J})$ est un idéal de A qui contient I.

Proposition

Les applications

$$\begin{aligned} \{\text{idéaux de } A \text{ contenant } I\} &\leftrightarrow \{\text{idéaux de } A/I\} \\ J &\mapsto \pi(J) = J/I \\ \pi^{-1}(\bar{J}) &\mapsfrom \bar{J} \end{aligned}$$

sont des bijections inverses l'une de l'autre. Par ailleurs, si $J \subset A$ est un idéal contenant I et $\bar{J} = J/I$, on a un isomorphisme naturel

$$A/J \xrightarrow{\sim} (A/I)/\bar{J}.$$

Théorème des restes chinois

Soient $I_1, \ldots, I_n \subset A$ des idéaux tels que pour $i \neq k$, on ait $I_j + I_k = A$. Alors $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$. En outre, si $\pi_j : A \to A/I_j$ désigne la projection canonique, on a un isomorphisme naturel

$$A/I_1 I_2 \cdots I_n \xrightarrow{\sim} \prod_{j=1}^{n} A/I_j$$

$$a \mapsto (\pi_j(a))_{1 \leq j \leq n}$$

Exemple

Soient $a_1, \ldots, a_n \in \mathbb{Z}$ des entiers non nuls deux-à-deux premiers entre eux (cela signifie exactement $a_j\,\mathbb{Z} + a_k\,\mathbb{Z} = \mathbb{Z}$ pour $j \neq k$). L'homomorphisme canonique

$$\mathbb{Z}\,/(a_1 a_2 \cdots a_n)\,\mathbb{Z} \xrightarrow{\sim} \prod_{j=1}^{n} \mathbb{Z}\,/a_j\,\mathbb{Z}$$

est un isomorphisme.

Exercice

Soient $a, b \in \mathbb{N}_{>0}$ et d et m leur pgcd et leur ppcm respectivement. Montrer que $(\mathbb{Z}\,/a\,\mathbb{Z}) \times (\mathbb{Z}\,/b\,\mathbb{Z}) \xrightarrow{\sim} (\mathbb{Z}\,/d\,\mathbb{Z}) \times (\mathbb{Z}\,/m\,\mathbb{Z})$.

Idéaux premiers, idéaux maximaux

Définition

Soient A un anneau et $I \subsetneq A$ un idéal strict.

(1) On dit que I est *maximal* si pour tout idéal strict $J \subset A$, on a $I \subset J \Rightarrow J = I$ (*i.e.* I est maximal pour l'inclusion parmi les idéaux stricts de A).

(2) On dit que I est *premier* si $(\forall (a, b) \in A^2)\ ab \in I \Rightarrow (a \in I \text{ ou } b \in I)$.

Proposition

Tout idéal maximal est premier.

Idéaux premiers, idéaux maximaux

Exemple

Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et les $p\mathbb{Z}$ avec p premiers.

Proposition

Soient A un anneau et $I \subset A$ un idéal. Alors

(1) A/I est un corps si et seulement si I est maximal ;

(2) A/I est intègre si et seulement si I est premier.

Remarques

(1) Une autre façon d'exprimer (1) est de dire qu'un anneau A est un corps si ses seuls idéaux sont $\{0\}$ et A.
(2) Si K est un corps et $f : K \to A$ un morphisme d'anneaux, alors f est automatiquement injectif.
(3) Comme tout corps est intègre, on retrouve le fait que tout idéal maximal est premier.

Proposition

Soient A un anneau et $I \subset A$ un idéal. La bijection

$$\{\text{idéaux de } A \text{ contenant } I\} \leftrightarrow \{\text{idéaux de } A/I\}$$
$$J \mapsto \pi(J) = J/I$$
$$\pi^{-1}(\bar{J}) \hookleftarrow \bar{J}$$

induit des bijections

$$\{\text{idéaux premiers de } A \text{ contenant } I\} \leftrightarrow \{\text{idéaux premiers de } A/I\}$$
$$\{\text{idéaux maximaux de } A \text{ contenant } I\} \leftrightarrow \{\text{idéaux maximaux de } A/I\}.$$

Idéaux premiers, idéaux maximaux

Définition

Un ensemble partiellement ordonné $(E, \leq)$ est *inductif* si toute chaîne (*i.e.* partie totalement ordonnée) de E admet un majorant.

Théorème de Zorn

Tout ensemble inductif non vide admet un élément maximal.

