Algèbre : théorie des anneaux

Florent Nacry (florent.nacry@univ-perp.fr)
Laboratoire LAMPS (Bât B, Etage 1)
Université Perpignan Via Domitia

Objectifs du chapitre

- Anneaux : définitions, exemples et premières propriétés.
- Eléments remarquables d'un anneau.
- Sous-anneaux et idéaux.
- Morphismes et caractéristique.
- Anneau quotient et théorème d'isomorphisme/de correspondance.
- Diverses classes d'anneaux et d'idéaux.
- Arithmétique dans les anneaux commutatifs.

Notion d'anneau

Nous commençons bien sûr par la définition d'un anneau.

Définition

Un **anneau** est la donnée d'un ensemble A et de deux lois de composition interne, notées $+$ et $\times$ (appelées respectivement addition et multiplication) telles que :

(i) $(A;+)$ est un groupe commutatif;

(ii) Pour tout $a, b, c \in A$,

$$(a \times b) \times c = a \times (b \times c).$$

(iii) Il existe un élément $1_A \in A$ tel que

$$a \times 1_A = 1_A \times a = a.$$

(iv) Pour tout $a, b, c \in A$,

$$a \times (b+c) = a \times b + a \times c \quad \text{et} \quad (b+c) \times a = b \times a + c \times a.$$

Non-vacuité et anneau nul

Soit $(A;+,\times)$ un anneau. Notons que l'ensemble A est nécessairement non vide : $(A;+)$ étant un groupe, on a $\{0_A\} \subset A$.

Lorsque l'inclusion ci-dessus est une égalité, on dit que A **est réduit à zéro ou encore que** A **est l'anneau nul.**

Si A est l'anneau nul, on a évidemment $0_A = 1_A$. Réciproquement, supposons que $1_A = 0_A$. On alors pour chaque $x \in A$,

$$x = x \times 1_A = x \times 0_A = x \times (0_A + 0_A) = x \times (1_A + 1_A) = x \times 1_A + x \times 1_A = x + x,$$

i.e., $x = 0_A$. Ceci montre alors que $A = \{0_A\}$, c'est-à-dire que A est réduit zéro.

A propos de la multiplication

- **Existence de l'unité pour la multiplication.** Certains auteurs ne supposent pas l'existence d'un élément 1_A donné par la propriété (*iii*) : les anneaux vérifiant cette propriété sont alors qualifiés *d'unitaires*. Nous n'utiliserons pas cette terminologie.

- **Commutativité de la multiplication.** Soit $(A;+,\times)$ un anneau. Lorsque $a \times b = b \times a$ pour tout $a, b \in A$, on dit que la loi multiplicative $\times$ est **commutative** ou encore que l'anneau $(A;+,\times)$ est **commutatif**.

Quelques exemples

- Les ensembles $\mathbb{Z}, \mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis des opérations usuelles sont des anneaux commutatifs.
- Soit $n \geq 2$ un entier. L'ensemble $M_n(A)$ des matrices à coefficients dans un anneau commutatif A est un anneau non commutatif.
- Soit G un groupe commutatif. Alors, l'ensemble des endomorphismes $\mathrm{End}(G)$ de G muni de l'addition et de la composition est un anneau (non commutatif en général).
- Pour $n \geq 2$, le groupe commutatif $\mathbb{Z}/n\mathbb{Z}$ muni de la multiplication définie par

$$\overline{k} \cdot \overline{l} := \overline{k \cdot l} \quad \text{pour tout } k, l \in \mathbb{Z}$$

est un anneau commutatif.

- L'ensemble $\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{Z}\}$ est un anneau commutatif.

Notations additives et multiplicatives

Soient $(A;+,\times)$ un anneau, $a,b \in A$ et $n \geq 1$ un entier.

- En général, on omet le $\times$ dans la multiplication : on écrit ab plutôt que $a \times b$.
- La loi multiplicative $\times$ est parfois notée à l'aide d'un simple point : $a \cdot b$ désignant alors le produit ab.
- Comme d'usage en théorie des groupes, $-a$ désigne l'inverse de a dans $(A;+)$.
- On note

$$na := \underbrace{a + \ldots + a}_{n-\text{fois}} \quad \text{et} \quad a^n := \underbrace{a \times \ldots \times a}_{n-\text{fois}}$$

  Il est clair que $n(-a) = -(na)$. On note traditionnellement $-na$ cet élément de A.
- On convient que $a^0 := 1_A$.

Règles de calculs sur un anneau

Les règles de calculs (naturelles !) ci-dessous doivent tout de même être établies.

Proposition

Soit $(A;+,\times)$ un anneau. Ont lieu :

(a) Pour tout $a \in A$, $0_A = a \times 0_A = 0_A \times a$.

(b) Pour tout $a, b \in A$, $a \times (-b) = -(a \times b) = (-a) \times b$.

(c) Pour tout $a, b \in A$, $a \times b = (-a) \times (-b)$.

(d) Pour tout $a, b, c, d \in A$, $(a+b) \times (c+d) = (a \times c) + (a \times d) + (b \times c) + (b \times d)$.

(e) Pour tout $n \in \mathbb{Z}$, pour tout $a, b \in A$, $(na) \times b = n(a \times b) = a \times (nb)$.

(f) Pour tout $m, n \in \mathbb{N}$, pour tout $a \in A$, $a^n \times a^m = a^{m+n}$ et $(a^m)^n = a^{mn}$.

La démonstration

(a) Soit $a \in A$. On a

$$a \times 0_A = a \times (0_A + 0_A) = a \times 0_A + a \times 0_A,$$

d'où $a \times 0_A = 0_A$. De même, $0_A \times a = 0_A$.
(b) Soient $a, b \in A$. On a

$$a \times b + a \times (-b) = a \times (b + (-b)) = a \times 0_A = 0_A,$$

d'où $a \times (-b) = -(a \times b)$. De même, on a $(-a) \times b = -(a \times b)$.
(c) Conséquence directe de (b).
(d) Découle de (iv) dans la définition des anneaux.
(e) On montre d'abord par une récurrence immédiate les égalités souhaitées pour tous les entiers naturels. L'extension à $\mathbb{Z}$ s'obtient via (b).
(f) Découle de la propriété d'associativité de la multiplication sur A.

$\blacksquare$

Binôme de Newton

Le lecteur a déjà rencontré le binôme de Newton dans $\mathbb{R}$ ou $\mathbb{C}$ ainsi que dans le calcul matriciel. C'est en fait un résultat général propre à la théorie des anneaux.

Proposition (Binôme de Newton)

Soient a, b deux éléments d'un anneau $(A; +, \times)$ et $n \geq 1$ un entier. Si a et b commutent (i.e., $ab = ba$), alors on a

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

et

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-k-1}.$$

La démonstration

Procédons par récurrence pour la première égalité. La propriété souhaitée a lieu pour l'exposant 0 puisque $(a+b)^0 = 1_A$ et $a^0 = b^0 = 1_A$. Fixons $l \in \mathbb{N}$ et supposons que

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

Le fait que a et b commutent donne

$$(a+b)^{l+1} = (a+b)(a+b)^l = \sum_{k=0}^{l} C_l^k a^{k+1} b^{l-k} + \sum_{k=0}^{l} C_l^k a^k b^{l+1-k}.$$

On a alors

$$(a+b)^{l+1} = \sum_{k=1}^{l+1} C_l^{k-1} a^k b^{l+1-k} + \sum_{k=0}^{l} C_l^k a^k b^{l+1-k},$$

d'où l'on tire

$$(a+b)^{l+1} = \sum_{k=1}^{l} \left(C_l^{k-1} + C_l^k\right) a^k b^{l+1-k} + a^{l+1} + b^{l+1}.$$

En combinant ceci et l'égalité $C_l^{k-1} + C_l^k = C_{l+1}^k$ valide pour tout $k \in \{1, \dots l\}$, on aboutit sans difficultés à

$$(a+b)^{l+1} = \sum_{k=1}^{l} C_{l+1}^k a^k b^{l-k+1} + a^{l+1} + b^{l+1} = \sum_{k=0}^{l+1} C_{l+1}^k a^k b^{l+1-k}.$$

La récurrence est terminée.

La démonstration - suite et fin

Pour la deuxième égalité, il suffit d'écrire (en gardant à l'esprit que $ab = ba$)

$$(a-b)\sum_{k=0}^{n-1} a^k b^{n-k-1} = \sum_{k=0}^{n-1} a^{k+1} b^{n-k-1} - \sum_{k=0}^{n-1} a^k b^{n-k} = \sum_{k=1}^{n} a^k b^{n-k} - \sum_{k=0}^{n-1} a^k b^{n-k}$$

puis

$$(a-b)\sum_{k=0}^{n-1} a^k b^{n-k-1} = a^n b^{n-n} - a^0 b^{n-0} = a^n - b^n.$$

■

L'anneau $A[X]$

Nous développons ici l'une des classes d'anneaux les plus importants : les anneaux de polynômes à une indéterminée.

Soit $(A;+,\times)$ un anneau commutatif. On appelle **polynôme à une indéterminée à coefficients dans** A une suite d'éléments $(a_n)_{n\in\mathbb{N}}$ de A à support fini (i.e., nulle à partir d'un certain rang). Cet ensemble est noté $A^{(\mathbb{N})}$.

L'ensemble $A^{(\mathbb{N})}$ est muni d'une structure d'anneau commutatif à travers les lois $\oplus$ et $\otimes$ définies pour tout $(a_n)_{n\in\mathbb{N}},(b_n)_{n\in\mathbb{N}} \in A^{(\mathbb{N})}$

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

et

$$(a_n)_{n\in\mathbb{N}} \otimes (b_n)_{n\in\mathbb{N}} = (\sum_{k=0}^{n} a_k b_{n-k})_{n\in\mathbb{N}}$$

Il est commode de noter P sous la forme $(a_0, a_1, \ldots, a_m, 0, 0, \ldots)$. L'élément neutre de $\oplus$ est évidemment $(0_A, 0_A, \ldots)$ et l'élément neutre de $\otimes$ est donné par $(1_A, 0_A, 0_A, \ldots)$.

L'indéterminée

L'élément $X := (0_A, 1_A, 0_A, 0_A, \ldots) \in A^{(\mathbb{N})}$ joue un rôle fondamental. On pose $X^0 := (1_A, 0_A, \ldots)$. Par ailleurs, on montre par une récurrence immédiate que pour chaque entier $k \geq 1$,

$$X^k = (\underbrace{0_A, \ldots, 0_A}_{k-fois}, 1_A, 0_A, 0_A, \ldots)$$

En définissant sur $A[X]$ une loi externe . via l'égalité

$$\lambda.(a_n)_{n\in\mathbb{N}} = (\lambda \times a_n)_{n\in\mathbb{N}}$$

pour tout $(a_n)_{n\in\mathbb{N}} \in A^{(\mathbb{N})}$ et pour tout $\lambda \in A$, nous voyons que pour tout entier $m \in \mathbb{N}$, pour tout $a_0, \ldots, a_m \in A$,

$$(a_0, a_1, \ldots, a_m, 0_A, 0_A, \ldots) = \sum_{n=0}^{m} a_n X^n.$$

Remarque. Traditionnellement, on abandonne l'écriture séquentielle (le terme de gauche) du polynôme au profit de l'écriture faisant intervenir les puissances successives de l'indéterminée X (le terme de droite). L'ensemble A est alors noté $A[X]$.

Le degré

On aura par la suite besoin du concept de degré d'un polynôme.

Soit A un anneau commutatif. Si $P \in A[X]$ est non nul, on appelle **degré** de P l'entier

$$\deg(P) := \max\{k \in \mathbb{N} : a_k \neq 0\}.$$

Traditionnellement, on convient que le degré du polynôme nul est $-\infty$.

Pour tout $P, Q \in A[X]$, on montre facilement que

$$\deg(PQ) \leq \deg(P) + \deg(Q).$$

Attention, toutefois que dans un anneau commutatif quelconque (contrairement aux polynômes sur un corps commutatif) l'inégalité ci-dessus n'est pas en général une égalité.

Pour $P \in A[X]$ non nul, il existe donc $a_0, \ldots, a_d$ avec $d := \deg(P)$ tels que

$$P = \sum_{k=0}^{d} a_k X^k.$$

L'élément non nul $a_d \in A$ est appelé **coefficient dominant** de P.

Le cas d'un polynôme constant

Soit A un anneau commutatif.

L'ensemble A_0 des polynômes de degré 0 s'identifie à $A^\star$ via l'application injective $\varphi : A^\star \to A_0$ définie par

$$\varphi(a) = \sum_{k=0}^{0} aX^k = (a, 0_A, 0_A, \ldots) \quad \text{pour tout } a \in A^\star.$$

De même, l'ensemble des polynômes constants (i.e., $A_0 \cup \{0\}$) s'identifie à A.

Anneau des polynômes à plusieurs indéterminées

Soit A un anneau commutatif. On a détaillé ci-dessus la construction de l'anneau des polynômes à une indéterminée X_1 à coefficients dans l'anneau A, noté $A[X_1]$. Puisque $A[X_1]$ est un anneau commutatif, on peut reproduire la même construction et ainsi obtenir l'anneau $A[X_1, X_2] := (A[X_1])[X_2]$ des polynômes à une indéterminée X_2 à coefficients dans l'anneau $A[X_1]$.

Un élément générique P de l'anneau $A[X_1, X_2]$ s'écrit sous la forme

$$P = \sum_{k=0}^{m} P_k {X_2}^k \quad \text{pour } m \in \mathbb{N} \text{ et } P_0, \ldots, P_k \in A[X_1].$$

En exploitant le fait que pour chaque chaque entier $k \in \{0, \ldots, m\}$, il existe un $r_k \in \mathbb{N}$ et $a_{0,k}, \ldots, a_{r_k,k}$ tels que $P_k = \sum_{l=0}^{r_k} a_{l,k} X_1^l$, on aboutit à l'écriture

$$P = \sum_{k=0}^{m} \Big(\sum_{l=0}^{r_k} a_{l,k} X_1^l \Big) {X_2}^k$$

On réitère ce procédé pour construire pour tout entier $n \geq 2$ l'anneau $A[X_1, \ldots, X_{n-1}][X_n] =: A[X_1, \ldots, X_n]$.

Les algèbres sur un corps

Sur $K[X]$ ou sur $M_n(\mathbb{K})$ (K corps commutatif) cohabitent trois lois usuelles : l'addition et la multiplication interne (conférant la structure d'anneau) mais aussi la multiplication externe (qui avec l'addition confère la structure de K-espace vectoriel). Ceci conduit à introduire la définition suivante :

Définition

Soient K un corps commutatif et E un ensemble. On dit que E est une K**-algèbre** lorsqu'il existe deux lois internes $+$ et $\times$ sur E et une loi externe $\cdot : K \times E \to E$ satisfaisant :

(i) $(E;+,\cdot)$ est un K-espace vectoriel;

(ii) $(E;+,\times)$ est un anneau;

(iii) Pour tout $\lambda \in K$, pour tout $a, b \in E$,

$$\lambda \cdot (a \times b) = (\lambda . a) \times b = a \times (\lambda . b).$$

On peut étendre la notion d'algèbre au cas d'anneaux à condition d'étendre au préalable la notion de K-espace vectoriels aux anneaux. Un espace vectoriel sur un anneau est connu sous le nom de *module*.

Produit d'anneaux

On cherche ici à munir le produit cartésien d'anneaux d'une structure d'anneau.

Soit $(A_i)_{i\in I}$ une famille non vide d'ensembles. On note $\prod_{i\in I} A_i$ l'ensemble des applications $f : I \to \bigcup_{i\in I} A_i$ vérifiant $f(i) \in A_i$ pour chaque $i \in I$. On l'appelle le **produit cartésien** de la famille $(A_i)_{i\in I}$. Un élément $f \in \prod_{i\in I} A_i$ est traditionnellement noté sous la forme $(x_i)_{i\in I}$ avec $x_i := f(i)$ pour chaque $i \in I$.

Supposons que chaque A_i soit un anneau muni d'une loi additive $+_i$ et multiplicative $\times_i$ (ces lois dépendent a priori de i). On vérifie sans difficultés que $\prod_{i\in I} A_i$ est naturellement muni d'une structure d'anneau pour les lois $+$ et $\cdot$ définies pour chaque $(x_i)_{i\in I}, (y_i)_{i\in I} \in \prod_{i\in I} A_i$ par

$$(x_i)_{i\in I} + (y_i)_{i\in I} := (x_i +_i y_i)_{i\in I}$$

et

$$(x_i)_{i\in I} \times (y_i)_{i\in I} := (x_i \times_i y_i)_{i\in I}.$$

En pratique, on s'autorise l'abus de notation (indispensable) en notant toutes les lois additives $+$ et toutes les lois multiplicatives $\times$.

Anneau d'applications

Dans la ligne du transparent précédent, nous voulons ici munir un ensemble d'applications d'une structure d'anneau.

Soient $(A;+,\times)$ un anneau et T un ensemble non vide. On note $\mathscr{F}(T,A)$ (ou A^T) des applications de T dans A.

On vérifie que l'on peut munir $\mathscr{F}(T,A)$ d'une structure d'anneau via les deux lois de composition internes $\oplus,\otimes : \mathscr{F}(T,A)^2 \to A$ définies pour tout $f,g \in \mathscr{F}(T,A)$ par

$$(f \oplus g)(t) := f(t) + g(t),$$

$$(f \otimes g)(t) := f(t) \times g(t).$$

Evidemment, $(\mathscr{F}(T,A);\oplus,\otimes)$ est un anneau commutatif lorsque A est lui-même commutatif.

En pratique, on réalise l'abus de notation usuel en notant $+$ et $\times$ les lois $\oplus$ et $\otimes$.

