Arithmétique des anneaux principaux

Brian Revesz, Louis Lascaud

December 12, 2022

Table des matières

Définitions

Anneau

Un anneau $(A, +, \times)$ est la donnée d'un groupe commutatif $(A, +)$ et d'une loi de composition interne $\times$ sur A associative, possédant un élément neutre et distributive à gauche et à droite sur $+$.

Anneau commutatif

Un anneau est commutatif si $\times$ l'est.

Sous-anneau

Un sous-anneau d'un anneau A est une partie B de A, qui, pour les lois induites, est un anneau.

Corps et inversibles

Définition

L'ensemble des éléments symétrisables pour la loi $\times$ de A est noté $A^\times$ ou A^* est appelé ensemble des *inversibles* ou *unités*.

Définition

Un corps est un anneau non nul, commutatif, dans lequel tout élément non nul admet un inverse.

Remarques

0 est absorbant

Dans tout anneau A, pour tout $a \in A$, $a \times 0 = 0 \times a = 0$.

0 n'est jamais inversible

Dans un anneau non trivial, 0 n'est pas inversible.

Anneaux intègres

Définition

Un anneau est dit *intègre* s'il est commutatif, non trivial et sans diviseur de zéro autre que zéro lui-même. Autrement dit, A est commutatif et pour tous $a, b \in A$, $ab = 0$ si et seulement si $a = 0$ ou $b = 0$.

Idéal

Définition

Soit A un anneau unitaire et I une partie de A. On dit que I est un *idéal à gauche* de A si $(I, +)$ est un sous-groupe de $(A, +)$ et pour tous $a \in A$, $x \in I$, on a $ax \in I$. On définit de même un *idéal à droite* de A. Si I est un idéal de A à gauche et à droite, on dit que I est un idéal *bilatère*. Dans un anneau commutatif, les notions d'idéal à droite et d'idéal à gauche sont confondues.

Somme et intersection d'idéaux

Intersection d'idéaux

Toute intersection d'idéaux à gauche (resp. à droite, bilatères) est un idéal à gauche (resp. à droite, bilatère). C'est le plus grand idéal contenu dans tous ceux-là.

Somme finie d'idéaux

Toute somme finie d'idéaux à gauche (resp. à droite, bilatères) est un idéal à gauche (resp. à droite, bilatère). C'est le plus petit idéal contenant tous ceux-là.

Réunion d'idéaux

En général, la réunion de deux idéaux n'est pas un idéal.

Idéal principal engendré par un élément

Définition

Soit $a \in A$. Alors aA est un idéal à droite de A, appelé *idéal à droite principal de A engendré par a*. On dit aussi que a est UN *générateur* de aA. On note $aA = (a)_d$. Un idéal est dit *principal* s'il est l'idéal principal engendré par un des éléments de A. On définit de même l'idéal à gauche principal engendré par a noté $(a)_g$, l'idéal bilatère engendré par a noté $(a) = AaA$ et dans le cas commutatif, $aA = Aa$ donc on parle d'idéal principal engendré par un élément et l'on note (a).

Remarque

Définition

Soit A un anneau unitaire, I un idéal à gauche (resp. à droite, bilatère) de A.

1. On a $I = A$ si et seulement si $I \cap A^* \neq \emptyset$.
2. Si A est de plus commutatif, pour tout $a \in A$, $(a) = A$ si et seulement si a est une unité.

Anneau quotient par un idéal bilatère

Définition

Soit I un idéal bilatère de A. Alors le quotient de groupes $A/I = \{a + I, a \in A\}$ est muni de la structure d'anneau.

Idéal maximal

Définition

Un idéal I de A est dit *maximal* s'il est élément maximal parmi les idéaux propres de A.

Propriété

L'idéal I est maximal si et seulement si A/I est un corps (non nécessairement commutatif).

Théorème de Krull

Théorème

Tout idéal propre d'un anneau A est inclus dans un idéal maximal de A.