- tout ensemble peut être muni d'un bon ordre ;
- le théorème de la base incomplète en dimension quelconque ;
- le théorème de Tychonov (un produit d'espaces compacts est compact) ;
- le théorème de Hahn-Banach ;
- le paradoxe de Banach-Tarski ;
- l'existence de parties de $\mathbb{R}$ non mesurables au sens de Lebesgue...

Idéaux premiers, idéaux maximaux

Théorème de Krull

Soient A un anneau et $I \subset A$ un idéal strict. Alors il existe un idéal maximal $\mathfrak{m} \subset A$ tel que $I \subset \mathfrak{m}$. En particulier tout anneau admet au moins un idéal maximal.

Remarque

Construction de $\mathbb{R}$ avec les suites de Cauchy.

Proposition

Soient A un anneau principal et I un idéal premier non nul. Alors I est maximal.

Exemple

Soient $A = \mathbb{Q}[X, Y]$ et $I = \langle X \rangle \subset A$. L'anneau $A/I \simeq \mathbb{Q}[Y]$ est intègre, mais ce n'est pas un corps : l'idéal I est donc premier non nul, non maximal. La proposition implique que A n'est pas principal.

Anneaux principaux

Dans tout ce qui suit, A désigne un anneau intègre.

Définition

Soient $a, b \in A \setminus \{0\}$. On dit que b *divise* a et on note $b \mid a$ s'il existe $c \in A$ tel que $a = bc$ (on dit aussi que b est un *diviseur* de a, ou que a est un *multiple* de b). Cela équivaut à $\langle a \rangle \subset \langle b \rangle$ (on note $b \nmid a$ dans le cas contraire). Cela munit $A \setminus \{0\}$ d'une relation d'ordre.

Remarque

Cette relation d'ordre n'est pas totale en général. Par exemple, dans $\mathbb{Z}$, on a $2 \mid 6$, mais on n'a pas de relation de divisibilité entre 2 et 3.

Définition

Soient $a, b \in A \setminus \{0\}$. On dit que a et b sont *associés* si $a \mid b$ et $b \mid a$.

Comme A est intègre, a et b sont associés si et seulement s'il existe $u \in A^\times$ tel que $b = ua$, soit encore si et seulement si $\langle a \rangle = \langle b \rangle$: « être associés » est une relation d'équivalence (les classes d'équivalence sont les parties de la forme $aA^\times$ pour $a \in A \setminus \{0\}$).

Définition

Soit $\pi \in A$.
(1) On dit que π est *irréductible* dans A si $\pi \neq 0$, $\pi \notin A^\times$ et pour tous $a, b \in A$ on a $\pi = ab \Rightarrow (a \in A^\times \text{ ou } b \in A^\times)$ (les seuls diviseurs de π sont les unités et les éléments associés à π).
(2) On dit que π est *premier* si l'idéal principal πA est premier.

Proposition

Un élément premier est irréductible.

Remarque

⚠La réciproque est fausse en général (*eg* 2 irréductible mais pas premier dans $\mathbb{Z}[\sqrt{-5}]$).

Exemple

$A = \mathbb{Z}\left[\sqrt{-5}\right] = \left\{x + y\sqrt{-5}\,;\, x, y \in \mathbb{Z}\right\} \subset \mathbb{C}$. On dispose du morphisme d'anneaux

$$f : \mathbb{Z}[T] \to \mathbb{C}$$
$$T \mapsto \sqrt{-5}$$

On a $\mathrm{Im}(f) = A$ et $T^2 + 5 \in \mathrm{Ker}(f)$. Soient $P(T) \in \mathrm{Ker}(f)$, et $P(T) = (T^2 + 5)Q(T) + x + yT$ avec $x, y \in \mathbb{Z}$ sa division euclidienne par $T^2 + 5$ dans $\mathbb{Z}[T]$. On a $0 = f(P) = x + y\sqrt{-5}$, donc $x^2 = -5y^2$, d'où $x = y = 0$, *i.e.* $P(T) \in \langle T^2 + 5 \rangle$. Donc $\mathrm{Ker}(f) = \langle T^2 + 5 \rangle$.