Elément inversible

A ce stade, la notion d'inversibilité a déjà été rencontrée en théorie des groupes, en calcul matriciel et en théorie des ensembles.

Définition

Soit a un élément d'un anneau A non réduit à zéro.

On dit que a est **inversible à gauche** (resp. **inversible à droite** (resp. **inversible**)) dans A lorsqu'il existe $b \in A$ (resp. $c \in A$ (resp. $d \in A$)) tel que $ba = 1_A$ (resp. $ac = 1_A$ (resp. $ad = da = 1_A$)). Un tel b (resp. c (resp. d)) est appelé un **inverse à gauche** (resp. **inverse à droite** (resp. **inverse**)) de a dans A.

- Si a admet un inverse dans A, alors celui-ci est unique : on le note traditionnellement a^{-1}. L'ensemble des éléments inversibles de A est noté $A^\times$. On montre tout de suite que $A^\times$ est un groupe.

- Soit $a \in A$ admettant un inverse à gauche a_g et un inverse à droite a_d dans A. Alors, a est inversible dans A et $a^{-1} = a_g = a_d$.

- Pour tout $a \in A$ et tout entier $n \geq 1$, on note $a^{-n} := (a^{-1})^n$.

Quelques exemples

- On a $\mathbb{Z}^\times = \{-1, 1\}$, $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{R}^\times = \mathbb{R}^*$ et $\mathbb{C}^\times = \mathbb{C}^*$.
- Soit $n \geq 2$ un entier. On a

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k} : k \in \{0, \ldots, n-1\}, \text{p.g.c.d.}(k, n) = 1\}.$$

- Soit $n \geq 2$ un entier. On a

$$GL_n(\mathbb{Z}) = \{M \in M_n(\mathbb{Z}) : |\det(M)| = 1\}.$$

- On a $\mathbb{Z}[i]^\times = \{-1, 1, -i, i\}$.
- On a $\mathbb{Z}[j]^\times = \{-1, 1, -j, j, -1-j, 1+j\}$.
- Soit A un anneau commutatif intègre. Alors, on a $A[X]^\times = A^\times$, où l'on a identifié les polynômes constants avec les éléments de A.

Corps

Définition

On appelle **corps** (ou **algèbre à division**) tout anneau non nul pour lequel tout élément non nul est inversible. [1]

- Les ensembles $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps commutatifs.
- Pour tout nombre premier p, l'ensemble $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif.
- L'ensemble

$$\mathbb{H} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$$

est un corps non commutatif (appelé corps des quaternions).

[1] Certains auteurs imposent dans la définition de corps la commutativité de la loi multiplicative. Nous ne suivrons pas cette voie.

Elément irréductible d'un anneau

L'inversibilité est au coeur de la notion d'irréductibilité.

Définition

Soient A un anneau **non nul** et $a \in A$. On dit que a est **irréductible** dans A (ou relativement à A) lorsque $a \notin A^\times$ et lorsque pour tout $x, y \in A$,

$$a = xy \Rightarrow x \in A^\times \quad \text{ou} \quad y \in A^\times.$$

- L'élément nul 0_A d'un anneau A n'est jamais irréductible dans A.
- Dans $\mathbb{Z}$, les éléments irréductibles sont exactement les entiers (relatifs) premiers.
- Soit $P = X^2 + 1$. Alors, P est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.
- Soit K un corps commutatif. Les polynômes de degré 1 à coefficients dans K sont irréductibles dans $K[X]$. Un polynôme P de degré 2 à coefficients dans K est irréductible dans $K[X]$ si et seulement si P n'a pas de racines dans K.

Anneau intègre

Les corps bénéficient de la propriété fondamentale énoncée de manière élémentaire sous la forme "un produit est nul si et seulement si l'un des facteurs est nuls".

Définition

Soit $(A;+,\times)$ un anneau. On dit que A est **intègre** lorsque :

(i) A n'est pas réduit à zéro;

(ii) Pour tout $a, b \in A$, on a l'implication

$$ab = 0_A \Rightarrow a = 0_A \quad \text{ou} \quad b = 0_A.$$

- Un corps est un anneau intègre. Plus généralement, un anneau non nul inclus dans un corps est intègre. Par ailleurs, on montre aisément qu'un anneau intègre fini est un corps.
- Les anneaux $\mathbb{Z}$, $K[X]$ avec K corps commutatif sont des anneaux intègres.
- Un produit d'anneaux intègres n'est en général pas intègre.
- Pour tout $n \geq 2$, l'anneau $M_n(\mathbb{R})$ n'est pas intègre.

Diviseur de zéro

La notion d'intégrité est liée à celle de diviseurs de zéros que nous introduisons ci-dessous :

Définition

Soient $(A;+,\times)$ un anneau, $a \in A$ avec $a \neq 0_A$.

On dit que a est un **diviseur de zéro à gauche** (resp. un **diviseur de zéro à droite**) dans A lorsqu'il existe $b \in A$ avec $b \neq 0_A$ tel que $ab = 0_A$ (resp. $ba = 0_A$). Si a est un diviseur de zéro à gauche ou à droite dans A, on dit que a est un **diviseur de zéro** dans A.

- L'élément $M := \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ est un diviseur de zéro à gauche et à droite.

  Attention cependant au fait qu'il n'existe pas $N \in M_2(\mathbb{R})$ **non nulle** telle que $MN = NM = 0$.
- Dans un corps, il n'y a pas de diviseurs de zéros.
- Dans $\mathbb{Z}/6\mathbb{Z}$, la classe $\overline{4}$ est un diviseur de zéro : $\overline{4}.\overline{3} = \overline{0}$.

Elément régulier

Considérons l'équation $\overline{2}x = \overline{6}$ d'inconnue $\mathbb{Z}/10\mathbb{Z}$. Il serait tentant de "simplifier" par $\overline{2}$ pour aboutir à une unique solution $x = \overline{3}$. Toutefois, cet argument ne saurait être correct puisque $\overline{8}$ est également une solution. Ceci conduit à la notion de régularité d'un élément d'un anneau.

Définition

Soit a un élément non nul d'un anneau $(A; +, \times)$. On dit que a est **régulier à gauche** (resp. **régulier à droite**) lorsque pour tout $b, c \in A$,

$$ab = ac \Rightarrow b = c$$

(resp.

$$ba = ca \Rightarrow b = c).$$

On dit que a est **régulier** lorsqu'il est régulier à gauche et à droite.

Un lien entre régularité et diviseurs de zéros

Le résultat ci-dessous relie les notions de régularité et de diviseur de zéro.

Proposition

Soit A un anneau. Les éléments réguliers à gauche (resp. à droite) sont les éléments non nuls qui ne sont pas des diviseurs de zéros à gauche (resp. à droite).

Démonstration. On montre le cas à gauche (le cas à droite étant totalement analogue). Soit $a \in A$. Si a est un diviseur de zéro à gauche, alors $a \neq 0_A$ et il existe $b \in A$ non nul tel que $ab = 0_A$. Si a était régulier à gauche, on aurait $b = 0_A$. Réciproquement, supposons que a ne soit pas un diviseur de zéro à gauche. Soient $b, c \in A$ tels que $ab = ac$. On a alors $a(b - c) = 0_A$ puis $b - c = 0_A$. Ceci confirme que a est régulier à gauche. ■

Elément nilpotent

Si $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, nous savons que pour $x \in A$ avec $x \neq 0$, on a

$$x^n \neq 0_A \quad \text{pour tout } n \geq 1.$$

La situation est différente dans les anneaux de matrices : on a par exemple dans $M_2(\mathbb{R})$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Une telle matrice ci-dessus est traditionnellement qualifié de nilpotente. Nous étendons ce vocabulaire au cadre de n'importe quel anneau.

Définition

Soient A un anneau non nul et $a \in A$. On dit que a est **nilpotent** lorsqu'il existe un entier $n \geq 1$ tel que $a^n = 0_A$.

- Un élément nilpotent n'est jamais inversible.
- L'ensemble des éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$ est donné par l'ensemble des $\overline{k}$ avec $k \in \{0, \ldots, n-1\}$ pour lesquels il existe un entier $r \geq 1$ tel que $n \mid k^r$.

Elément central et centre d'un anneau

La notion de centre a déjà été rencontrée en théorie des groupes.

Définition

Soient A un anneau et $a \in A$. On dit que a est **central** lorsqu'il commute avec tous les éléments de A, i.e., $ab = ba$ pour tout $b \in A$. On appelle **centre** de A l'ensemble des éléments centraux de A et on le note $Z(A)$.

- Soit A un anneau. Alors, A est commutatif si et seulement si $Z(A) = A$.
- On a $Z(\mathbb{H}) = \{a\mathrm{I}_2 : a \in \mathbb{R}\}$.
- Soit K un corps commutatif. Alors, on a $Z(M_n(K)) = \{a\mathrm{I}_n : a \in \mathbb{R}\}$.

Sous-anneau

De manière analogue aux sous-espaces vectoriels ou aux sous-groupes, on définit la notion de sous-anneaux.

Définition

Soit B une partie d'un anneau $(A;+,\times)$. On dit que B est un **sous-anneau** de A si muni des lois induites par A c'est un anneau.

Pour établir qu'une partie est un sous-anneau, il faut donc vérifier les quatre points de la définition des anneaux. En pratique, on préfère utiliser le critère ci-dessous :

Proposition

Soit B une partie d'un anneau $(A;+,\times)$. Alors, B est un sous-anneau de A si et seulement si les trois conditions suivantes ont lieu :

(a) $1_A \in B$;

(b) Pour tout $b_1, b_2 \in B$, on a $b_1 - b_2 \in B$;

(c) Pour tout $b_1, b_2 \in B$, on a $b_1 \cdot b_2 \in B$.

Démonstration. L'implication $\Rightarrow$ est claire. Réciproquement, supposons que $(i), (ii)$ et (iii) ont lieu. Seul le point (i) de la définition d'un anneau mérite d'être établie. Soit $b \in B \neq \emptyset$. On a $b - b = 0_A \in B$ par (ii). Ceci et (ii) entraînent que $(B;+)$ est un sous-groupe de $(A;+)$. ■

Exemples

- L'ensemble $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ est un sous-anneau de $\mathbb{R}$.
- L'ensemble $\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{C}\}$ est un sous-anneau de $\mathbb{C}$.
- L'ensemble $\mathbb{D} := \{\frac{n}{10^k} : n \in \mathbb{Z}, k \in \mathbb{N}\}$ est un sous-anneau de $\mathbb{Q}$.
- L'ensemble des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ est un sous-anneau de $\mathbb{R}^{\mathbb{R}}$.
- L'ensemble $2\mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$.
- L'ensemble

$$\left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbb{R} \right\}$$

n'est pas un sous-anneau de $M_2(\mathbb{R})$ muni de sa structure naturelle d'anneau. Néanmoins, muni de l'addition et de la multiplication matricielle cet ensemble est un anneau (d'élément neutre multiplicatif $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbb{R} \right\}$.

- Le centre d'un anneau est un sous-anneau.

Intersection et sous-anneau engendré par une partie

On montre facilement le résultat suivant :

Proposition

L'intersection d'une famille non vide de sous-anneau d'un anneau A est un sous-anneau de A.

Cette stabilité par intersection va bien entendu donner lieu au concept de sous-anneau engendré par une partie.

Soit S une partie non vide d'un anneau A. On note $\mathscr{F}$ l'ensemble des sous-anneaux de A contenant S qui est un ensemble non vide (puisqu'il contient A). L'ensemble $A[S] := \bigcap_{B \in \mathscr{F}} B$ est évidemment un sous-anneau de A contenant la partie S, i.e., $A[S] \in \mathscr{F}$. Il est appelé **sous-anneau de A engendré par la partie S** et il satisfait l'inclusion $A[S] \subset C$ pour chaque $C \in \mathscr{F}$. On conclut que $A[S]$ est le plus petit (au sens de l'inclusion $\subset$) sous-anneau de A contenant S.

Description explicite du sous-anneau engendré par une partie

Un élément générique du sous-anneau engendré par une partie S n'est nul autre au signe près qu'une somme de produits finis d'éléments de S. Plus précisément :

Proposition

Soient S une partie non vide d'un anneau A et $\mathscr{P}_S$ l'ensemble des éléments de A s'écrivant comme un produit non vide fini d'éléments de S.

On a

$$A[S] := \left\{ \sum_{k=0}^{n} \varepsilon_k p_k : n \in \mathbb{N}, p_0, \ldots, p_n \in \mathscr{P}_S \cup \{1_A\}, \varepsilon_0, \ldots, \varepsilon_n \in \{-1, 0, 1\} \right\}.$$

La démonstration

On note B le second membre de l'égalité donnée par l'énoncé. On a bien sûr $1_A = 1.p_0 \in B$ avec $p_0 = 1_A \in \mathscr{P}_S \cup \{1_A\} =: Q$. D'autre part, il est évident que B est stable par $+$. Concernant la stabilité par la loi $\times$, il suffit de voir que pour $\varepsilon \in \{-1, 0, 1\}$, $n \in \mathbb{N}$ et $p, p_0, \ldots, p_n \in Q$

$$(\varepsilon p) \times \sum_{k=0}^{n} \varepsilon_k p_k = \sum_{k=0}^{n} \varepsilon \varepsilon_k p p_k \in B.$$

Ainsi, B est un sous-anneau de A. Puisque B contient S, il contient le plus petit-sous anneau de A contenant S, i.e., $A[S] \subset B$.

Montrons l'inclusion renversée $B \subset A[S]$. Soit C un sous-anneau de A contenant S. Ce sous-anneau C contient bien sûr l'ensemble $\mathscr{P}_S$ ainsi que les éléments 0_A et 1_A. Il s'ensuit que tout élément de B est un élément de C. On conclut que $B \subset A[S]$. ■

Idéal à gauche, à droite, bilatère

Nous disposons d'une autre classe fondamentale de parties d'un anneau.

Définition

Soit I une partie d'un anneau $(A;+,\cdot)$. On dit que I est un **idéal à gauche** (resp. à **droite**) de A lorsque

(i) $(I;+)$ est un sous-groupe de $(A;+)$;

(ii) Pour tout $i \in I$, pour tout $a \in A$, $ai \in I$ (resp. $ia \in I$).

Lorsque I est à la fois un idéal à gauche et à droite de A, on dit que I est un idéal **bilatère** de A.

- Les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.
- Soit K un corps commutatif. Les idéaux de $\mathbb{K}[X]$ sont exactement les $PK[X]$ avec $P \in K[X]$.
- Soient A un anneau et $a \in A$. L'ensemble $Aa := \{xa : x \in A\}$ (resp. $aA := \{ax : x \in A\}$ est un idéal à gauche (resp. à droite) de A. L'ensemble $AaA := \left\{\sum_{k=0}^{n} a_k a a'_k : n \in \mathbb{N}, a_0, \ldots, a_n, a'_0, \ldots, a'_n \in A\right\}$ est un idéal bilatère de A. Lorsque A est commutatif, ces trois idéaux coïncident.

Idéaux et intersection

On montre aisément que la notion d'idéal est stable par intersection quelconque :

Proposition

L'intersection d'une famille non vide d'idéaux à gauche (resp. à droite (resp. bilatère)) d'un anneau est un idéal à gauche (resp. à droite (resp. bilatère)).

Soit S une partie non vide d'un anneau A. On note $\mathscr{G}$ (resp. $\mathscr{D}$ (resp. $\mathscr{B}$)) l'ensemble des idéaux à gauche (resp. à droite (resp. bilatère)) de A contenant S (c'est un ensemble non vide puisqu'il contient A). On a évidemment

$$(S)_g := \bigcap_{I \in \mathscr{G}} I \in \mathscr{G}, \quad (S)_d := \bigcap_{I \in \mathscr{D}} I \in \mathscr{D} \quad \text{et} \quad (S) := \bigcap_{I \in \mathscr{B}} I \in \mathscr{B}.$$

L'idéal $(S)_g$ (resp. $(S)_d$ (resp. (S))) est appelé **idéal à gauche** (resp. **idéal à droite** (resp. **idéal bilatère**)) de A **engendré par la partie** S**.** C'est le plus petit (au sens de l'inclusion $\subset$) idéal à gauche (resp. à droite (resp. bilatère)) de A contenant S.

On a toujours

$$(S_g) \cup (S_d) \subset (S).$$

Si de plus A est commutatif, les trois idéaux ci-dessus coïncident, i.e.,

$$(S)_g = (S)_d = (S).$$

Expression des idéaux engendrés

On dispose d'une expression explicite pour les idéaux engendrés par une partie.

Proposition

Soit S une partie non vide d'un anneau A. On a :

$$(S)_g := \left\{ \sum_{k=0}^{n} a_k s_k : n \in \mathbb{N}, a_0, \ldots, a_n \in A, s_0, \ldots, s_n \in S \right\},$$

$$(S)_d := \left\{ \sum_{k=0}^{n} s_k a_k : n \in \mathbb{N}, a_0, \ldots, a_n \in A, s_0, \ldots, s_n \in S \right\},$$

et

$$(S) := \left\{ \sum_{k=0}^{n} a_k s_k a'_k : n \in \mathbb{N}, a_0, \ldots, a_n, a'_0, \ldots, a'_n \in A, s_0, \ldots, s_n \in S \right\}.$$

La démonstration

On se contente de montrer le cas à gauche (i.e., la première égalité énoncée) les cas à droite et bilatère étant analogues.

On note $E := \{\sum_{k=0}^{n} a_k s_k : n \in \mathbb{N}, a_0, \ldots, a_n \in A, s_0, \ldots, s_n \in S\}$. Cet ensemble est évidemment un idéal à gauche de A qui contient S. Il s'ensuit que $(S)_g$ (qui est le plus petit idéal à gauche de A qui contient S) est inclus dans E, i.e., $(S)_g \subset E$.