Idéal premier

Définition

Un idéal I est premier si et seulement si pour tous $x, y \in A$, si $xy \in I$, $x \in I$ ou $y \in I$.

Propriété

On appelle *idéal premier* de A tout idéal I tel que l'anneau quotient A/I est intègre.

Lien entre les idéaux premiers et les idéaux maximaux

Propriété

Tout idéal maximal est premier.

Divisibilité

Définition

Soient $a, b \in A$. On dit que a *divise* b, ou que a est un *diviseur* de b, ou que b est un *multiple* de a, si b appartient à l'idéal principal à gauche engendré par a, c'est-à-dire, s'il existe $c \in A$ tel que $b = ac$. On note : $a|b$.

Reformulation

Soient $a, b \in A$. L'élément a divise b, si et seulement si, $bA \subseteq aA$.

Association

Définition

Deux éléments $a, b \in A$ sont dits *associés* si $a|b$ et $b|a$ (autrement dit, si $aA = bA$).

Propriété

Deux éléments d'un anneau **intègre** sont associés s'il existe une unité $c \in A^*$ telle que $b = ac$, cette relation étant bien sûr symétrique.

Primalité relative, étrangeté

Définition

On dit que $a, b \in A$ sont *premiers entre eux*, ou que a est *premier à* b, si pour tout $d \in A$, on a $(d|a \text{ et } d|b) \Rightarrow d \in A^*$.

Définition

On dit que $a, b \in A$ sont *étrangers*, s'il existe $u, v \in A$ tels que $au + bv = 1$.

Propriété

Deux éléments étrangers sont premiers entre eux.

Pgcd et ppcm

Définition

Soient $a, b \in A$. On dit que $d \in A$ est UN *plus grand diviseur commun*, ou *pgcd*, de a et b, si d divise a et b et pour tout $c \in A$, si c divise a et b, c divise d.

Définition

Soient $a, b \in A$. On dit que $m \in A$ est UN *plus grand multiple commun*, ou *ppcm*, de a et b, si a et b divisent m et pour tout $c \in A$, si a et b divisent c, m divise c.

Propriété

Deux pgcd (resp. ppcm) de deux éléments d'un anneau A, lorsqu'ils existent, sont uniques à association près.

Irréductibilité, primalité

Définition

Un élément $\pi \in A$ est dit *irréductible* s'il est non nul, non inversible, et si pour tous $a, b \in A$, on a $\pi = ab \Longrightarrow a \in A^*$ ou $b \in A^*$.

Définition

Un élément $\pi \in A$ est dit *premier* si l'idéal (π) est premier non nul, ou, ce qui revient au même, si π est non nul, non inversible et vérifie le lemme d'Euclide : pour tous $a, b \in A$, π divise ab si et seulement si π divise a ou π divise b.

Remarque

Si A est intègre, tout élément premier est irréductible d'après ce qui précède. Un élément irréductible n'est pas toujours premier.

Factorisation dans un anneau

Tout élément non nul d'un anneau peut-il se décomposer en produit d'un élément inversible et d'éléments irréductibles ? Si oui, la décomposition est-elle unique à permutation et association près des facteurs ?

- En toute généralité, l'existence d'une telle décomposition est infirmée.
- Pire, il existe des anneaux qui ne sont pas des corps et qui ne possèdent aucun élément irréductible.
- Dans un anneau où l'existence de la décomposition est assurée, l'unicité ne l'est pas forcément.

Factorisation dans un anneau

Propriété

Soit A un anneau simplifiable. On suppose que l'on a un égalité $up_1...p_r = u'\pi_1...\pi_s$ où r, s sont deux entiers naturels, u, u' inversibles, $p_1, ..., p_r$ premiers et $\pi_1, ..., \pi_s$ irréductibles. Alors $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que $p_i = \pi_{\sigma(i)}$ soient associés pour tout $i \in 1, r$. Puisque associés à des éléments premiers, les $\pi_1, ..., \pi_s$ sont en fait premiers.