Exemple

f induit un isomorphisme $\mathbb{Z}[T]/\langle T^2+5\rangle \xrightarrow{\sim} A$ donc $A/2A \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})[T]/\langle T^2+5\rangle = (\mathbb{Z}/2\mathbb{Z})[T]/\langle T+1\rangle^2$ n'est pas réduit, et 2 n'est pas premier dans A. Soit

$$N\colon A \to \mathbb{N}$$
$$z = x + y\sqrt{-5} \mapsto |z|^2 = x^2 + 5y^2$$

Si $z_1, z_2 \in A$, on a $N(z_1 z_2) = N(z_1)N(z_2)$. Supposons $2 = ab$ avec $a, b \in A$: on a donc $4 = N(2) = N(a)N(b)$, d'où $N(a), N(b) \in \{1, 2, 4\}$. L'équation $x^2 + 5y^2 = 2$ n'a pas de solution dans $\mathbb{Z}^2$: on a $N(a) = 1$ ou $N(b) = 1$, *i.e.* $a \in A^\times$ ou $b \in A^\times$ (si $a = x + y\sqrt{-5} \in A$ vérifie $N(a) = 1$, alors $a \in A^\times$ et $a^{-1} = \overline{a} = x - y\sqrt{-5} \in A$).

Exercices

(1) Soient K un corps, T une indéterminée et $A = K + T^2K[T] \subset K[T]$ (rappel : $K[X,Y]/\langle Y^2 - X^3 \rangle \xrightarrow{\sim} A$).
Montrer que T^2 est irréductible mais pas premier dans A.
(2) Soient $a, b \in A$ tels que $a \in A^\times$ ou bien a irréductible et $a \nmid b$.
Montrer que $aX + b$ est irréductible dans $A[X]$.

Anneaux principaux

On suppose que A est *principal* (*i.e.* intègre et dont idéaux sont principaux, *i.e.* engendrés par un élément).

Lemme

Soit $a \in A$. Les conditions suivantes sont équivalentes :

(i) a est irréductible ;

(ii) $\langle a \rangle$ est un idéal maximal ;

(iii) a est premier.

Lemme

Toute suite croissante d'idéaux de A est stationnaire.

Proposition

Soit $a \in A \setminus \{0\}$. Il existe $u \in A^\times$ et $\pi_1, \ldots, \pi_r \in A$ irréductibles tels que $a = u\pi_1 \cdots \pi_r$ (factorisation en produit d'éléments irréductibles). Si $a = v\varpi_1 \cdots \varpi_s$ avec $v \in A^\times$ et $\varpi_1, \ldots, \varpi_s$ irréductibles est une autre factorisation, alors $r = s$ et quitte à renuméroter, on a $\langle \pi_i \rangle = \langle \varpi_i \rangle$ pour tout $i \in \{1, \ldots, r\}$ (unicité de la factoriation).

Définition

Soient $a, b \in A$. L'idéal $\langle a, b\rangle = \langle a\rangle + \langle b\rangle$ (resp. $\langle a\rangle \cap \langle b\rangle$) est principal. On appelle *pgcd* (resp. *ppcm*) tout générateur de cet idéal, *i.e.*

$$\langle \mathrm{pgcd}(a, b)\rangle = \langle a\rangle + \langle b\rangle \quad \text{et} \quad \langle \mathrm{ppcm}(a, b)\rangle = \langle a\rangle \cap \langle b\rangle.$$

En particulier, si $a, b \in A$, il existe $u, v \in A$ tels que $au + bv = \mathrm{pgcd}(a, b)$ (relation de Bézout).

⚠ Les éléments $\mathrm{pgcd}(a, b)$ et $\mathrm{ppcm}(a, b)$ ne sont définis qu'à multiplication par un élément de $A^\times$ près.

Proposition - Lemme de Gauss

Soient $a, b, c \in A \setminus \{0\}$ tels que $\mathrm{pgcd}(a, b) = 1$. Si $a \mid bc$, alors $a \mid c$.

Anneaux euclidiens

Soit A est anneau *intègre*.

Définition

(1) Un *stathme euclidien* est une application $\phi\colon A \setminus \{0\} \to \mathbb{N}$ telle que si $a, b \in A \setminus \{0\}$ sont tels que b divise a, alors $\phi(b) \leq \phi(a)$.
(2) Un stathme euclidien ϕ définit une *division euclidienne* si pour tout $(a, b) \in A \times A \setminus \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ et ($r = 0$ ou $\phi(r) < \phi(b)$). L'élément q s'appelle alors « le » *quotient* et r « le » *reste* de la division.
(3) Un anneau est dit *euclidien* s'il admet un stathme euclidien définissant une division euclidienne.

Remarque

Si A est un anneau euclidien, il n'y a pas unicité d'un stathme euclidien sur A. En outre, on ne requiert pas l'unicité du quotient et du reste.