Montrons l'inclusion renversée. Soit $x \in E$. Il existe $m \in \mathbb{N}$, $\alpha_0, \ldots, \alpha_m \in A$ et $\zeta_0, \ldots, \zeta_m \in S$ tels que $x = \sum_{k=0}^{m} \alpha_k \zeta_k$. Fixons I un idéal à gauche de A contenant S. Pour tout $k \in \{0, \ldots, m\}$, on a $\zeta_k \in S \subset I$ et donc $\alpha_k \zeta_k \in I$. Ceci et le fait que $(I; +)$ soit un groupe nous dit que $\sum_{k=0}^{m} \alpha_k \zeta_k \in I$. Ainsi, x appartient à tous les idéaux à gauche de A contenant S, i.e., $x \in (S)_g$. On conclut que $(S)_g = E$ comme annoncé. ■

Idéal principal

Soit a un élément d'un anneau A.

On a déjà vu que l'ensemble $Aa := \{xa : x \in A\}$ (resp. $aA := \{ax : x \in A\}$ (resp. $AaA := \left\{\sum_{k=0}^{n} a_k a a'_k : n \in \mathbb{N}, a_0, \ldots, a_n, a'_0, \ldots, a'_n \in A\right\}$)) est un idéal à gauche (resp. à droite (resp. bilatère)) de A. D'après ce qui précède, cet idéal n'est nul autre que l'idéal à gauche (resp. à droite (resp. bilatère)) engendré par la partie $\{a\}$, i.e., $Aa = (\{a\})_g$ (resp. $aA = (\{a\})_d$ (resp. $AaA = (\{a\})$)).

Définition

L'idéal à gauche Aa (resp. à droite aA (resp. bilatère AaA)) de A est appelé idéal **principal à gauche** (resp. **à droite** (resp. **bilatère**)) **de** A **engendré par** a. On le note $(a)_g$ (resp. $(a)_d$ (resp. (a)).

Etant donné un idéal I de A, on dit que I est **principal à gauche** (resp. à **droite** (resp. **bilatère**)) s'il existe $x \in A$ tels que $I = (x)_g$ (resp. $I = (x)_d$ (resp. $I = (x)$)).

Idéal de type fini

Soient n éléments $a_0, \ldots, a_n$ d'un anneau A avec $n \in \mathbb{N}$.

De manière analogue aux idéaux principaux, on note $(a_0, \ldots, a_n)_g$ en lieu et place de $(\{a_0, \ldots, a_n\})_g$ l'idéal à gauche de A engendré par la partie $\{a_0, \ldots, a_n\}$. On procède de même pour le cas à droite et bilatère.

Définition

Soit I un idéal de A. On dit que I est **de type fini à gauche** (resp. à **droite** (resp. **bilatère**)) s'il existe $m \in \mathbb{N}$, $x_0, \ldots, x_m \in A$ tels que $I = (x_0, \ldots, x_m)_g$ (resp. $I = (x_0, \ldots, x_m)_d$ (resp. $I = (x_0, \ldots, x_m)$)).

Anneau principal - anneau noethérien

Nous introduisons maintenant deux classes fondamentales d'anneaux.

Définition

Soit A un anneau commutatif. On dit que A est **principal** s'il est intègre et si tous ses idéaux sont principaux. On dit que A est **noethérien** [2] si tous ses idéaux sont de type finis.

- On peut définir les notions d'anneaux principaux/noethérien à gauche et à droite de manière analogue. Nous n'en aurons toutefois pas l'usage.
- Tout anneau principal est noethérien (mais la réciproque est fausse).
- Soit A un anneau commutatif. Alors, l'anneau $A[X]$ est principal si et seulement si A est un corps. En particulier, $\mathbb{Q}[X], \mathbb{R}[X]$ et $\mathbb{C}[X]$ sont principaux et $\mathbb{Z}[X]$ n'est pas principal.
- L'anneau $\mathbb{Z}$ est principal.
- L'anneau $\mathbb{Z}[X]$ est noetherien. Plus généralement, nous verrons que $A[X]$ est noetherien lorsque A est un anneau commutatif noetherien.

[2] En hommage à la mathématicienne Emmy Noether (1882-1935).

Une caractérisation des anneaux noethériens

Nous donnons ici une caractérisation de la notion d'anneaux noethériens à travers des suites d'idéaux. Le résultat ci-dessous est souvent utilisé pour produire une définition alternative (et équivalente) du concept d'anneau noethérien.

Proposition

Soit A un anneau commutatif. Alors, A est noethérien si et seulement si toute suite croissante (pour l'inclusion $\subset$) d'idéaux est stationnaire.

Démonstration. $\Rightarrow$, Découle du fait que $\bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A si $(I_n)_{n\in\mathbb{N}}$ est une suite croissante d'idéaux de A.
$\Leftarrow$, Si A n'est pas noethérien, alors on peut trouver un idéal J de A qui n'est pas de type fini. On peut alors facilement construire une suite croissante $(I_n)_{n\in\mathbb{N}}$ d'idéaux (inclus dans J) de A qui n'est pas stationnaire. ■

Somme d'idéaux

On a vu précédemment que les idéaux sont stables à travers l'opération ensembliste "d'intersection". On poursuit ici l'étude des opérations sur les idéaux.

Soient A un anneau et I, J deux idéaux de A de même nature (i.e., deux idéaux à gauche (resp. à droite (resp. bilatères)) d'un anneau A.

On vérifie sans difficultés que l'ensemble

$$I + J := \{i + j : (i, j) \in I \times J\}$$

est un idéal à gauche (resp. à droite (resp. bilatère)) de A, appelé **idéal somme** de I et J à gauche (resp. à droite (resp. bilatère)).

De plus, on peut montrer que $I + J$ n'est nul autre que l'idéal à gauche (resp. à droite (resp. bilatère)) engendré par la partie $I \cup J$ de A, i.e.,

$$I + J = \left(I \cup J\right)_g \quad \left(\text{resp. } I + J = \left(I \cup J\right)_d \quad \left(\text{resp.} I + J = \left(I \cup J\right)_b\right)\right).$$

Produits d'idéaux

Soient I, J deux parties non vides d'un anneau A.

En général, l'ensemble $\mathscr{P} := \{ij : i \in I, j \in J\}$ n'est pas un idéal de A et ceci même si I et J sont des idéaux de A (considérer par exemple les idéaux de l'anneau commutatif $\mathbb{Z}[X]$: $I = (2, X)$ et $J = (3, X)$).

On définit **l'idéal produit à gauche** (resp. **à droite** (resp. **bilatère**)) de I et J noté IJ par

$$(IJ)_g := (\mathscr{P})_g, \quad (\text{resp. } (IJ)_d := (\mathscr{P})_d \quad (\text{resp. } IJ := (\mathscr{P}))).$$

Ces idéaux ont bien sûr une description explicite (comme tout idéal engendré par une partie). On notera le cas le plus important : si I et J sont deux idéaux bilatères de A, on a

$$IJ = \left\{ \sum_{k=0}^{m} i_k j_k : m \in \mathbb{N}, \forall 0 \leq k \leq m, (i_k, j_k) \in I \times J \right\}.$$

Radical d'un idéal

Nous poursuivons notre étude des opérations sur les idéaux.

Définition

Soit I un idéal d'un anneau A. On appelle **radical de l'idéal** I l'ensemble noté $\sqrt{I}$ défini par

$$\sqrt{I} = \{a \in A : \exists n \geq 1, a^n \in I\}.$$

On dit que **l'idéal** I **est radical** lorsque $I = \sqrt{I}$.

- Le radical $\sqrt{I}$ vérifie toujours l'inclusion $I \subset \sqrt{I}$.
- Avec l'idéal nul $I = \{0_A\}$, on voit tout de suite que $\mathrm{nil}(A) = \sqrt{\{0_A\}}$.
- Avec $A = \mathbb{Z}$, alors pour chaque $r \geq 1$, $p_1, \ldots, p_r \in \mathbb{P}$ et chaque $\alpha_1, \ldots, \alpha_r \geq 1$, on a
$$\sqrt{p_1^{\alpha_1} \ldots p_r^{\alpha_r} \mathbb{Z}} = p_1 \ldots p_r \mathbb{Z}.$$
- Soit I un idéal d'un anneau commutatif A. Alors, $\sqrt{I}$ est un idéal de A.

Morphisme d'anneaux

A ce stade, nous estimons le lecteur familier avec la notion de morphismes d'espaces vectoriels (mieux connus sous le nom d'applications linéaires) et de morphismes de groupes.

Définition

Soit $f : A \to B$ une application entre deux anneaux A et B. On dit que f est un **morphisme d'anneaux** (entre A et B) lorsque pour chaque $a, b \in A$,

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)(fb) \quad \text{et} \quad f(1_A) = 1_B.$$

Un morphisme d'anneaux d'un anneau dans lui-même est appelé un **endomorphisme d'anneaux**. Un morphisme d'anneaux bijectif est dit être un **isomorphisme d'anneaux**. Un endomorphisme bijectif d'anneaux est appelé **automorphisme d'anneaux**.

Remarque. Dans la littérature, on trouve parfois le terme de *morphisme d'anneaux unitaires* pour désigner ce type d'applications. Nous n'emploierons pas ce terme puisque nous développons (comme c'est désormais l'usage) la théorie des anneaux unitaires (i.e., avec existence d'un neutre multiplicatif).

Quelques exemples

Soit A un anneau.

- Si B est un sous-anneau de A, alors l'application $i : B \to A$ définie par

$$i(x) := x \quad \text{pour tout } x \in B$$

est un morphisme d'anneaux injectif.

- L'identité $\mathrm{Id}_{\mathbb{R}}$ est le seul endomorphisme d'anneaux de $\mathbb{R}$.
- La conjugaison complexe induit un automorphisme de l'anneau $\mathbb{C}$.
- Soient A un anneau, T un ensemble non vide et $t \in T$. L'application $\mathrm{ev}_t : \mathscr{F}(T; A) \to T$ définie par

$$\mathrm{ev}_t(f) := f(t) \quad \text{pour tout } f \in \mathscr{F}(T; A)$$

est un morphisme d'anneaux, appelé **morphisme d'évaluation** en t.

Quelques exemples - suite et fin

- Soient I un ensemble non vide, $(A_i)_{i\in I}$ une famille d'anneaux. Pour chaque $j \in J$, l'application $p_j : \prod_{i\in I} A_i \to A_j$ définie par

$$p_j\big((x_i)_{i\in I}\big) := x_j \quad \text{pour tout}\,(x_i)_i \in I \in \prod_{i\in I} A_i$$

est un morphisme d'anneaux.

- Etant donnés deux anneaux, il n'existe pas toujours de morphisme d'anneaux entre deux anneaux donnés ! A titre d'exemple, il n'existe pas de morphisme d'anneaux de $\mathbb{C}$ dans $\mathbb{R}$.

Premières propriétés des morphismes d'anneaux

La proposition suivante donne les premières propriétés des morphismes d'anneaux.

Proposition

Soient A, B deux anneaux et $f : A \to B$ un morphisme d'anneaux. Ont lieu :

(a) $f(0_A) = 0_B$ et $f(-x) = -f(x)$ pour tout $x \in A$;

(b) $\ker(f)$ est un idéal bilatère de A et $\mathrm{im}(f)$ est un sous-anneau de B.

(c) Si J est un idéal à gauche (resp. à droite (resp. bilatère)) de B, alors $f^{-1}(J)$ est un idéal à gauche (resp. à droite (resp. bilatère)) de A;

(d) Si I est un idéal à gauche (resp. à droite (resp. bilatère)) de A, alors $f(I)$ est un idéal à gauche (resp. à droite (resp. bilatère)) du sous-anneau $\mathrm{im}(f)$;

(e) f est injective si et seulement si $\ker(f) = \{0_A\}$.

(f) Si A est non nul, alors on a $f(A^\times) \subset B^\times$ et $f(a^{-1}) = f(a)^{-1}$ pour tout $a \in A^\times$.

(g) Si A et B sont des corps, alors f est injective.

(h) Si f est bijective, alors $f^{-1} : B \to A$ est un morphisme d'anneaux.

(i) Si C est un anneau et $g : B \to C$ est un morphisme d'anneaux, alors $g \circ f : A \to C$ est un morphisme d'anneaux.

Commentaires

- Seule (g) mérite une justification. Supposons que A et B soient des corps et fixons $a \in \ker(f)$. Supposons que $a \neq 0_A$. Dans ce cas, a est inversible dans A et son image $f(a)$ est inversible dans B d'après l'assertion (f). Ceci entraîne que $f(a) \neq 0_A$, i.e., $a \notin \ker(f)$. Ainsi, on a nécessairement $a = 0_A$ et on peut conclure grâce à (e).

- En général, $\mathrm{im}(f)$ n'est pas un idéal de B. L'ensemble $\mathrm{im}(f)$ contenant toujours 1_B, il est un idéal si et seulement si f est surjective, i.e., $\mathrm{im}(f) = B$.

- En général, $f(I)$ n'est pas un idéal de $\mathrm{im}(f)$ pour I un idéal de A. Pour le voir, on peut prendre $A = \mathbb{Z}$, $B = \mathbb{Z}[X]$, $I = 2\mathbb{Z}$ et $f : \mathbb{Z} \to A$ l'injection canonique.

Quotienter par un idéal

Nous allons nous intéresser ici à la notion d'anneau quotient. A ce stade, le lecteur est déjà familier avec $\mathbb{Z}/n\mathbb{Z}$, les groupes quotients ainsi que les espaces vectoriels quotients.

Soit I un idéal bilatère d'un anneau $(A;+,\times)$ (**pas nécessairement commutatif**). On considère la relation $\mathscr{R}$ binaire sur A définie par

$$x\mathscr{R}y \Leftrightarrow x-y\in I \quad \text{pour tout}\, x,y\in A.$$

On vérifie sans peine que $\mathscr{R}$ est une relation d'équivalence sur A. L'ensemble quotient $A/\mathscr{R}$ est en général noté A/I. On note $\pi_{A,I}: A\to A/I$ l'application canonique (évidemment surjective) de A dans A/I, c'est-à-dire celle qui à un élément $a\in A$ associe sa classe d'équivalence (pour la relation $\mathscr{R}$). S'il n'y a pas d'ambiguïtés, on pourra noter π_A en lieu et place de $\pi_{A,I}$.

Pour chaque $x\in A$, $\pi_A(x)$ désigne donc la classe d'équivalence de x relativement à $\mathscr{R}$: on la note $\overline{x}$, $[x]$ ou encore $\mathrm{cl}(x)$. Observons que pour tout $x\in A$, on a

$$\boxed{\overline{x} := \{y\in A : x-y\in I\} = \{y\in A : y-x\in I\} = x+I.}$$

Munir le quotient d'une structure d'anneau

Nous allons maintenant munir A/I d'une structure d'anneau quotient.

Soient $a_1, a_2, b_1, b_2 \in A$ avec $\overline{a_1} = \overline{a_2}$ et $\overline{b_1} = \overline{b_2}$. On a $i_1 := a_1 - a_2 \in I$ et $i_2 := b_1 - b_2 \in I$ puis

$$a_1 + b_1 = a_2 + b_2 + i_1 + i_2 \quad \text{et} \quad a_1 b_1 = (a_2 + i_1)(b_2 + i_2) = a_2 b_2 + a_2 i_2 + i_1 b_2 + i_1 i_2.$$

Ces égalités et le fait que I soit un idéal bilatère de A entraînent facilement

$$\overline{a_1 + b_1} = \overline{a_2 + b_2} \quad \text{et} \quad \overline{a_1 b_1} = \overline{a_2 b_2}.$$

Ces deux égalités sont souvent résumées à travers l'expression "la relation $\mathscr{R}$ est **compatible** avec les lois $+$ et $\times$". Ceci permet de définir les applications $s, p : (A/I)^2 \to A/I$ via les égalités

$$s(\overline{a}, \overline{b}) := \overline{a+b} \quad \text{et} \quad p(\overline{a}, \overline{b}) := \overline{ab} \quad \text{pour tout } a, b \in A.$$

Il découle des propriétés de l'anneau $(A; +, \times)$ que A/I muni des lois de composition interne s (addition) et p (multiplication) est un anneau (commutatif si A l'est) dont les éléments neutres respectifs sont $\overline{0_A} = 0_{A/I} = I$ et $\overline{1_A} = 1_{A/I}$. De plus, on tire directement des définitions de s et de p que l'application $\pi_{A,I} : A \to A/I$ est un morphisme d'anneaux (surjectif).

Peut-on quotienter autrement ?

On pourrait s'arrêter ici en disant que tout anneau A quotienté par un idéal bilatère I sera désormais muni des deux lois précédentes s et p qui font de la projection canonique $\pi_{A,I}$ un morphisme d'anneaux de noyau I.

Nous allons aller un peu plus loin en nous demandant s'il est possible de construire d'autres structures d'anneaux quotient bénéficiant de la compatibilité additive et multiplicative vues précédemment.

Soit $(A;+,\times)$ un anneau et $\mathscr{R}$ une relation d'équivalence sur A, compatible avec les lois $+$ et $\cdot$, i.e., pour tout $a_1, a_2, b_1, b_2 \in A$ avec $a_1 \mathscr{R} a_2$ et $b_1 \mathscr{R} b_2$,

$$(a_1 + b_1)\mathscr{R}(a_2 + b_2) \quad \text{et} \quad (a_1 b_1)\mathscr{R}(a_2 b_2).$$

Les égalités ci-dessus permettent bien sûr de munir $A/\mathscr{R}$ d'une structure d'anneau faisant de la projection canonique $q : A \to A/\mathscr{R}$ un morphisme d'anneaux. Son noyau $I := \ker(q)$ est donc un idéal bilatère de A. Il reste à voir que

$$x\mathscr{R}y \Leftrightarrow (x-y)\mathscr{R}0_A \Leftrightarrow x - y \in \ker(q) = I$$

pour conclure que $A/\mathscr{R}$ n'est nul autre que A/I et $q = \pi_{A,I}$.