Anneau principal

Définition

Un anneau est dit *principal* s'il est intègre et si tout idéal de A est principal. (En particulier, il est unitaire, commutatif et les idéaux sont automatiquement bilatères.)

Exemple fondamental

Théorème

L'anneau $\mathbb{Z}$ est principal.

Proof.

1. Il s'agit essentiellement de montrer que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$.
2. On considère le plus entier strictement positif inclus dans l'idéal n et l'on montre $I = n\mathbb{Z}$
3. Pour un élément de l'idéal, on effectue la division euclidienne par n et l'on constate que par minimalité de n, le reste doit être nul.

Anneaux euclidiens

Définition

Un anneau A est dit *euclidien* s'il est intègre et s'il existe une application appelée *stathme euclidien* $\delta : A \setminus \{0\} \longrightarrow \mathbb{N}$ telle que pour tout $a \in A$ et pour tout $b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$, et $r = 0$ ou $\delta(r) < \delta(b)$.

Généralisation du théorème précécent

Théorème

Tout anneau euclidien est principal.

Pgcd, ppcm

Propriété

Soit A un anneau principal. Soient $a, b \in A$ et $d \in A$ tels que $(a) + (b) = (d)$. Alors d est un pgcd de a et b. Soit $m \in A$ tel que $(a) \cap (b) = (m)$. Alors m est un ppcm de a et b.

Corollaire

Dans un anneau principal, tout couple d'élément admet un pgcd et un ppcm.

Quelques propriétés rassurantes

Théorème de Bézout

Soit A un anneau principal. Deux éléments sont étrangers si et seulement s'ils sont premiers entre eux.

Lemme de Gauss

Soient $a, b \in A$ deux éléments premiers entre eux d'un anneau principal. Alors pour tout $c \in A$, si a divise bc, alors a divise c.

Théorème des restes chinois

Soient $a_1, ..., a_n \in A$ principal deux à deux premiers entre eux. Alors les anneaux $A/(a_1...a_n)$ et $A/(a_1) \times ... \times A/(a_n)$ sont isomorphes.

Idéaux maximaux dans les anneaux principaux

Lemme

Soit A un anneau commutatif unitaire et π un élément irréductible. Alors (π) est maximal parmi les idéaux propres principaux de A.

Conséquence

Soit A un anneau principal. Tout irréductible de A engendre un idéal maximal.

Conséquence (lemme d'Euclide)

Dans un anneau principal, un élément est irréductible si et seulement s'il est premier.

Idéaux maximaux dans les anneaux principaux

Conséquence

Dans un anneau principal, un idéal non nul est premier si et seulement s'il est maximal.

Conséquence (lemme d'Euclide)

Soit A un anneau principal et π un élément non nul. Les propositions suivantes sont équivalentes :

(i) $A/(\pi)$ est un corps ;

(ii) $A/(\pi)$ est un anneau intègre ;

(iii) π est irréductible.

Anneaux factoriels

Définition

Un anneau A est dit *factoriel* s'il est intègre et tout élément non nul $a \in A$ peut s'écrire $a = u\pi_1 ... \pi_r$, où $\pi_1, ..., \pi_r$ sont irréductibles et $u \in A^*$ et si de plus, cette écriture est unique à permutation et association des facteurs près.

Lien entre anneaux principaux et anneaux factoriels

Théorème

Tout anneau principal est factoriel.