Anneaux euclidiens

Exemples

(1) Tout corps est un anneau euclidien. L'anneau $\mathbb{Z}$ est euclidien, avec le stathme donné par $\phi(a) = |a|$ (valeur absolue). Dans ce cas, la division est la division euclidienne habituelle ; elle est unique. Si K est un corps, l'anneau de polynômes $K[X]$ est euclidien, avec le stathme donné par $\phi(P) = \deg(P)$. Là encore, la division est la division euclidienne habituelle et elle est unique.
(2) L'anneau $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \,;\, a, b \in \mathbb{Z}\}$ des *entiers de Gauss* est euclidien, muni du stathme $\phi(a + ib) = a^2 + b^2$ (exercice).

Proposition

Tout anneau euclidien est principal.

Corollaire

$\mathbb{Z}$ et $K[X]$ (avec K un corps) sont principaux.

Remarque

Dans les anneaux euclidiens, on dispose de l'algorithme d'Euclide (étendu), qui permet de calculer le pgcd de deux éléments (de trouver une relation de Bézout).

Exercices

(1) Soient $n, m \in \mathbb{N}_{>0}$. Calculer $\text{pgcd}(X^n - 1, X^m - 1)$ dans $\mathbb{Q}[X]$.
(2) Montrer que l'anneau $\mathbb{Z}[j] = \{a + bj \,;\, a, b \in \mathbb{Z}\}$ est euclidien.

Soit A un anneau.

Définition

L'anneau des *séries formelles* à coefficients dans A est l'ensemble $A^{\mathbb{N}}$ des suites à valeurs dans A muni des deux lois suivantes :

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}}$$
$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}}$$

où $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

Remarque

⚠ Il ne faut pas le confondre avec l'anneau produit $A^{\mathbb{N}}$ (*i.e.* muni des lois « composante par composante »).

Notons X l'élément $(0,1,0,0,\ldots) \in A^{\mathbb{N}}$: par définition, on a $X^n = (\underbrace{0,\ldots,0}_{n},1,0,\ldots)$ pour tout $n \in \mathbb{N}$, donc

$$(a_n)_{n\in\mathbb{N}} = \sum_{n=0}^{\infty} a_n X^n$$

(c'est sous cette forme qu'on écrit une série formelle dans la pratique).

Définition

Avec la notation qui précède, X s'appelle l'*indéterminée*. On parle alors de l'anneau des séries formelles en l'indéterminée X à coefficients dans A, et on le note $A[\![X]\!]$.

Définition

L'anneau des *polynômes* en l'indéterminée X à coefficients dans A est le sous-anneau $A[X]$ de l'anneau $A[\![X]\!]$ constitué des suites à support fini.

Remarque

Un polynôme s'écrit donc comme une somme finie

$$P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_dX^d.$$

Définition

(1) Si $f(X) = \sum_{n=0}^{\infty} a_n X^n \in A[\![X]\!]$, l'élément a_0 s'appelle le coefficient constant de $f(X)$.
(2) Soit $P \in A[X] \setminus \{0\}$. On peut écrire $P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$ avec $a_d \neq 0$. L'entier d s'appelle le *degré* de P : on le note $\deg(P)$ par convention, on a $\deg(0) = -\infty$). L'élément a_d s'appelle le *coefficient dominant* de P. On dit que P est *unitaire* lorsque son coefficient dominant vaut 1.
(3) Un polynôme de la forme aX^d s'appelle un *monôme*.

Remarque

L'application $A \to A[X]$ qui envoie a sur $(a, 0, \ldots)$ est un morphisme injectif d'anneaux : l'anneau A est donc naturellement un sous-anneau de $A[X]$ (polynômes constants).

Propriétés du degré

Si $P, Q \in A[X]$, on a

$$\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}$$
$$\deg(PQ) \leq \deg(P) + \deg(Q).$$

Ces inégalités sont strictes en général. La première est une égalité si $\deg(P) \neq \deg(Q)$, la deuxième si le coefficient dominant de P ou de Q n'est pas diviseur de zéro.

Exemple

Si $P = Q = 1 + 2X \in (\mathbb{Z}/4\mathbb{Z})[X]$, alors $PQ = 1$ est de degré 0.

Corollaire

Si A est intègre, il est de même de $A[X]$.

Exercice

Si A est intègre, on a $A[X]^\times = A^\times$.

