5. Arithmétique dans les anneaux

1. $\mathbb{Z}$, l'anneau modèle
2. Expression de l'arithmétique dans un anneau commutatif
3. Propriété des anneaux intègres
4. Lien entre élément premier et élément irréductible
5. Anneau euclidien, principal, factoriel
6. A euclidien $\implies$ A principal
7. A principal $\implies$ A factoriel
8. A corps $\iff$ $A[X]$ principal
9. A factoriel $\implies$ $A[X]$ factoriel

1. $\mathbb{Z}$, l'anneau modèle

$(\mathbb{Z}, +, 0, \cdot, 1)$ est un anneau commutatif intègre.

Propiétés arithmétiques de $\mathbb{Z}$

1. division euclidienne
2. les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$
3. factorisation unique (à l'ordre et au signe près)

et aussi : Algorithme d'Euclide, Théorème de Bézout, Lemme de Gauss

Remarque :
$\mathbb{Z}^* = \{-1; 1\}$ et donc : "au signe près" $=$ "à un inversible près"

2. Expression de l'arithmétique dans un anneau commutatif

Soit un anneau $(A, +, 0, *, e)$ commutatif.

• Soit $a \in A$. Le plus petit idéal de A contenant a s'appelle l'idéal engendré par a et se note (a).

Définition (idéal principal)

On dit que $I \subset A$, est un idéal principal s'il existe $a \in A$ tel que $I = (a)$.

Exercices :

1. $\boxed{(a) = aA = \{a * x \ : x \in A\}}$
2. $u \in A^* \iff (u) = A$

• Soient $a, a' \in A$.

a divise a'

$$a|a' \overset{\text{déf}}{\iff} (\exists b \in A) \ \ a * b = a' \iff a' \in (a) \iff (a') \subset (a)$$

arithmétique dans un anneau commutatif (2)

- Exercice : On définit une relation d'équivalence sur A par

$$\forall a, a' \in A, \qquad \boxed{a \sim a' \overset{\text{déf}}{\iff} (\exists u \in A^*) \;\; a * u = a'}$$

Définition (éléments associés)

On dit que les éléments a et a' de A sont associés si $a \sim a'$.

Exercice : $a \sim a' \implies a|a'$ et $a'|a \iff (a) = (a')$
(réciproque fausse en général . . .)

• Définition (un pgcd)

Soient $a, a' \in A$. On dit que $d \in A$ est un pgcd de a et a' si

$$d|a, \;\; d|a' \text{ et } \big((\forall c \in A) \;\; \big(c|a \text{ et } c|a'\big) \implies c|d\big)$$

existence ? unicité ?
s'il existe, $\mathrm{pgcd}(a, a')$ désigne un pgcd quelconque de a et a'.

arithmétique dans un anneau commutatif (3)

• Définition (un ppcm)

Soient $a, a' \in A$. On dit que $m \in A$ est un ppcm de a et a' si

$$a|m,\ a'|m \text{ et } \big((\forall c \in A) \quad \big(a|c \text{ et } a'|c\big) \implies m|c\big)$$

existence ? unicité ?
s'il existe, $\mathrm{ppcm}(a, a')$ désigne un ppcm quelconque de a et a'.

• Définition (premiers entre eux)

Soient $a, a' \in A$. On dit que a et a' sont premiers entre eux (ou étrangers) si leurs seuls diviseurs communs sont les inversibles. Dans ce cas, l'ensemble des pgcd est A^*, on notera simplement $\mathrm{pgcd}(a, a') \sim e$.

arithmétique dans un anneau commutatif (4)

• Définition (élément irréductible)

On dit que $a \in A$ est irréductible si

$$a \notin A^* \quad \text{et} \quad ((\forall x, y \in A) \quad a = x * y \quad \Longrightarrow \quad (x \in A^* \text{ ou } y \in A^*) \quad)$$

Exercice : a irréductible $\Longrightarrow$ $a \neq 0$.

• Définition (élément premier)

On dit que $a \in A$ est premier si (a) est un idéal premier, *i.e.*

$$(a) \neq A \quad \text{et} \quad ((\forall x, y \in A) \quad x * y \in (a) \quad \Longrightarrow \quad (x \in A \text{ ou } y \in A) \quad)$$

Exercice : A est intègre $\Longleftrightarrow$ 0 est premier.

arithmétique dans un anneau commutatif (5)

• Propriété de Bézout

$$(\forall a, b \in A \setminus \{0\}) \qquad d \sim \operatorname{pgcd}(a,b) \iff \underbrace{(a)+(b)}_{=(a,b)=aA+bA} = (d)$$

Exercices : On a toujours :

1. $(\forall a, b \in A \setminus \{0\}) \qquad d \sim \operatorname{pgcd}(a,b) \implies (a)+(b) \subset (d).$
2. $(\forall a, b \in A \setminus \{0\}) \qquad (a)+(b) = (d) \implies d \sim \operatorname{pgcd}(a,b).$

• Propriété de Gauss

$$(\forall a, x, y \in A) \qquad (a|x*y \ \text{ et } \ \operatorname{pgcd}(a,x) \sim e) \implies a|y$$

Exercice : Bézout $\implies$ Gauss.