Vers la propriété universelle du quotient

Soient A, B deux anneaux, I un idéal bilatère de A et $\varphi : A/I \to B$ un morphisme d'anneaux. Ces données peuvent se synthétiser selon le diagramme suivant :

$$\begin{tikzcd} A \arrow[r, "\varphi\circ\pi_A"] \arrow[d, "\pi_A"'] & B \\ A/I \arrow[ur, "\varphi"'] & \end{tikzcd}$$

L'application $f := \varphi \circ \pi_A$ est un morphisme d'anneaux par composition de deux morphismes d'anneaux. Par ailleurs, on a $I \subset \ker(f)$ puisque pour tout $x \in I$,

$$f(x) = \big(\varphi \circ \pi_A\big)(x) = \varphi\big(\pi_A(x)\big) = \varphi(0_{A/I}) = 0_B.$$

Question. La donnée d'un morphisme d'anneaux $f : A \to B$ vérifiant $I \subset \ker(f)$ induit-elle l'existence d'un morphisme d'anneaux de A/I dans B ?

Passage au quotient

La réponse est "oui" et le morphisme obtenu est en fait unique. Ce fait est connu sous le nom de *propriété universelle du quotient*. Ce résultat n'est pas propre à la théorie des anneaux mais se retrouve dans de nombreux contextes : espaces vectoriels, groupes, modules, etc.

Théorème

Soient $f : A \to B$ un morphisme d'anneaux entre deux anneaux A et B, I un idéal bilatère de A avec $I \subset \ker(f)$. Alors, il existe un unique morphisme d'anneaux $\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ \pi_A$.

Il est commode de traduire ce théorème sous la forme d'un diagramme :

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi_A"'] & B \\ A/I \arrow[ur, dotted, "\overline{f}"'] & \end{tikzcd}$$

La démonstration

Existence. Soient $a_1, a_2 \in A$ tels que $\pi_A(a_1) = \pi_A(a_2)$. On a donc $a_1 - a_2 \in I$. Puisque $I \subset \ker(f)$, on a $f(a_1 - a_2) = 0_B$ ou encore (car f est un morphisme d'anneaux) $f(a_1) = f(a_2)$. On peut donc considérer l'application $\overline{f} : A/I \to B$ définie par

$$\overline{f}\big(\pi_A(a)\big) = f(a) \quad \text{pour tout } a \in A.$$

Nous allons établir que $\overline{f}$ est un morphisme d'anneaux. On a évidemment $\overline{f}(1_{A/I}) = 1_B$. Soient $x, y \in A/I$. Il existe $a, b \in A$ tels que $x = \pi_A(a)$ et $y = \pi_A(b)$. En utilisant le fait que π_A et f est un morphisme d'anneaux, on peut écrire

$$\overline{f}(x+y) = \overline{f}\big(\pi_A(a) + \pi_A(b)\big) = \overline{f}(\pi_A(a+b)) = f(a+b) = f(a) + f(b) = \overline{f}(x) + \overline{f}(y).$$

De même, on a $f(xy) = f(x)f(y)$.

Unicité. Soit $\widehat{f} : A/I \to B$ une application vérifiant $\widehat{f} \circ \pi_A = f$. Soit $x \in A/I$. La surjectivité de π_A nous permet de trouver $a \in A$ tel que $\pi_A(a) = x$. Il vient alors

$$\widehat{f}(x) = \big(\widehat{f} \circ \pi_A\big)(a) = f(a) = \big(\overline{f} \circ \pi_A\big)(a) = \overline{f}(x).$$

■

Un problème "universel"

Nous allons voir que l'anneau quotient est l'unique solution (en un sens à préciser) d'un problème "universel".

Etant donné un idéal bilatère I d'un anneau A, on considère le problème :

$(\mathscr{P})$: Déterminer un anneau U et un morphisme d'anneaux $u : A \to U$ surjectif avec $I \subset \ker(u)$ tel que pour tout anneau B et tout morphisme d'anneaux $f : A \to B$ avec $I \subset \ker(f)$, il existe un unique morphisme d'anneaux $g : U \to B$ satisfaisant $f = h \circ u$, i.e., faisant commuter le diagramme

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "u"'] & B \\ U \arrow[ur, dotted, "g"'] & \end{tikzcd}$$

On a vu précédemment que $(A/I, \pi_A)$ est une solution au problème $(\mathscr{P})$.

Proposition

Soit (U, u) une solution du problème $(\mathscr{P})$. Alors, il existe un unique isomorphisme d'anneaux $\varphi : A/I \to U$ tel que $u = \varphi \circ \pi_A$.

La démonstration

En exploitant le fait que A/I satisfait la propriété universelle du quotient et le fait que (U, u) soit solution de $(\mathscr{P})$, on obtient deux applications $\varphi : A/I \to U$ et $\psi : U \to A/I$ faisant respectivement commuter les diagrammes

$$\begin{tikzcd} A \arrow[r, "u"] \arrow[d, "\pi_A"'] & U \\ A/I \arrow[ur, dotted, "\varphi"'] & \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "\pi_A"] \arrow[d, "u"'] & A/I \\ U \arrow[ur, dotted, "\psi"'] & \end{tikzcd}$$

Puisque $u = \varphi \circ \pi_A$ et $\pi_A = \psi \circ u$, il vient

$$\pi_A(x) = (\psi \circ \varphi)\big(\pi_A(x)\big) \quad \text{pour tout } x \in A.$$

Ceci et la surjectivité de π_A entraîne que $\psi \circ \varphi = \mathrm{Id}_{A/I}$. De même, l'égalité $u = \varphi \circ \psi \circ u$ et la surjectivité de u donnent $\varphi \circ \psi = \mathrm{Id}_U$. La propriété d'existence voulue est donc établie. L'unicité découle de l'unicité fournie par la propriété universelle satisfaite par A/I. Ceci termine la démonstration. ■

1er théorème d'isomorphisme

Nous donnons à présent trois résultats connus sous le nom de 1er, 2ème et 3ème théorème d'isomorphisme en théorie des anneaux.

Théorème (noyau-image)

Soit $f : A \to B$ un morphisme d'anneaux entre deux anneaux A et B. Alors, $A/\ker(f)$ est isomorphe à $\mathrm{im}(f)$.

Démonstration. On applique le théorème de passage au quotient avec $g = f^{|\mathrm{im}(f)}$ (qui est un morphisme d'anneaux surjectif) et $I = \ker(g) = \ker(f)$. Il existe (un unique) morphisme d'anneaux $\overline{g} : A/\ker(f) \to \mathrm{im}(f)$ tel que $g = \overline{g} \circ \pi_A$ où $\pi_A : A \to A/\ker(f)$ est la projection canonique. L'application $\overline{g}$ est surjective puisque pour $y \in \mathrm{im}(f)$, il existe $a \in A$ tel que

$$y = g(a) = (\overline{g} \circ \pi_A)(a) = \overline{g}(\pi_A(a)).$$

L'application $\overline{g}$ est injective : pour $\overline{x} \in \ker(\overline{g})$, on peut écrire $\overline{x} = \pi_A(b)$ pour un $b \in A$ d'où

$$0_A = \overline{g}(\overline{x}) = (\overline{g} \circ \pi_A)(b) = g(b),$$

i.e., $b \in \ker(g)$ ou encore $\overline{x} = 0_{A/I}$. La démonstration est terminée. ■

2ème théorème d'isomorphisme

On poursuit avec le deuxième théorème d'isomorphisme. Il convient de noter qu'il s'obtient comme conséquence assez directe du premier.

Théorème

Soient A un anneau, I un idéal bilatère de A, B un sous-anneau de A. Ont lieu :

(a) $B+I$ est un sous-anneau de A.

(b) I (resp. $B \cap I$) est un idéal bilatère de $B+I$ (resp. de B).

(c) Les anneaux $(B+I)/I$ et $B/B \cap I$ sont isomorphes.

La démonstration

Les assertions (a) et (b) ne posent aucune difficulté et sont laissées au lecteur.

Nous allons établir (c). Remarquons que (a) et (b) nous assurent que $(B+I)/I$ et $B/B\cap I$ sont des anneaux quotients. On note $\pi : B+I \to (B+I)/I$ la projection canonique de l'anneau $B+I$ sur l'anneau quotient $(B+I)/I$. On note i l'injection canonique de B dans $B+I$. Il est clair que $\varphi = \pi \circ i : B \to (B+I)/I$ est un morphisme d'anneaux. D'après le premier théorème d'isomorphisme, nous savons que les anneaux $B/\ker(\varphi)$ et $\mathrm{im}(\varphi)$ sont isomorphes. Nous allons maintenant montrer que $\mathrm{im}(\varphi) = (B+I)/I$ (i.e., φ est surjective) et $\ker(\varphi) = B\cap I$. Pour le premier point, il suffit de remarquer que pour chaque $x \in (B+I)/I$, on peut écrire pour un certain $(b,i) \in B\times I$

$$x = \pi(b+i) = \pi(b+0_A) + \pi(0_A+i) = \pi\circ i(b) = \varphi(b).$$

Le deuxième point résulte quant à lui du fait que pour chaque $b \in B$,

$$\varphi(b) = 0_{(B+I)/I} \Leftrightarrow \pi(b+0_A) = 0_{(B+I)/I} \Leftrightarrow b \in I.$$

■

3ème théorème d'isomorphisme

Voici enfin le troisième théorème d'isomorphisme.

Théorème

Soient A un anneau, I et J deux idéaux bilatères de A avec $J \supset I$. Alors, les anneaux $(A/I)/\pi_A(J)$ et A/J sont isomorphes, où π_A désigne la projection canonique de A sur A/I.

Remarque. En notant $\pi_A(J) = J/I$ (attention aux confusions : J/I **n'est pas** un anneau quotient en général !) on trouve souvent ce résultat écrit sous forme condensée

$$(A/I)/(J/I) \simeq A/J.$$

Démonstration. L'ensemble $J/I := \pi_A(J)$ est un idéal bilatère de $B := A/I$. Notons $\pi_B : B \to B/(J/I)$ la surjection canonique. L'application $f := \pi_B \circ \pi_A$ est évidemment un morphisme d'anneaux surjectif. Par ailleurs, l'inclusion $I \subset J$ entraîne sans difficultés que $\ker(f) = J$. Il reste à invoquer le 1er théorème d'isomorphisme pour conclure que $\ker(f) = A/J$ est isomorphe à $\mathrm{im}(f) = B/(J/I)$. ■

Description des idéaux d'un anneau quotient

Le résultat suivant permet de décrire l'ensemble des idéaux bilatères d'un anneau quotient A/I. Notons qu'il s'étend facilement au cas des idéaux à gauche ou à droite de A/I.

Proposition

Soit I un idéal bilatère d'un anneau A. On note B l'ensemble des idéaux bilatères de A contenant I et $\mathscr{B}$ l'ensemble des idéaux bilatères de A/I.

Alors, l'application $\varphi : B \to \mathscr{B}$ définie par

$$\varphi(J) = \pi_A(J) \quad \text{pour tout } J \in B$$

est bijective.

Démonstration. L'application φ est bien définie car $\mathrm{im}(\pi_A) = A/I$. L'injectivité de φ s'obtient comme conséquence directe de la définition de B. La surjectivité de φ découle de l'égalité

$$\mathscr{J} = \pi_A\left(\pi_A^{-1}(\mathscr{J})\right)$$

valide pour tout idéal bilatère $\mathscr{J}$ de A/I. ■

Remarque. Bien sûr, l'application φ n'est pas un isomorphisme d'anneaux (ce n'est même pas un morphisme d'anneaux !).

Introduction à la caractéristique d'un anneau

Avant de poursuivre avec le développement des restes chinois (un autre théorème d'isomorphisme !) arrêtons-nous un instant sur le concept de caractéristique d'un anneau.

Etant donnés un anneau $(A; +, \times)$ et un élément $a \in A$ avec $a \neq 0_A$, deux (et seulement deux) situations peuvent se produire :

1. Pour tout $k \geq 1$, on a $ka \neq 0_A$. C'est le cas dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ou encore dans des anneaux de matrices.
2. Il existe un entier $k \geq 1$ tel que $ka = 0_A$. C'est le cas si $A = \mathbb{Z}/n\mathbb{Z}$ pour un certain entier $n \geq 2$ car alors $na = 0_A$.

Ces deux situations distinctes vont nous amener naturellement au concept de caractéristique d'un anneau.

Caractéristique d'un anneau - Sous-anneau premier

Soit $(A;+,\times)$ un anneau. Il n'est pas difficile de voir que l'application $\varphi_A : \mathbb{Z} \to A$ définie par

$$\varphi_A(k) = k1_A \quad \text{pour tout } k \in \mathbb{Z}$$

est un morphisme d'anneaux. On vérifie que c'est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A. Son image $\mathrm{im}\varphi_A$ est un sous-anneau de A.

Puisque $\ker(\varphi_A)$ est un idéal de l'anneau $(\mathbb{Z};+,\times)$, nous savons qu'il s'écrit pour un unique $n_A \in \mathbb{N}$

$$\ker(\varphi_A) = n_A\mathbb{Z}.$$

Par le 1er théorème d'isomorphisme, nous savons que $\mathbb{Z}/n_A\mathbb{Z}$ est isomorphe à $\mathrm{im}\,\varphi_A$. Notons que si $n_A = 0$, alors $\mathbb{Z}$ est lui-même isomorphe à $\mathrm{im}\,\varphi_A$.

Définition

L'entier naturel n_A est appelé **caractéristique de l'anneau** A et est noté $\mathrm{car}(A)$. Le sous-anneau $\mathrm{im}\varphi_A = \{k1_A : k \in \mathbb{Z}\}$ est appelé **sous-anneau premier** de A.

Premières propriétés de la caractéristique

On donne ici les premières propriétés de la caractéristique.

Proposition

Soit A un anneau. Ont lieu :

(a) Pour tout $a \in A$, on a $\mathrm{car}(A)a = 0_A$.

(b) Soit B un sous-anneau de A. Alors, $\mathrm{car}(A) = \mathrm{car}(B)$.

(c) La caractéristique d'un anneau intègre est soit nulle soit un nombre premier.

(d) Soient B un anneau et $f : A \to B$ un morphisme d'anneaux. Alors, $\mathrm{car}(B) \mid \mathrm{car}(A)$.

(e) Il n'existe pas de morphisme de corps entre deux corps de caractéristiques distinctes.

La démonstration

Pour un anneau C, $\varphi_C : \mathbb{Z} \to A$ désigne l'unique morphisme d'anneaux entre $\mathbb{Z}$ et C (vu précédemment).

(a) Soit $a \in A$. Par définition, on a

$$\mathrm{car}(A)\mathbb{Z} = \ker(\varphi_A) = \{n \in \mathbb{Z} : n1_A = 0_A\},$$

en particulier $\mathrm{car}(A)1_A = 0_A$.

(b) Il est clair que restriction au but $\varphi_A^{|B}$ de φ_A coïncide avec le morphisme d'anneaux φ_B, en particulier

$$\mathrm{car}(A)\mathbb{Z} = \ker(\varphi_A^{|B}) = \ker(\varphi_B) = \mathrm{car}(B)\mathbb{Z}.$$

On conclut que $\mathrm{car}(A) = \mathrm{car}(B)$.

(c) Supposons que $\mathrm{car}(A) \neq 0$. Posons $n = \mathrm{car}(A)$ qui est le plus petit entier strictement positif tel que $n1_A = 0_A$. Supposons également qu'il existe deux entiers positifs k et l tels que $n = kl$. En écrivant $(k1_A)(l1_A) = 0_A$ et en exploitant l'intégrité de A, on obtient $k1_A = 0_A$ ou $l1_A = 0_A$ puis $k = n$ ou $l = n$. En conséquence, l'entier n est premier.

La démonstration - suite et fin

(d) On a

$$0_B = f(0_A) = f(\mathrm{car}(A)1_A) = \mathrm{car}(A)1_B$$

d'où $\mathrm{car}(A) \in \ker(\varphi_B) = \mathrm{car}(B)\mathbb{Z}$.

(e) Soient K_1, K_2 deux corps de caractéristiques distinctes et $f : K_1 \to K_2$ un morphisme de corps. On a vu qu'un morphisme de corps est nécessairement injectif. On a également vu que $\mathrm{car}(K_2) \mid \mathrm{car}(K_1)$. Si $\mathrm{car}(K_2) = 0$, on a tout de suite $\mathrm{car}(K_1) = 0$. Supposons $\mathrm{car}(K_2) \neq 0$, i.e., $p := \mathrm{car}(K_2) \in \mathbb{P}$. Si $\mathrm{car}(K_1) \neq 0$, alors nécessairement $\mathrm{car}(K_1) = p$. Si $\mathrm{car}(K_1) = 0$, alors

$$0_{K_2} = pf(1_{K_1}) = f(p1_{K_1}),$$

en particulier (par injectivité de f) $p1_{K_1} = 0_{K_1}$ ce qui est contradictoire. ■

Le théorème des restes chinois dans $\mathbb{Z}$

Nous allons maintenant étendre un résultat très classique d'arithmétique sur $\mathbb{Z}$, à savoir l'isomorphisme d'anneaux suivant

$$\mathbb{Z}/n_1 \dots n_m\mathbb{Z} \simeq (\mathbb{Z}/n_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/n_m\mathbb{Z})$$

pour $n_1, \dots, n_m$ des entiers deux à deux premiers entre eux. Ce résultat est connu dans la littérature sous le nom de **"théorème des restes chinois".**

D'après le théorème de Bézout, nous savons que deux entiers a, b sont premiers entre eux si et seulement si il existe deux entiers u, v tels que

$$au + bv = 1.$$

Cette dernière égalité est encore équivalente à

$$a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}.$$

Cette égalité entre idéaux va être le point de départ de l'étude à venir.