Théorème - Division euclidienne

Soient A un anneau et $P, D \in A[X]$. On suppose que le coefficient dominant de D est inversible. Alors il existe un unique couple $(Q, R) \in A[X]$ tel que

$$\begin{cases} P = QD + R \\ \deg(R) < \deg(D) \end{cases}$$

Le polynôme Q (resp. R) s'appelle le *quotient* (resp. le *reste*) dans la division euclidienne de P par Q.

Remarques

Si K est un corps, la division euclidienne par un polynôme non nul existe toujours dans $K[X]$.

⚠ Il n'existe pas de division euclidienne de X par 2 dans $\mathbb{Z}[X]$.

Théorème - Propriété universelle

Soient $f : A \to B$ un morphisme d'anneaux et $b \in B$. Il existe un unique morphisme d'anneaux $\widetilde{f} : A[X] \to B$ tel que $\widetilde{f}(a) = f(a)$ pour tout $a \in A$ et $\widetilde{f}(X) = b$.

Dans la pratique, si $P \in A[X]$, on note $P(b)$ l'élément $\widetilde{f}(P) \in B$.

Définition

Soient A un anneau et $\alpha \in A$. Le morphisme d'*évaluation* en α est l'unique morphisme $\mathrm{ev}_\alpha : A[X] \to A$ prolongeant l'identité de A et envoyant X sur α.

Remarque

Un polynôme $P \in A[X]$ fournit donc l'application

$$\begin{aligned} A &\to A \\ \alpha &\mapsto P(\alpha) \end{aligned}$$

Les fonctions ainsi obtenues sont appelées *fonctions polynômiales*.
⚠Ne pas confondre un polynôme avec la fonction polynômiale qu'il définit. Par exemple si $A = \mathbb{Z}/2\mathbb{Z}$, le polynôme $X^2 - X$ est non nul, mais ne prend que des valeurs nulles sur $\mathbb{Z}/2\mathbb{Z}$.

Exemple

Soient $\mathbb{Z}[i] = \{a + ib\,;\, a, b \in \mathbb{Z}\} \subset \mathbb{C}$ et $f :\ \mathbb{Z}[X] \to A$ qui envoie X sur i. f est surjectif, et la division euclidienne implique que $\mathrm{Ker}(f) = \langle X^2 + 1\rangle$. En passant au quotient, on obtient un isomorphisme

$$\mathbb{Z}[X]/\langle X^2 + 1\rangle \xrightarrow{\sim} \mathbb{Z}[i].$$

De même, on a un isomorphisme $\mathbb{R}[X]/\langle X^2 + 1\rangle \xrightarrow{\sim} \mathbb{C}$.

Exercice

Soient A un anneau, $I \subset A$ un idéal. Montrer qu'on a un isomorphisme naturel

$$A[X]/IA[X] \xrightarrow{\sim} (A/I)[X].$$

Définition

(1) Si A est un anneau, on pose

$$A[X_1, \ldots, X_r] = (A[X_1, \ldots, X_{r-1}])[X_r].$$

Concrètement, un élément de $A[X_1, \ldots, X_r]$ est une somme finie

$$P(X_1, \ldots, X_r) = \sum_{\underline{n} \in \mathbb{N}^r} a_{\underline{n}} X_1^{n_1} \cdots X_r^{n_r}$$

où $a_{\underline{n}} \in A$ est nul sauf pour un nombre fini d'indices $\underline{n} = (n_1, \ldots, n_r) \in \mathbb{N}^r$.

(2) Un polynôme $P \in A[X_1, \ldots, X_r]$ est dit *homogène* de degré d si c'est une somme de monômes de degré d, c'est-à-dire si $P(X_1, \ldots, X_r) = \sum_{\underline{n} \in \mathbb{N}^r} a_{\underline{n}} X_1^{n_1} \cdots X_r^{n_r}$ avec $a_{\underline{n}} = 0$ dès que $|\underline{n}| := n_+ \cdots + n_r \neq d$. Tout élément $P \in A[X_1, \ldots, X_r]$ s'écrit de façon unique $P = P_0 + P_1 + \cdots + P_d$ avec P_i homogène de degré i.

Théorème - Propriété universelle

Soient $f : A \to B$ un morphisme d'anneaux et $b_1, \ldots, b_r \in B$. Il existe un unique morphisme d'anneaux $\widetilde{f} : A[X_1, \ldots, X_r] \to B$ tel que $\widetilde{f}(a) = f(a)$ pour tout $a \in A$ et $\widetilde{f}(X_i) = b_i$ pour tout $i \in \{1, \ldots, r\}$.