Lien entre anneaux principaux et anneaux factoriels

Lemme

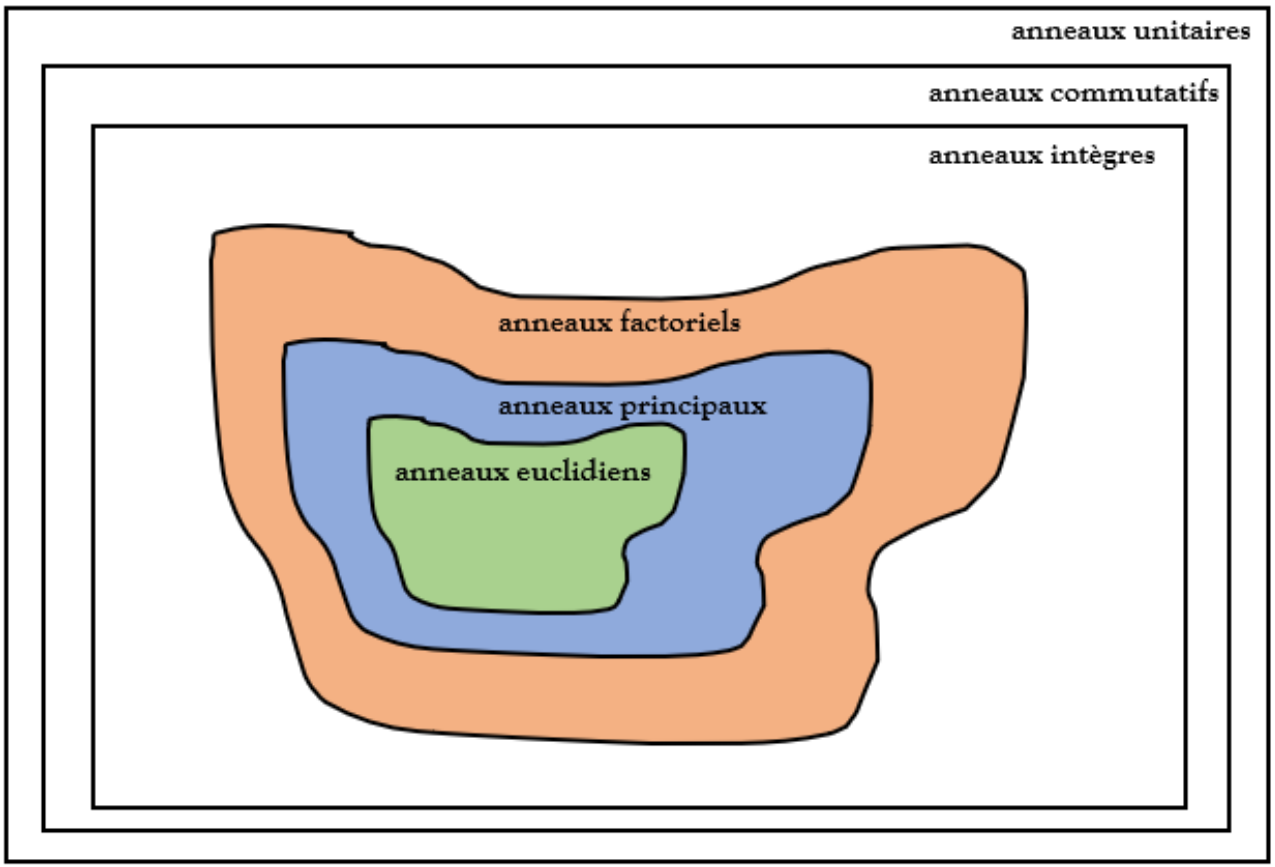
Dans un anneau principal, tout élément non nul non inversible possède un diviseur irréductible.

Preuve

Proof.

1. On peut supposer a non nul, non inversible.
2. On note $a = \pi_1 a_1$. Si a_1 est inversible, c'est terminé. Sinon, $(a) \subsetneq (a_1)$.
3. Par récurrence, on construit une chaîne infinie d'idéaux $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq ... \subsetneq (a_n) \subsetneq ...$, où $a_n \in A \setminus A^*$ pour tout $n \geqslant 1$ si c'est possible.
4. On pose $I = \bigcup_{n \in \mathbb{N}} (a_n)$. C'est un idéal, engendré par x. Mais $x \in (a_j)$, dont on déduit $(x) \subsetneq (x)$: contradiction.
5. Donc la construction des a_i est finie, ce qu'il fallait montrer.
6. L'unicité a déjà été traitée.

Conclusion


anneaux unitaires
anneaux commutatifs
anneaux intègres
anneaux factoriels
anneaux principaux
anneaux euclidiens