Idéaux étrangers

L'égalité précédente nous amène à introduire le concept suivant :

Définition

Soient I, J deux idéaux d'un anneau commutatif A. On dit que I et J sont **étrangers** (ou **comaximaux**) lorsque $I + J = A$.

Produit de deux idéaux étrangers

Avant de pouvoir établir le théorème des restes chinois, nous devons énoncer et démontrer un certain nombre de résultats préliminaires.

Lemme

Soient I et J deux idéaux d'un anneau commutatif A. Si I et J sont étrangers, alors $IJ = I \cap J$.

Démonstration. On a toujours (même si I et J ne sont pas étrangers)

$$IJ \subset I \cap J.$$

Supposons I et J étrangers et fixons $x \in I \cap J$. Il existe $i \in I$ et $j \in J$ tels que $i + j = 1_A$. Il s'ensuit

$$ix + jx = x.$$

Il reste à voir que $ix \in IJ$ et $jx \in IJ$ pour conclure que $x \in IJ$. ■

Vers les restes chinois

Nous allons étendre ce dernier résultat à un nombre fini d'idéaux. C'est dans cet objectif que nous allons établir le lemme ci-dessous :

Lemme

Soient A un anneau commutatif, $n \geq 1$ un entier, $I, I_1, \ldots, I_n$ des idéaux de A. Si I est étranger avec I_k pour chaque $k \in \{1, \ldots, n\}$, alors il est étranger au produit $I_1 \ldots I_n$.

Démonstration. On note $P := I_1 \ldots I_n$. Supposons que I soit étranger avec I_k pour chaque $k \in \{1, \ldots, n\}$. On peut donc trouver pour chaque $k \in \{1, \ldots, n\}$ $x_k \in I$ et $a_k \in I_k$ tels que $1_A = x_k + a_k$. Il vient alors

$$\prod_{k=1}^{n} (x_k + a_k) = 1_A.$$

En développant le produit ci-dessus, on peut écrire pour un certain $b \in I$

$$b + \prod_{k=1}^{n} a_k = 1_A.$$

On conclut alors que $1_A \in I + P$, i.e., $A = I + P$. ■

Produit fini d'idéaux étrangers

Lemme

Soient A un anneau commutatif, $n \geq 1$ un entier, $I_1, \ldots, I_n$ des idéaux de A deux à deux étrangers. Alors, on a $I_1 \ldots I_n = I_1 \cap \ldots \cap I_n$.

Démonstration. Soit $(J_n)_{n \geq 1}$ une suite d'idéaux de A deux à deux étrangers. Pour chaque entier $k \geq 2$, on note $P(k)$ la propriété : "$J_1 \ldots J_k = J_1 \cap \ldots \cap J_k$". Nous allons montrer par récurrence que $P(k)$ a lieu pour tout entier $k \geq 2$.

La propriété $P(2)$ a déjà été établie précédemment.

Fixons un entier $k \geq 2$. Supposons que $P(k)$ ait lieu. On pose $H := J_1 \ldots J_k$. Notre hypothèse de récurrence nous dit que $H = J_1 \cap \ldots \cap J_k$. Puisque J_{k+1} est étranger avec $J_1, \ldots, J_k$, le lemme précédent nous dit que J_{k+1} est étranger avec l'idéal H. On conclut alors (là encore par un résultat vu ci-dessus) que $HJ_{k+1} = H \cap J_{k+1}$, i.e.,

$$J_1 \ldots J_{k+1} = J_1 \cap \ldots \cap J_{k+1}.$$

La récurrence est terminée et la démonstration également. ■

Théorème des restes chinois

Nous sommes maintenant en mesure d'énoncer et d'établir l'extension du théorème des restes chinois au cadre d'un anneau commutatif quelconque.

Théorème

Soient A un anneau commutatif, $n \geq 1$ un entier et $I_1, \ldots, I_n$ des idéaux de A deux à deux étrangers, $P = I_1 \ldots I_n$ leur produit. Alors, l'application $\varphi : A/P \to A/I_1 \times \ldots \times A/I_n$ définie par

$$\varphi(x + P) = (x + I_1, \ldots, x + I_n) \quad \text{pour tout } x \in A$$

est un isomorphisme d'anneaux.

La démonstration

Le fait que φ soit un morphisme d'anneaux découle des structures d'anneaux quotients et de la structure naturelle d'anneau produit. On note $B = A/I_1 \times \ldots \times A/I_n$.

On vérifie tout de suite que pour tout $x \in A$, on a

$$\varphi(x+P) = 0_B \Leftrightarrow \forall k \in \{1, \ldots, n\}, x + I_k = 0_{A/I_k} \Leftrightarrow x \in \bigcap_{k=1}^{n} I_k.$$

Ces équivalences et l'égalité $\bigcap_{k=1}^{n} I_k = \prod_{k=1}^{n} I_k$ entraînent que $\ker(\varphi) = \{0_{A/P}\}$, i.e., φ est injective.

La démonstration - suite et fin

Montrons que φ est surjective. Pour chaque $k \in \{1, \ldots, n\}$ fixons $y_k \in A/I_k$. Pour chaque $k \in \{1, \ldots, n\}$, il existe $x_k \in A$ tel que $x_k + I_k = y_k$. Pour chaque $r \in \{1, \ldots, n\}$, posons

$$J_r := \bigcap_{k \neq r} I_k = \prod_{k \neq r} I_k.$$

Notons que pour tout $r \in \{1, \ldots, n\}$ I_r est J_r sont étrangers (d'après un résultat précédent) donc il existe $a_r \in I_r$ et $c_r \in J_r$ tels que $a_r + c_r = 1_A$. On pose maintenant

$$x := \sum_{k=1}^{n} c_k x_k.$$

Fixons $i \in \{1, \ldots, n\}$. On a évidemment

$$x - x_i = \sum_{k \neq i} c_k x_k + (c_i - 1_A) x_i.$$

Pour tout $k \in \{1, \ldots, n\}$ avec $k \neq i$, on a $c_k \in J_k = \bigcap_{j \neq k} I_j \subset I_i$. Ceci et l'égalité $c_i - 1_A = -a_i \in I_i$ montrent que $x - x_i \in I_i$. On conclut que $x + I_i = x_i + I_i = y_i$ puis $\varphi(x + P) = (x_1 + I_1, \ldots, x_n + I_n) = (y_1, \ldots, y_n)$. ■

Corps des fractions d'un anneau intègre

Question. Etant donné un anneau commutatif A, peut-on construire un corps K contenant A ?

Pour $A = \mathbb{Z}$ (resp. $A = \mathbb{R}[X]$) la réponse est "oui" avec $K = \mathbb{Q}$ le corps des rationnels (resp. $K = \mathbb{R}[X]$ le corps des fractions rationnelles à une indéterminée à coefficients réels). Rappelons qu'un élément de $K = \mathbb{Q}$ est décrit par un élément $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\star$ traditionnellement noté $\frac{a}{b}$. De même un élément de $K = \mathbb{R}(X)$ est décrit par un élémént $(P, Q) \in \mathbb{R}[X] \times \mathbb{R}[X]^\star$ noté $\frac{P}{Q}$.

Nous allons étendre cette construction au cas d'un anneau commutatif **intègre** quelconque en s'inspirant des équivalences

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \qquad\qquad \frac{P}{Q} = \frac{R}{S} \Leftrightarrow PS = QR,$$

valides pour tout $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^\star$, pour tout $(P, Q), (R, S) \in \mathbb{R}[X] \times \mathbb{R}[X]^\star$. Notons que l'intégrité est une **condition nécessaire** puisqu'un corps est intègre.

La construction

Soit A un anneau commutatif intègre. On munit l'ensemble $E := A \times A^\star$ d'une relation binaire $\mathscr{R}$ définie pour tout $(a, b), (c, d) \in E$,

$$(a, b)\mathscr{R}(c, d) \Leftrightarrow ad = bc.$$

On commence par vérifier (grâce à la commutativité et à l'intégrité de A) que $\mathscr{R}$ est une relation d'équivalence, i.e., réflexive, symétrique et transitive. L'ensemble quotient $E/\mathscr{R}$ est noté $\mathrm{Frac}(A)$ ou parfois $K(A)$.

Traditionnellement, la classe d'équivalence d'un élément $(a, b) \in E$ est notée $\frac{a}{b}$, i.e.,

$$\frac{a}{b} := \big\{(c, d) \in E : (a, b)\mathscr{R}(c, d)\big\} = \big\{(c, d) \in E : ad = bc\big\}.$$

Elle est appelée **fraction** de **numérateur** a et de **dénominateur** b.

L'ensemble $\mathrm{Frac}(A)$ s'appelle **l'ensemble des fractions de** A.

Structure de corps pour l'ensemble des fractions

Nous allons ici voir comment munir naturellement l'ensemble des fractions d'une structure de corps commutatif.

Soit A un anneau commutatif intègre. On note $K := \mathrm{Frac}(A)$ et $E := A \times A^\star$.

En observant que pour tout $(a_1, b_1), (c_1, d_1), (a_2, b_2), (c_2, d_2) \in E$

$$\forall i \in \{1, 2\}, \frac{a_i}{b_i} = \frac{c_i}{d_i} \Rightarrow \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} = \frac{c_1 d_2 + c_2 d_1}{d_1 d_2} \quad \text{et} \quad \frac{a_1 a_2}{b_1 b_2} = \frac{c_1 c_2}{d_1 d_2},$$

nous pouvons définir deux lois internes sur K, notées $+_K$ et $\times_K$ en posant pour tout $(a, b), (a', b') \in E$

$$\frac{a}{b} +_K \frac{a'}{b'} := \frac{ab' + a'b}{bb'} \quad \text{et} \quad \frac{a}{b} \times_K \frac{a'}{b'} := \frac{aa'}{bb'}.$$

Des vérifications immédiates permettent d'établir le résultat crucial ci-après :

Théorème

L'ensemble des fractions de A muni des deux lois ci-dessus $+_K$ et $\times_K$ est un corps commutatif dont les éléments neutres respectifs sont $0_K := \frac{0_A}{1_A}$ et $1_K = \frac{1_A}{1_A}$.

L'ensemble $\mathrm{Frac}(A)$ est mieux connu sous le nom de **corps des fractions**.

Injection canonique dans le corps des fractions

Nous répondons ici à notre question initiale, à savoir que tout anneau commutatif intègre s'identifie à une partie d'un corps commutatif. Plus précisément :

Proposition

Soient A un anneau commutatif intègre. L'application $j : A \to \mathrm{Frac}(A)$ définie par

$$j(a) := \frac{a}{1_A} \quad \text{pour tout } a \in A$$

est un morphisme d'anneaux injectif.

Démonstration. Ceci découle directement de la définition de la loi additive et multiplicative du corps des fractions $\mathrm{Frac}(A)$. ■

Vers la propriété universelle du corps des fractions

Un constat évident : si le corps des fractions d'un anneau commutatif intègre A s'injecte dans un corps K, alors l'anneau A doit s'injecter dans K.

Plus précisément, notons $F := \mathrm{Frac}(A)$ et considérons un morphisme d'anneaux $\varphi : F \to K$. Ce dernier est injectif puisque F et K sont des corps. On en déduit que l'application $\varphi \circ j$ est un morphisme d'anneaux injectif. Ceci est résumé à travers le diagramme ci-dessous :

$$\begin{tikzcd}
A \arrow[r, hook, "j"] \arrow[dr, hook, "f=\varphi\circ j"'] & F \arrow[d, hook, "\varphi"] \\
& K
\end{tikzcd}$$

Propriété universelle du corps des fractions

Question : Existe t-il une réciproque au constat ci-dessus ? Autrement dit, si A s'injecte dans un corps K, est-ce que $\mathrm{Frac}(A)$ s'injecte dans K ?

Théorème

Soient A un anneau commutatif intègre, K un corps commutatif et $f : A \to K$ un morphisme d'anneaux injectif. Alors, il existe un unique morphisme d'anneaux $\varphi : F := \mathrm{Frac}(A) \to K$ tel que $f = \varphi \circ j$.

$$\begin{tikzcd} A \arrow[r, hook, "j"] \arrow[dr, hook, "f"'] & F \arrow[d, dotted, "\varphi"] \\ & K \end{tikzcd}$$

La démonstration

On commence par vérifier (en exploitant le fait que f soit un morphisme d'anneaux injectif et que K est un corps) pour tout $a, a' \in A$, $b, b' \in A \setminus \{0_A\}$

$$\frac{a}{b} = \frac{a'}{b'} \Rightarrow f(a)f(b)^{-1} = f(a')f(b')^{-1}.$$

Ceci permet de considérer l'application $\varphi : F \to K$ définie par

$$\varphi\Big(\frac{x}{y}\Big) = f(x)f(y)^{-1} \quad \text{pour tout}\, (x, y) \in A \times A \setminus \{0_A\}.$$

On vérifie sans difficultés que φ est un morphisme d'anneaux qui satisfait $f = \varphi \circ j$.

Soit $\psi : F \to K$ un morphisme d'anneaux tel que $f = \psi \circ j$. On a

$$\psi(\frac{a}{1_A}) = \varphi(\frac{a}{1_A}) = f(a) \quad \text{pour tout}\, a \in A.$$

Il reste à voir que ceci entraîne pour tout $a \in A$ et $b \in A \setminus \{0_A\}$

$$\varphi(\frac{a}{b}) = f(a)f(b)^{-1} = \psi(\frac{a}{1_A})\psi(\frac{b}{1_A})^{-1} = \psi(\frac{a}{1_A}\frac{1_A}{b}) = \psi(\frac{a}{b}).$$

La démonstration est terminée. ■

Maximalité et corps

A ce stade, nous savons que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier. Observons que l'idéal (p) avec p premier bénéficie d'une certaine propriété de maximalité, à savoir pour tout entier $k \geq 1$,

$$(p) \subset (k) \Rightarrow (k) = (p) \quad \text{ou} \quad (k) = \mathbb{Z}.$$

Ceci conduit à introduire la définition suivante :

Définition

Soit I un idéal d'un anneau commutatif A avec $I \neq A$. On dit que I est **maximal** si les seuls idéaux qui le contiennent sont lui-même et A.

Nous allons exploiter cette propriété afin de caractériser le type d'ideaux I pour lesquels le quotient A/I est un corps.

Maximalité et corps

On a l'important résultat suivant :

Proposition

Soient A un anneau commutatif et I un idéal de A. Alors, l'idéal I est **maximal** si et seulement si l'anneau quotient A/I est un corps.

$\Rightarrow$, Supposons que I soit maximal (en particulier, $I \neq A$). Soit $a \in A \setminus I$. On a $I \subset I + aA$ et $I \neq I + aA$ (sinon $a \in I$). Via la maximalité de I, on a $I + aA = A$. On peut alors écrire $i + ak = 1_A$ pour un couple $(i, k) \in I \times A$. Il vient

$$\pi_A(i + ak) = \pi_A(a)\pi_A(k) = 1_{A/I},$$

en particulier $\pi_A(a)$ est inversible dans A/I. On conclut que A/I est un anneau (commutatif) non nul dont tout élément non nul est inversible, i.e., A/I est un corps.

$\Leftarrow$, Supposons que A/I soit un corps (en particulier, A/I contient deux éléments et donc $I \neq A$). Soit J un idéal de A contenant I et tel que $J \neq I$. Fixons $j \in J \setminus I$. On a $\pi_A(j) \neq 0_{A/I}$, donc il existe $k \in A$ tel que

$$\pi_A(kj) = 1_{A/I}$$

ce qui donne $i \in I$ tel que $kj + i = 1_A$. Puisque $I \subset J$, on a $1_A \in J$ et ceci nous dit que $J = A$. En conclusion, l'idéal J est maximal. ■

Idéal maximal et irréductibilité

On dispose d'une description explicite des idéaux maximaux d'un anneau principal :

Proposition

Soient A un anneau commutatif intègre et $a \in A \setminus \{0_A\}$.

Si l'idéal (a) est maximal, alors l'élément a est irréductible dans A. Si de plus, A est principal, alors l'implication ci-dessus est une équivalence, i.e., (a) est maximal si et seulement si a est irréductible dans A.

Avant de donner la démonstration de ce résultat, il convient de noter que :

- Si A est un anneau réduit à deux éléments, disons $A = \{0_A, 1_A\}$, alors (0_A) est un idéal maximal tandis que l'élément 0_A n'est pas irréductible dans A.
- Nous verrons plus loin que 2 est irréductible dans $A = \mathbb{Z}[i\sqrt{5}]$ mais que l'idéal (2) n'est pas maximal dans A. En vertu du résultat précédent, nous obtenons que A n'est pas principal.

La démonstration

$\Rightarrow$, Supposons que (a) soit maximal. Observons que $a \notin A^\times$ (dans le cas contraire, on aurait $(a) = A$). Ecrivons maintenant $a = bc$ avec $b, c \in A$. Puisque $a \in (b)$ et $a \in (c)$, on doit avoir $(b) = (a)$ ou $(b) = A$ et de même $(c) = (a)$ ou $(c) = A$. Supposons que $(b) = (a)$ et $(c) = (a)$. Il existe alors $k, k' \in A$ tels que $b = ak$ et $c = ak'$. On obtient alors

$$a = bc = akak' = a^2kk'$$

ou encore $a(akk' - 1_A) = 0_A$. L'intégrité de A et la non nullité de a donnent alors $akk' = 1_A$, en particulier $a \in A^\times$. Ceci étant contradictoire, nous devons avoir nécessairement $(b) = A$ ou $(c) = A$ ce qui garantit que b ou c est inversible dans A.