Là encore, on note $P(b_1, \ldots, b_r)$ l'élément $\widetilde{f}(P)$.

Exercice

Soient K un corps et X, Y, T des indéterminées.
(1) Montrer que le morphisme d'anneaux $f : K[X, Y] \to K[T]$ qui est l'identité sur K et envoie X sur T^2 et Y sur T^3 a l'idéal $\langle Y^2 - X^3 \rangle$ pour noyau et $A := K + T^2K[T] \subset K[T]$ pour image.
(2) Montrer que l'idéal engendré par T^2 et T^3 n'est pas principal dans A.

Corps des fractions

Soit A un anneau intègre. On construit un corps qui contient A et qui est « minimal » pour cette propriété. On munit l'ensemble $A \times (A \setminus \{0\})$ de la relation binaire donnée par :

$$(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow a_1 s_2 = a_2 s_1.$$

Lemme

C'est une relation d'équivalence.

On note $\mathrm{Frac}(A)$ l'ensemble quotient de $A \times (A \setminus \{0\})$ par cette relation d'équivalence. Pour $(a, s) \in A \times (A \setminus \{0\})$, on note $[(a, s)]$ son image dans $\mathrm{Frac}(A)$. On le munit de deux lois définies par

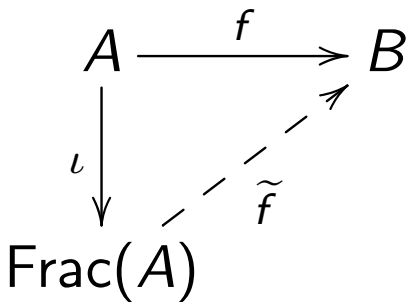
$$[(a_1, s_1)] + [(a_2, s_2)] = [(a_1 s_2 + a_2 s_1, s_1 s_2)]$$
$$[(a_1, s_1)] \cdot [(a_2, s_2)] = [(a_1 a_2, s_1 s_2)].$$

Proposition

Ces lois sont bien définies, et munissent $\mathrm{Frac}(A)$ d'une structure de corps : on l'appelle le *corps des fractions* de A. L'application

$$\iota : A \to \mathrm{Frac}(A);\ a \mapsto [(a, 1)]$$

définit un morphisme injectif d'anneaux (de sorte qu'on peut voir A comme un sous-anneau de $\mathrm{Frac}(A)$). Le couple $(\mathrm{Frac}(A), \iota)$ a la *propriété universelle suivante* : pour tout morphisme d'anneaux $f : A \to B$ tel que $(\forall a \in A \setminus \{0\})\ f(a) \in B^\times$, il existe un unique morphisme d'anneaux $\widetilde{f} : \mathrm{Frac}(A) \to B$ tel que $f = \widetilde{f} \circ \iota$.



Corps des fractions

Exemple

Le corps des fractions de $\mathbb{Z}$ est le corps $\mathbb{Q}$.

Soit K un corps. L'anneau des polynômes $K[X]$ est intègre : on dispose de son corps des fractions.

Définition

Le *corps des fractions rationnelles* (en l'indéterminée X) sur K est $K(X) := \mathrm{Frac}(K[X])$.

Ses éléments peuvent donc s'écrire comme des fractions $\frac{P}{Q}$ avec $P, Q \in K[X]$ et $Q \neq 0$. Cette écriture est unique si on suppose $\mathrm{pgcd}(P, Q) = 1$ et Q unitaire (on parle alors de forme irréductible).

Irréductibilité des polynômes

Soient A un anneau intègre, K son corps des fractions. On va donner des critères d'irréductibilité dans $A[X]$ et dans $K[X]$.

Remarque

⚠Cette question est bien entendu très sensible à l'anneau de coefficents considéré. Par exemple, le polynôme X^2+1 est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$. De même, le polynôme $2X$ est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{Z}[X]$. Il convient donc de toujours préciser « irréductible dans $A[X]$ ».

Définition

Soient $P \in A[X]$ et $\alpha \in A$. On dit que α est une *racine* de P si $P(\alpha) = 0$.

Critères d'irréductibilité

Lemme

Soient $P \in A[X] \setminus A$ et $\alpha \in A$. Si α est racine de P, alors P est divisible par $X - \alpha$. En particulier, P est réductible si $\deg(P) \geq 2$.

Corollaire

Soient K un corps et $P \in K[X]$. Alors P a un facteur de degré 1 si et seulement si P a une racine dans K.

Proposition

Soient K un corps et $P \in K[X]$.
(1) Si $\deg(P) = 1$, alors P est irréductible.
(2) Si $\deg(P) \in \{2, 3\}$, alors P est irréductible si et seulement s'il n'a pas de racine dans K.

Remarque

⚠ L'énoncé qui précède est très faux en degré ≥ 4. Par exemple, le polynôme $(X^2+1)^2$ n'a pas de racine dans $\mathbb{R}$, mais il est réductible. De même, il est faux en général sur un anneau qui n'est pas un corps : le polynôme $(2X+1)^2$ est réductible dans $\mathbb{Z}[X]$, mais n'a pas de racine dans $\mathbb{Z}$.

Lemme

Soit $P \in A[X]$ unitaire et réductible. Alors il existe $P_1, P_2 \in A[X]$ unitaires tels que $P = P_1 P_2$ et $\deg(P_1), \deg(P_2) < \deg(P)$.

Remarque

$2X+2$ est réductible dans $\mathbb{Z}[X]$.

Critères d'irréductibilité

Supposons A principal et posons $K = \mathrm{Frac}(A)$.

Définition

(1) Soit $P = a_0 + a_1 X + \cdots + a_d X^d \in A[X] \setminus \{0\}$. Le *contenu* de P est

$$\mathrm{c}(P) = \mathrm{pgcd}\{a_0, \ldots, a_d\}.$$

(2) Un polynôme $P \in A[X] \setminus \{0\}$ est primitif si et seulement si $\mathrm{c}(P) = 1$.

Lemme

Si $P, Q \in A[X] \setminus \{0\}$, on a
(1) $\mathrm{c}(aP) = a\,\mathrm{c}(P)$ pour tout $a \in A \setminus \{0\}$;
(2) $P = \mathrm{c}(P)\widetilde{P}$ avec $\widetilde{P} \in A[X]$ primitif ;
(3) $\mathrm{c}(PQ) = \mathrm{c}(P)\,\mathrm{c}(Q)$.

Critères d'irréductibilité

Proposition

Supposons A principal et soit $P \in A[X]$ de degré ≥ 1.
(1) Si P est irréductible dans $A[X]$, alors il l'est dans $K[X]$.
(2) Si P est primitif et irréductible dans $K[X]$, il l'est dans $A[X]$.

Exemples

(1) Un polynôme non constant et irréductible dans $\mathbb{Z}[X]$ est irréductible dans $\mathbb{Q}[X]$.
(2) Le polynôme $2X + 2$ est irréductible dans $\mathbb{Q}[X]$, mais réductible dans $\mathbb{Z}[X]$.

Remarque

⚠Si $A = \mathbb{Z}\left[\sqrt{-5}\right] \subset \mathbb{R}$ (il n'est pas principal), alors $P(X) := 2X^2 - 2X + 3$ est irréductible sur A, mais $P(X) = 2\left(X - \frac{1+\sqrt{-5}}{2}\right)\left(X - \frac{1-\sqrt{-5}}{2}\right)$ dans $K[X]$.

Soit $I \subset A$ un idéal strict. On dispose de la surjection canonique $A \to A/I$: elle induit un morphisme surjectif $A[X] \to (A/I)[X]$. Si $P \in A[X]$, notons $\bar{P}$ son image dans $(A/I)[X]$. Observons que $\deg(\bar{P}) \leq \deg(P)$, avec égalité si et seulement si le coefficient dominant de P n'appartient pas à I.

Théorème - Critère d'irréductibilité par réduction I

Supposons $P \in A[X]$ *unitaire*. Si $\bar{P} \in (A/I)[X]$ ne se factorise pas en un produit de deux polynômes de degrés $< \deg(P)$, alors P est irréductible dans $A[X]$.

Exemples

(1) $X^2 + X + 1 \in \mathbb{Z}[X]$ est irréductible, car unitaire et d'image modulo 2 irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$.
(2) Soit $P(X, Y) = X^2 + XY + 1 \in \mathbb{Q}[X, Y]$, $A = \mathbb{Q}[Y]$ et $I = Y\,\mathbb{Q}[Y]$. On a $A/I = \mathbb{Q}$ et l'image de P dans $\mathbb{Q}[X]$ est $X^2 + 1$, irréductible dans $\mathbb{Q}[X]$ donc P est donc irréductible dans $\mathbb{Q}[X, Y]$.