$\Leftarrow$, Supposons que a soit irréductible dans A. Par définition, on a $a \notin A^\times$ et ceci entraîne $A \neq (a)$. Soit J un idéal de A contenant (a) et $J \neq (a)$. Puisque A est principal, il existe $b \in A$ tel que $J = (b)$. L'inclusion $(a) \subset (b)$ nous dit qu'il existe $c \in A$ tel que $a = bc$. L'irréductibilité de a dans A entraîne que $b \in A^\times$ ou $c \in A^\times$. Si $c \in A^\times$, on voit tout de suite que $b = c^{-1}a$ puis que $(a) = (b)$ et ceci est contradictoire. Finalement, on a $b \in A^\times$ et ceci montre que $J = A$. ■

Idéal premier

On s'intéresse maintenant au type d'idéaux I qui font du quotient A/I un anneau intègre.

Définition

Soient A un anneau commutatif et I un idéal de A avec $I \neq A$. On dit que I est **premier** lorsque pour tout $a, b \in A$, on a l'implication

$$ab \in I \Rightarrow a \in I \quad \text{ou} \quad b \in I.$$

- Soit $p \geq 2$ un entier. Alors, p est un nombre premier si et seulement si $p\mathbb{Z}$ est un idéal premier.
- Soit A un anneau commutatif. Alors, A est intègre si et seulement si (0_A) est premier.
- Dans $\mathbb{R}^{\mathbb{R}}$ muni de sa structure naturelle d'anneau, l'idéal

$$I_0 = \{f \in \mathbb{R}^{\mathbb{R}} : f(0) = 0\}$$

est premier.
- Soit $f : A \to B$ un morphisme d'anneaux non nul entre deux anneaux A et B. Si B est intègre, alors $\ker(f)$ est un idéal premier.

Proposition

Soient A un anneau commutatif et I un idéal de A avec $I \neq A$. Alors, l'idéal I est **premier** si et seulement si l'anneau quotient A/I est intègre.

Démonstration. $\Rightarrow$, Supposons que I soit premier. Soient $a, b \in A/I$ tels que $ab = 0_{A/I}$. Il existe $x, y \in A$ tels que $a = \pi_A(x)$ et $b = \pi_A(y)$. Il vient alors

$$\pi_A(xy) = ab = 0_{A/I},$$

i.e., $xy \in I$. Le fait que I soit premier nous dit alors que $x \in I$ ou $y \in I$, i.e., $a = 0_{A/I}$ ou $b = 0_{A/I}$.

$\Leftarrow$, Supposons que A/I soit intègre. Soient $a, b \in A$ tels que $ab \in I$. On a

$$0_{A/I} = \pi_A(ab) = \pi_A(a)\pi_A(b).$$

L'intégrité de A/I nous dit alors que $\pi_A(a) = 0_{A/I}$ ou $\pi_A(b) = 0_{A/I}$, i.e., $a \in I$ ou $b \in I$. ■

Maximal entraîne premier

Corollaire

Tout idéal maximal d'un anneau commutatif est premier.

Démonstration. Ceci résulte du fait que tout corps est un anneau intègre. ■

La réciproque est fausse ! Dans un anneau commutatif intègre A, l'idéal nul (0_A) est premier alors qu'il est rarement maximal.

Un bref retour sur les ensembles ordonnés

Nous allons avoir besoin d'un résultat de théorie des ensembles pour poursuivre notre étude.

Soit $(E, \preceq)$ un ensemble ordonné.

On dit qu'une partie non vide C de E est une **chaîne** (ou encore **totalement ordonnée**) lorsque pour toute paire d'éléments $x, y \in C$, on a $x \preceq y$ ou $y \preceq x$.

Un élément z de l'ensemble ordonné $(E, \preceq)$ est dit être **maximal** lorsqu'il n'existe dans E aucun élément $y \in E \setminus \{z\}$ vérifiant $z \preceq y$.

Pour une partie S non vide de l'ensemble ordonné $(E, \preceq)$, un élément $m \in E$ est dit être un **majorant** de S dans E lorsque pour tout $x \in S$, on a $x \preceq m$.

On dit que $(E, \preceq)$ est ordonné **inductivement** lorsque toute chaîne de E admet un majorant dans E.

Nous pouvons maintenant énoncer le résultat suivant :

Théorème (Lemme de Zorn)

Tout ensemble ordonné inductivement admet un élément maximal.

Le lemme de Zorn est connu pour être équivalent à :

Axiome (du choix)

Soient I un ensemble non vide et $(A_i)_{i \in I}$ une famille de parties non vides d'un ensemble X. Il existe une application $f : I \to X$ telle que $f(i) \in A_i$ pour tout $i \in I$.

Théorème de Krull

Nous sommes maintenant en mesure d'établir le résultat ci-dessous :

Théorème (Krull)

Soient A un anneau commutatif et I un idéal de A avec $I \neq A$. Alors, il existe un idéal maximal M de A tel que $I \subset M$.

Démonstration. On note E l'ensemble des idéaux J de A différents de A et contenant I. Cet ensemble est évidemment non vide car il contient I. On munit E de la relation d'ordre induite par l'inclusion $\subset$. Soit $\mathscr{C}$ une chaîne de E. On vérifie sans peine que l'ensemble $L := \bigcup_{J \in \mathscr{C}} J$ est un élément de E. Par ailleurs, l'ensemble L est un majorant de $\mathscr{C}$.

L'ensemble $(E, \subset)$ est donc ordonné inductivement : il admet un élément maximal M d'après le lemme de Zorn. L'ensemble M est donc un idéal de A différent de A contenant I. Soit B un idéal de A avec $M \subset B$ et $B \neq A$. Si $B \neq M$, alors M n'est pas un élément maximal de $(E, \subset)$. On conclut que $M = B$, i.e., M est un idéal maximal de A. Ceci termine la démonstration ■

Divisibilité dans les anneaux commutatifs

Nous allons étendre les nombreuses propriétés arithmétiques de $\mathbb{Z}$ et $K[X]$ et les concepts associés (pgcd, ppcm, premiers,...) à un grand nombre d'anneaux commutatifs.

Définition

Soient A un anneau commutatif et $a, b \in A$. On dit que a **divise** b lorsqu'il existe $c \in A$ tel que $ac = b$. On note alors $a \mid b$.

- On pourrait sans peine définir la notion de divisibilité à gauche et à droite (qui coïncident dans un anneau commutatif) : nous n'en aurons pas l'usage.
- Un élément inversible d'un anneau commutatif divise tous les éléments de cet anneau.
- Tout élément d'un anneau commutatif A divise 0_A.
- Soient a, b deux éléments d'un anneau commutatif A. On vérifie que $a \mid b$ si et seulement si $(b) \subset (a)$.
- La relation binaire induite par la divisibilité dans un anneau commutatif est réflexive et transitive : elle n'est cependant pas antisymétrique.

Association dans un anneau commutatif

Revenons un instant sur l'absence d'antisymétrie de la relation de divisibilité dans un anneau commutatif et observons que :

- Pour tout $m, n \in \mathbb{Z}$,

$$(n \mid m \quad \text{et} \quad m \mid n) \Rightarrow m = \pm n,$$

  i.e., m et n sont égaux à un inversible près de $\mathbb{Z}$.

- Pour tout $P, Q \in K[X]$ (où K est un corps commutatif) :

$$(P \mid Q \quad \text{et} \quad Q \mid P) \Rightarrow \exists \lambda \in K \setminus \{0\}, P = \lambda Q,$$

  i.e., P et Q sont égaux à un inversible près de $K[X]$.

Ceci amène à introduire le concept ci-dessous :

Définition

Soient a, b deux éléments d'un anneau commutatif A. On dit que a et b sont **associés** lorsque $a \mid b$ et $b \mid a$.

Caractérisations de l'association dans un anneau intègre

On peut caractériser l'association comme suit :

Proposition

Soient a, b deux éléments d'un anneau commutatif et intègre. Sont équivalentes :

(i) Les éléments a et b sont associés.

(ii) Il existe $c \in A^\times$ tel que $a = bc$.

(iii) Les idéaux (a) et (b) coïncident, i.e., $(a) = (b)$.

Démonstration. $(i) \Rightarrow (ii)$, Supposons que a et b soient associés. On peut supposer $a \neq 0_A$ (sinon la propriété voulue est immédiate). Il existe $c, d \in A$ tels que $ac = b$ et $bd = a$. Il vient alors $acd = bd = a$ puis $a(cd - 1_A) = 0_A$. L'intégrité de A nous dit alors que $cd = 1_A$, i.e., c et d sont inversibles dans A.
$(ii) \Rightarrow (iii)$, Supposons que $a = bc$ pour un certain $c \in A^\times$. On a tout de suite $a \in (b)$ puis $(a) \subset (b)$. Pour obtenir l'inclusion renversée, il suffit de procéder de même en exploitant l'égalité $b = ac^{-1}$.
$(iii) \Rightarrow (i)$, Il suffit de voir que l'inclusion $(b) \subset (a)$ entraîne $a \mid b$ tandis que l'inclusion $(a) \subset (b)$ donne $b \mid a$. ■

Elément premier

La notion de divisibilité dans un anneau commutatif va maintenant nous permettre de définir le concept de primalité dans un anneau. On s'inspire pour cela du célèbre lemme d'Euclide ou encore de la définition d'idéaux premiers vue ci-dessus.

Définition

Soit a un élément d'un anneau commutatif A. On dit que a est **premier** lorsque $a \notin A^{\times}$ et lorsque pour tout $x, y \in A$,

$$a \mid xy \Rightarrow a \mid x \quad \text{ou} \quad a \mid y.$$

Idéal principal engendré par un premier

On a déjà vu que si l'idéal (a) est maximal, alors l'élément a est irréductible (on rappelle que la réciproque est fausse en général). Dans le cas de la primalité, on dispose d'une équivalence :

Proposition

Soient A un anneau commutatif et $a \in A \setminus A^{\times}$. Alors, l'élément a est premier dans A si et seulement si l'idéal (a) est premier dans A.

Démonstration. $\Rightarrow$, Supposons que a soit premier. Notons que si $(a) = A$, alors $1_A \in (a)$ et ceci montre que a est inversible. On a donc $(a) \neq A$. Soient $c, d \in A$ tels que $cd \in (a)$. On a $a \mid cd$ puis (par primalité de a) $a \mid c$ ou $a \mid d$, i.e., $c \in (a)$ ou $d \in (a)$.

$\Leftarrow$, Supposons que (a) soit premier. Soient $c, d \in A$ tels que $a \mid cd$. On a $cd \in (a)$ puis (par primalité de l'idéal (a)) $c \in (a)$ ou $d \in (a)$, i.e., $c \in (a)$ ou $d \in (a)$. ■

Premier implique irréductible

Il convient d'examiner les liens entre primalité et irréductibilité.

Proposition

Soient A un anneau commutatif intègre et $a \in A \setminus \{0_A\}$. Si a est premier dans A, alors a est irréductible dans A.

Démonstration. Supposons que a soit premier dans A. Notons que $A \neq \{0_A\}$ et que a n'est pas inversible dans A. Par l'absurde, supposons que a ne soit pas irréductible dans A. On peut écrire $a = xy$ avec $x, y \in A$ non inversibles dans A. Supposons par l'absurde que $a \mid x$. Puisque $x \mid a$, a et x sont associés, i.e., il existe $b \in A^\times$ tel que $a = xb = xy$. L'intégrité de A assure alors que $b = y$ et ceci est absurde compte-tenu du caractère non inversible de y. On conclut que $a \nmid x$. De même, $a \nmid y$. Ainsi, a n'est pas premier dans A et ceci est contradictoire. ■

La réciproque est fausse !

On considère l'anneau $A = \mathbb{Z}[i\sqrt{5}] := \{a + i\sqrt{5}b : a, b \in \mathbb{Z}\}$ qui est commutatif (et intègre puisque $A \subset \mathbb{C}$). Nous allons montrer que 2 est irréductible dans A mais qu'il n'est pas premier dans A.

On observe facilement que

$$z := (1 - i\sqrt{5})(1 + i\sqrt{5}) = 2 \times 3,$$

en particulier $2 \mid z$. Puisque $2 \nmid (1 + i\sqrt{5})$ et $2 \nmid (1 - i\sqrt{5})$, on conclut que 2 n'est pas premier dans A.

Pour obtenir l'irréductibilité, on introduit l'application $N : A \to \mathbb{N}$ définie par

$$N(a + i\sqrt{5}b) := a^2 + 5b^2 \quad \text{pour tout } a, b \in \mathbb{Z}.$$

On vérifie que N est multiplicative, i.e., $N(zz') = N(z)N(z')$ pour tout $z, z' \in A$. Il découle de ceci que $A^\times = \{-1, 1\}$ et donc 2 n'est pas inversible dans A. Il reste à voir que si $2 = xy$ pour un certain couple $(x, y) \in A^2$, on a $4 = N(2) = N(xy) = N(x)N(y)$ et nécessairement $N(x) = 1$ ou $N(y) = 1$. On conclut que 2 est irréductible dans A.

Cet exemple montre que :

- 2 est irréductible dans $A := \mathbb{Z}[i\sqrt{5}]$ mais pas premier dans A.
- A n'est pas principal.
- (2) n'est pas un idéal premier de A (donc $A/(2)$ n'est pas un anneau intègre). En particulier, (2) n'est pas un idéal maximal de A (bien que 2 soit irréductible dans l'anneau A).

Anneau euclidien

Sur $\mathbb{Z}$ ou sur $K[X]$ (où K est un corps commutatif) nous disposons d'une division euclidienne. Cette division euclidienne permet notamment d'établir la principalité de ces anneaux. Nous introduisons maintenant une forme de division euclidienne sur les anneaux :

Définition

Soit $(A;+,\cdot)$ un anneau intègre et commutatif. On dit que A est **euclidien** lorsqu'il existe une application $\nu : A \setminus \{0_A\} \to \mathbb{N}$ telle que pour tout $a \in A$ et pour tout $b \in A \setminus \{0_A\}$, il existe un couple $(q,r) \in A^2$ (non nécessairement unique) tels que

$$a = bq + r \quad \text{avec} \quad r = 0_A \quad \text{ou} \quad \nu(r) < \nu(b).$$

Une telle application ν est appelée **stathme euclidien** sur A.

Euclidien implique principal

En adaptant (légèrement) la démonstration du caractère principal de $\mathbb{Z}$, on montre la

Proposition

Soit $(A;+,\cdot)$ un anneau commutatif. Si A est euclidien, alors A est principal.

Démonstration. Supposons que A soit euclidien, en particulier $A \neq \{0_A\}$. Notons ν un stathme euclidien de A. Soit $\mathscr{I}$ un idéal de A. L'ensemble

$$\Omega := \{\nu(i) : i \in \mathscr{I} \setminus \{0_A\}\}$$

étant une partie non vide de $\mathbb{N}$, elle admet un plus petit élément noté ω. Soit $b \in \mathscr{I} \setminus \{0_A\}$ tel que $\nu(b) = \omega$. Nous allons établir que $\mathscr{I} = bA$. Commençons par voir que l'inclusion $bA \subset \mathscr{I}$ est évidente. Montrons l'inclusion renversée. Fixons $a \in \mathscr{I}$. Il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0_A$ ou $\nu(r) < \nu(b)$. Si $r = 0_A$, alors $a \in bA$ et l'égalité désirée a lieu. Supposons donc $r \neq 0_A$. Puisque $b, aq \in \mathscr{I}$, on doit avoir $r = a - bq \in \mathscr{I} \setminus \{0_A\}$ et ceci entraîne $\nu(r) \geq \omega = nu(b)$, une contradiction. On conclut que l'idéal $\mathscr{I}$ est principal. La démonstration est terminée. ■

La réciproque est fausse : il existe des anneaux principaux qui ne sont pas euclidiens. L'exemple classique (et non trivial) est donné par $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$.

Plus grand commun diviseur

Définition

Soient a, b deux éléments d'un anneau commutatif intègre A. On dit que $d \in A$ est un **plus grand commun diviseur** (abrégé en p.g.c.d.) de a et b lorsque $d \mid a$ et $d \mid b$ et lorsque pour tout $x \in A$,

$$\big(x \mid a \quad \text{et} \quad x \mid b\big) \Rightarrow x \mid d.$$

L'ensemble des p.g.c.d. de a et b est noté $\mathrm{P.G.C.D.}(a, b)$.

- On a bien sûr que tout p.g.c.d. de a et de b est un p.g.c.d. de b et de a (et donc $\mathrm{P.G.C.D.}(a, b) = \mathrm{P.G.C.D.}(b, a)$).
- Pour tout $x \in A$, $x \in \mathrm{P.G.C.D.}(x, 0_A)$ (en particulier, $0_A \in \mathrm{P.G.C.D.}(0_A, 0_A)$).
- Le p.g.c.d. de deux éléments non simultanément nuls est non nul.
- On peut définir de manière analogue la notion de p.g.c.d. pour une famille finie d'éléments non nuls d'un anneau commutatif intègre.

Un p.g.c.d. ou le p.g.c.d. ?

Un simple examen de la situation sur $\mathbb{Z}$ ou sur $K[X]$ (avec K corps commutatif) nous dit d'ores et déjà que l'unicité du p.g.c.d. sur ces deux anneaux est artificielle. Elle provient en effet d'une convention : positif pour $\mathbb{Z}$ et unitaire pour $K[X]$.

Soient a, b deux éléments d'un anneau commutatif intègre A et d un p.g.c.d. de a et de b. Si $\delta \in A$ désigne un p.g.c.d. de a et de b, on a doit avoir $d \mid \delta$ et $\delta \mid d$. L'intégrité de l'anneau A nous dit alors que d et δ sont égaux à un inversible près, i.e., $d = u\delta$ avec $u \in A^\times$. En conséquence, on a l'égalité

$$\mathrm{P.G.C.D.}(a, b) = \{du : u \in A^\times\} =: dA^\times.$$

Ainsi, l'ensemble des p.g.c.d. de a et de b est entièrement déterminé par la donnée d'un seul p.g.c.d. de a et de b.

Générateur de l'idéal somme et p.g.c.d.

Le résultat ci-dessous est aussi simple que fondamental :

Proposition

Soient a, b deux éléments d'un anneau A commutatif intègre. Si $(a) + (b) = (d)$ pour un certain $d \in A$, alors d est un p.g.c.d. de a et de b. [3]

Démonstration. On suppose qu'il existe $d \in A$ tel que $(a) + (b) = (d)$. On vérifie tout de suite que pour tout $x \in A$,

$$(x \mid a \quad \text{et} \quad x \mid b) \Leftrightarrow (d) = (a) + (b) \subset (x).$$

L'élément d divise bien sûr a et b. Par ailleurs, si x est un diviseur commun à a et b, alors $(d) \subset (x)$ d'après ce qui précède, i.e., $x \mid d$. On conclut que d est un p.g.c.d. de a et de b. ■

[3] **Remarque.** L'idéal engendré par un p.g.c.d. de a et b n'est pas toujours $(a) + (b)$. Dans $\mathbb{R}[X, Y] := (\mathbb{R}[X])[Y]$, 1 est un p.g.c.d. de X et Y mais $(X) + (Y) \neq (1)$.

Anneau à p.g.c.d.

Nous introduisons ici une nouvelle classe d'anneaux en lien avec la notion de p.g.c.d.

Définition

On dit qu'un anneau est un **anneau à p.g.c.d.** lorsqu'il est commutatif, intègre et si tout couple d'éléments non nuls admet un p.g.c.d.

Cette définition et le résultat précédent donnent sans difficultés :

Proposition

Tout anneau principal est un anneau à p.g.c.d.

Plus petit commun multiple

Sans surprise, nous pouvons définir de manière analogue la notion de p.p.c.m.

Définition

Soient a, b deux éléments d'un anneau commutatif intègre A. On dit que $m \in A$ est un **plus grand commun multiple** (abrégé en p.p.c.m.) de a et b lorsque $a \mid m$ et $b \mid m$ et lorsque pour tout $x \in A$,

$$\big(a \mid x \quad \text{et} \quad b \mid x\big) \Rightarrow m \mid x.$$

L'ensemble des p.p.c.m. de a et b est noté $\mathrm{P.P.C.M.}(a, b)$.

- On a bien sûr que tout p.p.c.m. de a et de b est un p.p.c.m. de b et de a (et donc $\mathrm{P.P.C.M.}(a, b) = \mathrm{P.P.C.M.}(b, a)$).
- Pour tout $x \in A$, $0_A \in \mathrm{P.P.C.M.}(x, 0_A)$ (en particulier, $0_A \in \mathrm{P.P.C.M.}(0_A, 0_A)$).
- On peut définir de manière analogue la notion de p.p.c.m. pour une famille finie d'éléments d'un anneau commutatif intègre.

Unicité du p.p.c.m. ?

Comme dans le cas des p.g.c.d., on ne peut espérer une propriété d'unicité du p.p.c.m.

Etant deux éléments a, b d'un anneau commutatif intègre qui admettent un p.p.c.m. noté m, on peut vérifier sans difficultés (grâce à l'intégrité de A) que l'ensemble $\mathrm{P.P.C.M.}(a, b)$ des p.p.c.m. de a et de b satisfait

$$\mathrm{P.P.C.M.}(a, b) = \{mu : u \in A^\times\} =: mA^\times .$$

Ainsi, la donnée d'un p.p.c.m. de a et de b suffit à déterminer complètement l'ensemble des p.p.c.m. de a et de b.

Générateur de l'idéal intersection et p.p.c.m.

On a vu ci-dessus que le p.g.c.d. est lié à la somme des idéaux $(a)+(b)$. On donne ci-dessous un résultat analogue pour le p.p.c.m.

Proposition

Soient a, b deux éléments non nuls d'un anneau A commutatif intègre. L'idéal $(a)\cap(b)$ est principal si et seulement si a et b admettent un p.p.c.m. Si tel est le cas, tout générateur de $(a)\cap(b)$ est un p.p.c.m. de a et de b.

Démonstration. On vérifie tout de suite que pour tout $x \in A$,

$$(a \mid x \quad \text{et} \quad b \mid x) \Leftrightarrow (x) \subset (a)\cap(b).$$

$\Rightarrow$, On suppose qu'il existe $m \in A$ tel que $(a)\cap(b) = (m)$. L'élément m est bien sûr un multiple commun à a et à b. Il reste à voir que l'équivalence ci-dessus entraîne que tout multiple commun m' de a et de b satisfait $(m') \subset (m)$, i.e., $m \mid m'$.
$\Leftarrow$, Soit m un p.p.c.m. de a et de b. L'équivalence énoncée ci-dessus nous dit que $(m) \subset (a)\cap(b) =: I$. Fixons $c \in I$. Il est clair que c est un multiple commun à a et à b, d'où l'inclusion $c \in (m)$. L'égalité voulue en découle. ■

Corollaire

Tout couple d'éléments non nuls d'un anneau principal admet un p.p.c.m.

L'existence d'un p.p.c.m. entraîne l'existence d'un p.g.c.d.

Il est naturel d'étudier les liens entretenus par ces deux concepts.

Théorème

Soient a, b deux éléments non nuls d'un anneau commutatif intègre A admettant un p.p.c.m. Alors, a et b admettent un p.g.c.d. De plus, on a

$$md \sim ab,$$

pour tout $d \in \mathrm{P.G.C.D.}(a, b)$ et pour tout $m \in \mathrm{P.P.C.M.}(a, b)$.

La démonstration

Notons m un p.p.c.m. de a et de b. Observons tout d'abord que $m \mid ab$ puisque ab est un multiple de a et de b. Il existe ainsi $d \in A$ tel que $md = ab$. Nous allons montrer que d est un p.g.c.d. de a et de b.

On tire de $a \mid m$ et de $b \mid m$ l'existence de $k, l \in A$ tels que $ak = m$ et $bl = m$. Il s'ensuit $a(kd - b) = 0_A$ et $b(ld - a) = 0_A$. L'intégrité de A nous dit que $kd - b = 0_A = ld - a$, en particulier $d \mid a$ et $d \mid b$.

Soit δ un diviseur commun de a et de b. Il existe alors $k', l' \in A$ tels que $\delta k' = a$ et $\delta l' = b$. On a bien sûr $\delta \mid ab$ et ceci permet d'écrire $ab = \delta c$ pour un certain $c \in A$. Il vient $abk' = \delta k' c = ac$ et $abl' = \delta l' c = bc$ puis par intégrité de A, $a \mid c$ et $b \mid c$. On en déduit que c est un multiple commun à a et b et donc $m \mid c$. Cette dernière relation nous donne $e \in A$ tel que $me = c$. En multipliant par δ, on en arrive à $\delta me = \delta c = ab = md$. En combinant le caractère intègre de A avec le fait que $m \neq 0_A$, on aboutit à $\delta \mid d$. On conclut que d est un p.g.c.d. de a et de b.

La relation d'association souhaitée découle de l'égalité $md = ab$ et du fait que deux p.g.c.d. (resp. deux p.p.c.m.) de a et de b sont associés. ■

L'existence d'un p.g.c.d. N'ENTRAINE PAS l'existence d'un p.p.c.m.

Nous allons voir que l'existence d'un p.g.c.d. n'entraîne pas l'existence d'un p.p.c.m. On note $A = \mathbb{Z}[i\sqrt{5}]$ et on définit l'application $N : A \to \mathbb{N}$ par

$$N(x + iy\sqrt{5}) = x^2 + 5y^2 \quad \text{pour tout } a, b \in \mathbb{Z}.$$

On vérifie sans difficultés que N est multiplicative. A l'aide de cette application, on montre que $A^\times = \{-1, 1\}$ et que les seuls diviseurs communs à $a := 2$ et à $b := 1 + i\sqrt{5}$ sont les inversibles. Ainsi, $d := 1$ est un p.g.c.d. de a et de b. Supposons que a et b admettent un p.p.c.m. noté m. Le résultat précédent nous dit alors que $m1 = m \sim ab = 2(1 + i\sqrt{5})$. Par ailleurs, 6 est un multiple commun de a et b puisque

$$(1 - i\sqrt{5})(1 + i\sqrt{5}) = 6 = 3 \times 2.$$

On en déduit que $m \mid 6$ puis $b = 1 + i\sqrt{5} \mid 3$. Il existe alors $z \in A$ tel que $bz = 3$. Ceci entraîne $N(b)N(z) = N(3) = 9$, i.e., $6N(z) = 9$. Ceci étant absurde, on conclut que a et b n'ont pas de p.p.c.m.

Eléments premiers entre eux

On peut étendre le concept d'éléments premiers entre eux sans avoir recours aux notions de p.g.c.d ou de p.p.c.m.

Définition

Soient a, b deux éléments non nuls d'un anneau commutatif et intègre A. On dit que a et b sont **premiers entre eux** lorsque les seuls diviseurs communs à a et à b sont les éléments inversibles de A.

Soient A un anneau commutatif intègre, $a, b \in A \setminus \{0_A\}$.

- Supposons que a n'est pas inversible dans A. Si $b \in (a)$, alors a et b ne sont pas premiers entre eux.
- Supposons que a est irréductible dans A (donc en particulier a n'est pas inversible dans A) et $b \notin (a)$. Alors, a est b ne sont pas premiers entre eux. Nous verrons que la réciproque a lieu dans les anneaux à p.g.c.d.

Eléments premiers entre eux - Caractérisations

On caractérise ici les éléments premiers entre eux via les notions de p.g.c.d. et p.p.c.m.

Proposition

Soient a, b deux éléments non nuls d'un anneau A commutatif et intègre. Ont lieu :

(a) Les éléments a et b sont premiers entre eux si et seulement si 1_A est un p.g.c.d. de a et b, i.e., $\mathrm{P.G.C.D.}(a, b) = A^{\times}$.

(b) Si a et b ont un p.p.c.m., alors a et b sont premiers entre eux si et seulement si ab est un p.p.c.m de a et b, i.e., $\mathrm{P.P.C.M.}(a, b) = abA^{\times}$.

La démonstration

Commençons par établir (a).
$\Rightarrow$, Evidemment 1_A est un diviseur commun à a et à b. Soit d un diviseur commun à a et à b. Par hypothèse, $d \in A^\times$ et ceci nous dit que $dd^{-1} = 1_A$, en particulier $d \mid 1_A$.
$\Leftarrow$, Soit d un diviseur commun à a et à b. Par hypothèse, $d \mid 1_A$, i.e., il existe $e \in A$ tel que $de = 1_A$. On conclut que d est inversible dans A.

Nous allons maintenant montrer (b). Supposons que a et b admettent un p.p.c.m. noté m.
$\Rightarrow$, D'après l'implication $\Rightarrow$ précédente, nous savons que 1_A est un p.g.c.d. de a et b. Il suffit alors d'invoquer le résultat liant l'existence d'un p.p.c.m. à celle d'un p.g.c.d. pour obtenir $m1_A = m \sim ab$.

$\Leftarrow$, Par application du résultat d'existence p.p.c.m./p.g.c.d., nous sommes assurés de l'existence d'un p.g.c.d. pour a et b noté d. Ce même résultat nous dit également que $md \sim ab$. D'autre part, notre hypothèse nous donne tout de suite $m \sim ab$. On en déduit que d est inversible dans A, en particulier 1_A est un p.g.c.d. de a et de b. ■

Eléments premiers entre eux dans un anneau à p.g.c.d.

Soient $a, b \in \mathbb{Z}$ non nuls et d un p.g.c.d. de a et b. Il est bien connu que les entiers a' et b' tels que $a = da'$ et $b = db'$ sont premiers entre eux. Nous étendons ce résultat très utile dans le cadre des anneaux à p.g.c.d.

Proposition

Soient a, b deux éléments non nuls d'un anneau commutatif intègre A admettant un p.g.c.d. et d un diviseur commun à a et à b. Soient $a', b' \in A$ tels que $a = da'$ et $b = db'$. Alors, $d \in \mathrm{P.G.C.D.}(a, b)$ si et seulement si a', b' sont premiers entre eux.

Démonstration. $\Rightarrow$, Supposons que a et b admettent d pour p.g.c.d. Soit $\delta \in A$ un diviseur commun de a' et de b'. Bien sûr, δd est un diviseur commun de $a = da'$ et $b = db'$. Le fait que d soit un p.g.c.d. de a et b nous donne alors que δd divise d, d'où l'on tire (par intégrité de A et le fait que $d \neq 0_A$) que δ est inversible.

$\Leftrightarrow$, Supposons que a et b soient premiers entre eux. Soit δ un p.g.c.d. de a et de b. On a bien sûr que d est un diviseur commun à $a = da'$ et $b = db'$ et ceci entraîne que $d \mid \delta$. Soit $k \in A$ tel que $kd = \delta$. Puisque δ divise da' et db', il existe $l, m \in A$ tels que $l\delta = da'$ et $m\delta = db'$. Il s'ensuit $kdl = da'$ et $kdm = db'$ puis par intégrité de A (et le fait que $d \neq 0$) $kl = a'$ et $km = b'$. On obtient alors que k est un diviseur commun à a' et b', i.e., k est inversible dans A. On conclut que $\delta \mid d$. La démonstration est terminée. ■

Extension du lemme de Gauss

Le célèbre lemme de Gauss s'étend au cadre des anneaux à p.g.c.d.

Proposition (Lemme de Gauss)

Soient a, b deux éléments non nuls d'un anneau commutatif intègre A admettant un p.g.c.d. Sont équivalentes :

(a) Les éléments a et b sont premiers entre eux.

(b) Pour tout $c \in A$, on a l'implication

$$a \mid bc \Rightarrow a \mid c.$$

Démonstration. $(a) \Rightarrow (b)$, Soit $c \in A$. Supposons que $a \mid bc$. Si $c = 0_A$, il n'y a rien à établir. Supposons donc $c \neq 0_A$. D'après un résultat précédent, c est un p.g.c.d. de ca et cb. Ceci et le fait que a soit un diviseur commun à bc et à ac donnent tout de suite que $a \mid c$.

$(b) \Rightarrow (a)$, Soit d un diviseur commun à a et à b. Il existe alors $c, d \in A$ tels que $a = dc$ et $b = de$. On a $bc = dec = ae$, en particulier $a \mid bc$. Par hypothèse, il vient $a \mid c$. On obtient alors $k \in A$ tel que $ak = c$. Cette dernière égalité combinée à $a = dc$ donne $dck = c$. L'intégrité de A et le fait que $c \neq 0_A$ entraînent $dk = 1_A$, i.e., d est inversible dans A. ■

Homogénéité du P.G.C.D.

Nous déduisons du lemme de Gauss un résultat d'homogénéité pour le p.g.c.d.

Proposition

Soient a, b deux éléments non nuls d'un anneau commutatif intègre A admettant un p.g.c.d. Alors, on a

$$\mathrm{P.G.C.D.}(ca, cb) = c\mathrm{P.G.C.D.}(a, b) \quad \text{pour tout } c \in A \setminus \{0\}.$$

Démonstration. Fixons $c \in A$ non nul. Soit $d \in \mathrm{P.G.C.D.}(a, b) \neq \emptyset$. Il nous suffit d'établir que cd est un p.g.c.d. de ca et cb car alors

$$\mathrm{P.G.C.D.}(ca, cb) = cdA^{\times} = c\mathrm{P.G.C.D.}(a, b).$$

Bien sûr, l'élément cd est un diviseur commun de ca et cb puisque d est lui-même un diviseur commun de a et b. Considérons maintenant x un diviseur commun de ca et cb et montrons que x divise cd. Soient $k, l \in A$ tels que $kx = ca$ et $lx = cb$. Soient $a', b' \in A$ tels que $da' = a$ et $db' = b$. Nous savons par ailleurs que les éléments a' et b' sont premiers entre eux. On a $kx = cda'$ et $lx = cdb'$ d'où l'on tire

$$lcda' = lkx = klx = kcdb'.$$

Par intégrité de A (et via le fait que $cd \neq 0_A$) $kb' = la'$, en particulier $a' \mid kb'$.

La démonstration - suite et fin

Une application du lemme de Gauss donne alors $a' \mid k$. On dispose donc de $e \in A$ tel que $a'e = k$. On déduit alors

$$kxe = cae = cda'e = cdk$$

puis par intégrité de A (et le fait que $k \neq 0_A$) $xe = cd$, en particulier $x \mid cd$. La démonstration est terminée. ■

Existence du p.p.c.m. dans les anneaux à p.g.c.d.

On a vu que l'existence d'un p.p.c.m. entraîne celle d'un p.g.c.d. et que la réciproque est fausse en général. Nous allons établir que celle-ci a lieu dans les anneaux à p.g.c.d.

Théorème

Tout couple d'éléments non nuls d'un anneau à p.g.c.d. admet un p.p.c.m.