Remarque

(1) ⚠ L'hypothèse P unitaire n'est pas superflue : si $P = (1 + X^2)(1 + Y) \in \mathbb{Q}[X, Y]$, alors P est réductible, mais sa réduction modulo Y est irréductible.
(2) Dans l'énoncé qui précède, l'hypothèse « unitaire » peut être affaiblie en « à coefficient dominant inversible ».

Définition

Soient A un anneau intègre et $P \in A[X] \setminus \{0\}$. On dit que P est *primitif* si l'égalité $P = aQ$ avec $a \in A$ et $Q \in A[X]$ implique $a \in A^\times$.

Théorème - Critère d'irréductibilité par réduction II

Soient $\mathfrak{p} \subset A$ un idéal premier et $P(X) = a_0 + a_1 X + \cdots + a_d X^d \in A[X]$ *primitif* tels que

(i) $a_d \notin \mathfrak{p}$;

(ii) l'image $\bar{P}$ de P dans $(A/\mathfrak{p})[X]$ est irréductible.

Alors P est irréductible dans $A[X]$.

Exemple

Le polynôme $P(X) = 7X^3 - 4X^2 + X + 3$ est irréductible dans $\mathbb{Z}[X]$ car primitif et de réduction modulo 2 irréductible (c'est le polynôme $X^3 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ qui est de degré 3 sans racine).

Remarque

Les hypothèses du théorème sont nécessaires. Par exemple, $(2X + 1)X$ est réductible dans $\mathbb{Z}[X]$ bien que primitif et de réduction modulo 2 irréductible, parce que son coefficient dominant est 2.

Théorème - Critère d'Eisenstein

Soient $\mathfrak{p} \subset A$ un idéal premier et
$P(X) = a_0 + a_1 X + \cdots + a_d X^d \in A[X]$ *primitif* tels que

(i) $a_d \notin \mathfrak{p}$;

(ii) $a_0, a_1, \ldots, a_{d-1} \in \mathfrak{p}$;

(iii) $a_0 \notin \mathfrak{p}^2$.

Alors P est irréductible dans $A[X]$.

Remarque

(1) ⚠Bien sûr, l'hypothèse $a_0 \notin \mathfrak{p}^2$ est cruciale, par exemple le polynôme $X^2 - 4 = (X+2)(X-2) \in \mathbb{Z}[X]$ n'est pas irréductible.
(2) Ce critère ne s'applique pas lorsque A est un corps (le seul idéal premier est $\{0\}$...)
(3) À l'inverse des critères par réduction, le critère d'Eisenstein s'applique quand la réduction $\bar{P}$ est très réductible.

Exemples

(1) Le polynôme $X^4 + 4X^3 + 6X^2 + 10$ est irréductible dans $\mathbb{Z}[X]$ (prendre $\mathfrak{p} = 2\,\mathbb{Z}$). Par contre, le critère ne s'applique pas au polynôme $X^5 - 4$ (qui est irréductible dans $\mathbb{Z}[X]$ cependant).
(2) Le polynôme $2X^3 + 3$ est irréductible dans $\mathbb{Z}[X]$ (prendre $\mathfrak{p} = 3\,\mathbb{Z}$) ; le polynôme $Y^{14} - X(X-1)(X+1)$ est irréductible dans $\mathbb{Q}[X, Y]$ (prendre $A = \mathbb{Q}[X]$ et $\mathfrak{p} = \langle X \rangle$).

Exemples

(3) Soit p un nombre premier et $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$ (on l'appelle le p-ième polynôme cyclotomique). Alors Φ_p est irréductible. On a $\Phi_p(X) = \frac{X^p-1}{X-1} \in \mathbb{Q}(X)$: on effectue le changement de variable $X = Y + 1$. On a alors $\Phi_p(X) = \frac{(Y+1)^p-1}{Y}$ d'où

$$\Phi_p(X) = Y^{p-1} + \binom{p}{1} Y^{p-2} + \binom{p}{2} Y^{p-3} + \cdots + \binom{p}{p-1}.$$

Comme $p \mid \binom{p}{k}$ pour tout $k \in \{1, \ldots, p-1\}$ et $\binom{p}{p-1} = p$ est non divisible par p^2, le critère d'Eisenstein s'applique et $\Phi_p(Y+1)$ est irréductible dans $\mathbb{Z}[Y] = \mathbb{Z}[X]$: il en est de même de Φ_p.