Démonstration. Soient a, b deux éléments non nuls d'un anneau à p.g.c.d. A. Notons d un p.g.c.d. de a et de b. Il existe $a', b' \in A$ tels que $a = da'$ et $b = db'$. D'après un résultat précédent, nous savons que a' et b' sont premiers entre eux. Posons $m = da'b'$ qui est évidemment un multiple de a et de b. Soit m' un autre multiple de a et de b. Il existe $\alpha, \beta \in A$ tels que $m' = a\alpha = b\beta$. Il vient alors $da'\alpha = db'\beta$ puis par intégrité de A, $a'\alpha = b'\beta$, en particulier $a' \mid b'\beta$. Par application du lemme de Gauss, on obtient $a' \mid \beta$. Il s'ensuit $m = ba' \mid b\beta = m'$. On conclut que m est un p.p.c.m. de a et de b. ■

Deux corollaires

Le théorème précédent et le fait que (dans un anneau commutatif intègre) l'existence d'un p.p.c.m. entraîne l'existence d'un p.g.c.d. donne aisément le résultat suivant :

Corollaire

Soit A un anneau commutatif intègre. Alors, A est un anneau à p.g.c.d. si et seulement si tout couple d'éléments non nuls de A admet un p.p.c.m.

Nous sommes également en mesure de caractériser les anneaux à P.G.C.D. via la principalité de certains idéaux:

Corollaire

Soit A un anneau commutatif intègre. Alors, A est un anneau à p.g.c.d. si et seulement si l'intersection de deux idéaux principaux de A est un idéal principal.

Démonstration. Il suffit d'exploiter le corollaire ci-dessus et le fait que pour $x, y \in A$ non nuls, on a équivalence entre l'existence d'un p.p.c.m. pour a et b et le caractère principal de l'idéal $(a) \cap (b)$. ■

Primalité vs irréductibilité

On se propose maintenant d'établir que dans tout anneau à P.G.C.D., les notions de primalité et d'irréductibilité coïncident. Il n'est pas inutile de rappeler que :

- Dans les anneaux commutatifs intègres, tout élément premier est irréductible.
- La réciproque est fausse (un contre-exemple a été donné dans $\mathbb{Z}[i\sqrt{5}]$).

Lemme

Soit A un anneau à p.g.c.d. et $a \notin \left(A^\times \cup \{0_A\}\right)$. Alors, a est irréductible dans A si et seulement si il est premier avec tous les éléments de A qui ne sont pas dans (a).

Démonstration. $\Rightarrow$, Soit $b \in A \setminus (a)$. Soit d un diviseur commun de a et b. Il existe $\lambda, \mu \in A$ tels que $d\lambda = a$ et $d\mu = b$. Supposons que $d \notin A^\times$. Par irréductibilité de A, on doit avoir $\lambda \in A^\times$. Il vient alors $\lambda^{-1}\mu a = b$, en particulier $b \in (a)$. Ceci est contradictoire et nous permet de conclure que $d \in A^\times$, i.e., a et b sont premiers entres eux.
$\Leftarrow$, Soient $x, y \in A$ tels que $a = xy$. Supposons dans un premier temps que $x \in (a)$. Le fait que $a \neq 0_A$ et l'intégrité de A donnent facilement que $y \in A^\times$. Supposons que $x \notin (a)$. Par hypothèse, x est premier avec a. En combinant ceci et la relation $a \mid xy$, nous pouvons appliquer le lemme de Gauss pour obtenir $a \mid y$. De même que ci-dessus, l'intégrité de A nous assure de l'inclusion $x \in A^\times$. ■

Un cas d'équivalence entre premier et irréductible/Lemme d'Euclide

Nous pouvons maintenant facilement établir le résultat attendu:

Proposition (Lemme d'Euclide)

Soient A un anneau à p.g.c.d. et $p \in A \setminus \{0_A\}$. Alors, p est irréductible si et seulement si p est premier.

Démonstration. Seule l'implication $\Rightarrow$ est à établir. Supposons que p soit irréductible (en particulier, $p \notin \left(A^\times \cup \{0_A\}\right)$). Soient $x, y \in A$. Supposons que $p \mid xy$. Si $x \in (p)$, il n'y a rien à établir. On peut donc supposer $x \notin (p)$ et ainsi appliquer le lemme ci-dessus pour obtenir que x est premier avec p. On conclut par le lemme de Gauss. ■

La seule implication digne d'intérêt (i.e. l'implication $\Rightarrow$) dans le résultat ci-dessus *dit exactement* que pour un élément irréductible p d'un anneau à P.G.C.D. noté A, on a pour chaque $x, y \in A^2$

$$p \mid xy \Rightarrow p \mid x \quad \text{ou} \quad p \mid y.$$

Anneau de Bézout

Remarquons que le théorème de Bézout n'a encore pas été évoqué dans les développements précédents. Notre objectif est à présent d'étendre ce célèbre résultat d'arithmétique pour une vaste classes d'anneaux.

Définition

Soit A un anneau commutatif et intègre. On dit que A est un anneau de **Bézout** lorsque la somme de deux idéaux principaux de A est un idéal principal de A.

Tout de suite, constatons que :

Proposition

Tout anneau principal est un anneau de Bézout [4] et tout anneau de Bézout est un anneau à p.g.c.d.

Démonstration. Le fait que tout anneau principal est un anneau de Bézout est évident. Soient a, b deux éléments non nuls d'un anneau de Bézout A. Il existe alors $d \in A$ tel que $(a) + (b) = (d)$ et ceci entraîne (comme nous l'avons déjà vu) que d est un p.g.c.d. de a et de b. ■

[4] Il existe des anneaux de Bézout non principaux : l'exemple classique vient de *l'analyse complexe*.

Théorème de Bézout

Le théorème de Bézout possède une extension naturelle dans les anneaux de Bézout.

Théorème

Soient a, b deux éléments non nuls d'un anneau de Bézout A. Alors, a et b sont premiers entre eux si et seulement si il existe $u, v \in A$ tels que

$$au + bv = 1_A.$$

Démonstration. $\Rightarrow$, Supposons que a et b soient premiers entre eux. Le fait que A soit un anneau de Bézout garantit l'existence de $d \in A$ tel que $(a) + (b) = (d)$. Il s'ensuit que d est un p.g.c.d. de a et de b. Ces deux éléments étant premiers entre eux, ils admettent pour p.g.c.d. l'élément 1_A. Il vient alors $(d) = A$.

$\Leftarrow$, Supposons qu'il existe $u, v \in A$ tels que $au + bv = 1_A$. On a $1_A \in (a) + (b)$ et ceci entraîne $A = (1_A) = (a) + (b)$. On conclut que 1_A est un p.g.c.d. de a et de b, i.e., a et b sont premiers entre eux. ■

Nous allons voir que la proportionnalité de deux éléments irréductibles est liée à leur caractère premier entre eux.

Proposition

Soient A un anneau principal, $a, b \in A$ deux éléments irréductibles. Alors, $(a) \neq (b)$ si et seulement si a et b sont premiers entre eux.

Démonstration. Supposons $(a) \neq (b)$. Les idéaux (a) et (b) sont maximaux par irréductibilité de a et b et par principalité de l'anneau A. On a bien sûr $(a) \subset (a, b)$ et $(a) \neq (a, b)$ (si $(a, b) = (a)$, alors $b \in (a)$ puis $(b) \subset (a)$ et par maximalité de (b) on aurait $(b) = (a, b)$, en particulier $a \in (b)$ et enfin $(a) = (b)$). Par maximalité de (a), il vient $(a, b) = A$, d'où l'existence de $u, v \in A$ tels que $au + bv = 1_A$. L'anneau A étant de Bézout, nous concluons que a et b sont premiers entre eux.
$\Leftarrow$, Supposons que a et b soient premiers entre eux. On a donc $(a) + (b) = A$. Si $(a) = (b)$, alors $(a) = A$ et c'est absurde car (a) est maximal. ■

Définition

Soit A un anneau intègre et commutatif. On dit que A est **factoriel** lorsque les deux conditions suivantes ont lieu : :

(E) pour chaque $a \in A \setminus \{0_A\}$, il existe $u \in A^\times$ et une famille finie (éventuellement vide) $(p_i)_{i \in I}$ d'éléments irréductibles de A tels que $a = u \prod_{i \in I} p_i$;

(U) pour tout $r, s \geq 1$ entiers et tout $p_1, \ldots, p_r, q_1, \ldots, q_s \in A$ irréductibles tels que

$$p_1 \ldots p_r = q_1 \ldots q_s,$$

on a $r = s$ et de plus, il existe une permutation σ de $\{1, \ldots, r\}$ telle que pour tout $i \in \{1, \ldots, r\}$, p_i et $q_{\sigma(i)}$ sont associés dans A.

Autrement exprimée la condition (U) signifie que la décomposition en irréductibles donnée par (E) est unique aux inversibles près et à l'ordre près des facteurs.

Systèmes de représentants des éléments irréductibles

Soit A un anneau commutatif intègre.

Considérons la relation binaire $\mathscr{R}$ sur A définie pour tout $a, b \in A$ par $a\mathscr{R}b$ si et seulement si a et b sont associés (ce qui est noté $a \sim b$ et qui signifie qu'il existe $u \in A^\times$ tel que $a = ub$). Il est clair que $\mathscr{R}$ est une relation d'équivalence sur A : on note $A\backslash\sim$ à la place de $A/\mathscr{R}$. La classe d'équivalence d'un élément $a \in A$ est donnée par

$$\widetilde{a} := \{b \in A : a\mathscr{R}b\} = \left\{\lambda a : \lambda \in A^\times\right\} = A^\times a = aA^\times.$$

Pour chaque élément p irréductible dans A, choisissons (c'est possible grâce à l'axiome du choix) un unique représentant dans la classe $\widetilde{p}$ (qui ne contient bien sûr que des éléments irréductibles de A). On note $\mathscr{I}$ l'ensemble de ses représentants.

On vérifie aisément les deux faits suivants :

(i) pour tout élément irréductible q de A, il existe $p \in \mathscr{I}$ tel que $p \sim q$;

(ii) pour tout $p, q \in A$, on a l'implication $p \sim q \Rightarrow p = q$.

Soit $\mathscr{I}$ un système de représentants des éléments irréductibles d'un anneau factoriel A un anneau factoriel. Pour tout $a \in A$ non nul, il existe $u \in A^\times$ et une unique famille $(k_p)_{p \in \mathscr{I}}$ d'entiers naturels, nuls sauf un nombre fini, tels que

$$a = u \prod_{p \in \mathscr{I}} p^{k_p}.$$

Pour chaque $p \in \mathscr{I}$, l'unique entier k_p ci-dessus est appelée la valuation de a en p et est notée $v_p(a)$.

Propriétés de la valuation

Expression d'un p.g.c.d. et d'un p.p.c.m. dans un anneau factoriel

Théorème

Soit $\mathscr{I}$ un système de représentants des éléments irréductibles d'un anneau factoriel A. Soient $a, b \in A$ non nuls de décomposition en irréductibles

$$a = u \prod_{p \in \mathscr{I}} p^{v_p(a)} \quad \text{et} \quad b = v \prod_{p \in \mathscr{I}} p^{v_p(b)},$$

avec $u, v \in A^\times$. Alors, les éléments

$$d = \prod_{p \in \mathscr{I}} p^{\min(v_p(a), v_p(b))} \quad \text{et} \quad m = \prod_{p \in \mathscr{I}} p^{\max(v_p(a), v_p(b))}$$

sont respectivement un p.g.c.d. et un p.p.c.m. de a et b

Avant d'établir le résultat, notons l'importante conséquence suivante :

Corollaire

Tout anneau factoriel est un anneau à p.g.c.d.

La démonstration

******

On déduit de la proposition précédente le résultat suivant qui vient en complément du fait que tout anneau à p.g.c.d. noethérien est factoriel.

Théorème

Soit A un anneau intègre. Alors, A est factoriel si et seulement les deux propriétés suivantes ont lieu :

(i) toute suite croissante d'idéaux principaux de A est stationnaire;

(ii) tout élément irréductible de A est premier.

La démonstration de l'implication $\Rightarrow$

$\Rightarrow$, Supposons que A soit un anneau factoriel. Montrons que (ii) est satisfaite. Fixons $p \in A$ un élément irréductible de A. Soient $x, y \in A$. Supposons que $p \mid xy$. Il existe $k \in A$ tels que $xy = pk$. Notons que si x est nul, on a tout de suite $p \mid x$ tandis que si x est inversible, on a $y = pkx^{-1}$ et là encore $p \mid y$. Les mêmes constatations valent pour y. Nous pouvons donc supposer que x, y sont non nuls et non inversibles. Si k est nul, alors x et ou y est nul et on a $p \mid x$ ou $p \mid y$. Si k est inversible, alors $xyk^{-1} = p$ et p apparaît (à un inversible près) dans la décomposition en irréductibles de x ou de y, en particulier $p \mid x$ ou $p \mid y$. Nous pouvons alors supposer k non nul et non inversible. Remarquons maintenant que xy peut s'écrire comme un produit d'irréductibles de deux manières :
- la première en remplaçant k par sa décomposition en irréductibles de A; - la deuxième consiste à décomposer x et y en irréductibles de A. Le caractère factoriel de A nous dit que les deux décompositions en irréductibles de xy sont les mêmes à l'ordre des termes près et à la multiplication par des inversibles près. Comme p apparaît dans la première, il doit y avoir un irréductible associé à p dans la décomposition de x ou de y. Il s'ensuit $p \mid x$ ou $p \mid y$.

Suite de la démonstration de l'implication $\Rightarrow$

Montrons maintenant que (i) a lieu. Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de A telle que

$$(a_n) \subset (a_{n+1}) \quad \text{pour tout } n \in \mathbb{N}.$$

On peut supposer que pour tout $n \in \mathbb{N}$, $a_n \notin A^\times$ (sinon la suite d'idéaux $(a_n)_{n\in\mathbb{N}}$ est stationnaire de valeur A). On peut également supposer qu'il existe $N \in \mathbb{N}$ tel que $a_N \neq 0$. Notons que $a_n \notin (A^\times) \cup \{0_A\}$ pour tout $n \geq N$. Pour chaque $n \geq N$, notons l_n le nombre d'éléments irréductibles dans la décomposition de a_n. Puisque $a_N \in (a_{N+1})$, il existe $d_N \in A$ avec $d_N \neq 0_A$ tel que $a_N = d_N a_{N+1}$. Si $d_N \in A^\times$, il est clair que $l_N = l_{N+1}$. Si ce n'est pas le cas, alors d admet une décomposition (unique à association près et à l'ordre près des facteurs) en irréductibles de A et ceci donne facilement $l_N \geq l_{N+1}$. Ainsi, $(l_n)_{n\in\mathbb{N}}$ est une suite décroissante d'entiers naturels : elle est donc stationnaire. Soit $n_0 \geq N$ tel que $l_n = l_{n+1}$ pour tout $n \geq n_0$. Soient $p, q \geq n_0$ avec $q > p$. Il existe $d \in A$ avec $d \neq 0_A$ tel que $a_p = da_q$. Si d admet une décomposition en irréductible, alors nécessairement $l_p > l_q$ et ceci est contradictoire. Ceci montre que d est inversible dans A et permet de conclure que $(a_p) = (a_q)$. La suite $(a_n)_{n\in\mathbb{N}}$ est stationnaire.

Suite de la démonstration de l'implication $\Leftarrow$

$\Leftarrow$, Supposons que A vérifie (i) et (ii) de l'énoncé. Fixons (si possible!) $x \in A \setminus A^{\times} \cup \{0_A\}$. Si x est irréductible, alors x satisfait la propriété (E) de la définition des anneaux factoriels. Supposons que x ne soit pas irréductible. Il existe alors $a_1, b_1 \in A$ non inversibles tels que $x = a_1 b_1$. Si a_1 et b_1 sont irréductibles, alors x vérifie la propriété (E) de la définition des anneaux factoriels. Supposons que ce ne soit pas le cas et supposons sans pertes de généralités que a_1 n'est pas irréductible. On a évidemment $(x) \subset (a_1)$. Si $(a_1) \subset (x)$, alors l'intégrité de A et le fait que $a_1 \neq 0$ montrent que b_1 est inversible ce qui n'est pas le cas. On a donc $(x) \neq (a_1)$.

L'élément a_1 étant non nul, non inversible et non irréductible, nous pouvons reproduire la discussion réalisée ci-dessus pour x. On obtient donc a_2 et b_2 non inversibles tels que $a_1 = a_2 b_2$. Si ces deux éléments sont irréductibles, alors ou bien b_1 est irréductible et c'est terminé car $x = a_2 b_2 b_1$ ou bien b_1 ne l'est pas. Supposons donc

Principal entraîne factoriel

Il s'agit à présenter de situer le concept d'anneau factoriel vis-à-vis des autres notions d'anneaux étudiées auparavant.

Proposition

Tout anneau à p.g.c.d. noethérien est factoriel. En particulier, tout anneau principal est factoriel.

Démonstration. On a déjà vu que dans un anneau à p.g.c.d. les éléments irréductibles sont premiers. Il suffit alors d'appliquer le théorème précédent pour conclure. ■

Remarque. La réciproque du cas particulier de la proposition ci-dessus n'a évidemment pas lieu : en effet, $\mathbb{Z}[X]$ est factoriel (car $\mathbb{Z}$ l'est) mais n'est pas principal. De manière moins évidente : on peut construire des anneaux factoriels non noethériens.

Proposition

Soit A un anneau factoriel. Alors, $A[X]$ est factoriel.

Proposition

Tout anneau de Bézout factoriel est principal.

Démonstration. Supposons qu'il existe un idéal de A qui ne soit pas principal. Fixons $a_1 \in I$ et posons $I_1 := (a_1)$. Puisque I n'est pas principal, nous pouvons choisir $b_1 \in I \setminus I_1$ et poser $I_2 := I_1 + (b_1)$. Le fait que A soit un anneau de Bézout nous dit alors que I_2 est principal et nous donne $a_2 \in I_2$ tel que $I_2 = (a_2)$. Observons alors que $I_1 \subset I_2$ et $I_1 \neq I_2$. On construit ainsi une suite $(I_n)_{n \geq 1}$ d'idéaux de A strictement croissante (pour l'inclusion $\subset$) et ceci contredit bien sûr le caractère noetherien de A.

■