3. Propriété des anneaux intègres

Soit $(A, +, 0, *, e)$ un anneau commutatif intègre.

Proposition

1. $\forall a, a' \in A$,
   $a \sim a' \overset{déf}{\iff} (\exists u \in A^*) \ a * u = a' \iff a|a' \text{ et } a'|a \iff (a) = (a')$
2. *Si d et d' sont deux pgcd de a et a', alors $d \sim d'$.*
3. *0 est premier.*
4. *a premier non nul $\Longrightarrow$ a irréductible.*
5. *Soient $a, a' \in A$ tels que $a \sim a'$. Alors on a :*

$$a \text{ irréductible} \iff a' \text{ irréductible}$$
$$a \text{ premier} \iff a' \text{ premier}$$

Démonstration : exercices. □

Les anneaux considérés dans la suite seront tous commutatifs et intègres.

4. Anneau euclidien, principal, factoriel

Définition (anneau euclidien)

Un anneau $(A, +, 0, *, e)$ est euclidien s'il est intègre et admet une application $\delta : A \setminus \{0\} \to \mathbb{N}$, appelée stathme euclidien, ayant la propriété :

$$(\forall (a,b) \in A \times A \setminus \{0\})(\exists (q,r) \in A \times A) \quad \begin{cases} a = b * q + r \\ r = 0 \ \text{ ou } \delta(r) < \delta(b) \end{cases}$$

Exemples :

1. $\mathbb{Z}$ est un anneau euclidien pour le stathme $\delta(n) = |n|$.
2. $K[X]$ (où K est un corps) est un anneau euclidien pour le stathme $\delta(P) = \deg(P)$.

Anneau principal

Définition (anneau principal)

Un anneau $(A, +, 0, *, e)$ est principal s'il est intègre et si tous ses idéaux sont principaux.

Exemples :

1. $\mathbb{Z}$ est un anneau principal.
2. Tout anneau euclidien est principal (voir plus loin), en particulier $K[X]$ est principal.
3. La réciproque est fausse : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal et non euclidien [admis, Réf. Perrin].

Proposition (théorème de Bézout pour les anneaux principaux)

Tout anneau principal possède la propriété de Bézout.

Démonstration : il suffit de montrer $d \sim \mathrm{pgcd}(a,b) \implies (d) \subset (a)+(b)$.
$(a)+(b) = (d')$ puisque principal. Donc $\mathrm{pgcd}(a,b) \sim d'$, puis $(d) = (d')$. $\square$

Anneau factoriel

Soit $(A, +, 0, *, e)$ un anneau commutatif intègre.

- $a \in A$ admet une décomposition en irréductibles si

$$a = u * p_1^{\alpha_1} * \cdots * p_n^{\alpha_n} \text{ où : } u \in A^* \text{ et } (\forall k \in [\![1, n]\!]) \quad \alpha_k \in \mathbb{N}, p_k \text{ irréductible}$$

- Deux décompositions de a en irréductibles, $a = u * p_1^{\alpha_1} * \cdots * p_n^{\alpha_n}$ et $a = v * q_1^{\beta_1} * \cdots * q_m^{\beta_m}$ sont équivalentes si $n = m$ et s'il existe $\sigma \in \mathfrak{S}_n$ telle que

$$(\forall k \in [\![1, n]\!]) \qquad p_{\sigma(k)} \sim q_k \quad \text{et} \quad \alpha_{\sigma(k)} = \beta_k$$

Définition (anneau factoriel)

Un anneau $(A, +, 0, *, e)$ est factoriel s'il est intègre et si tout $a \in A \setminus \{0\}$ admet une décomposition en irréductibles, unique à équivalence près.

Exemples :

1. $\mathbb{Z}$ est un anneau factoriel ; plus généralement, tout anneau principal est factoriel (voir plus loin), en particulier $K[X]$ est factoriel.
2. Réciproque fausse : $\mathbb{Z}[X]$ est factoriel et non principal (voir plus loin).

Anneau factoriel (suite)

Soit $(A, +, 0, *, e)$ un anneau factoriel.

• formons une famille $\mathbb{P}$ d'éléments irréductibles de A en choisissant exactement un élément dans chaque classe d'équivalence d'élément irréductible pour la relation $\sim$.

• tout $a \in A \setminus \{0\}$ s'écrit de manière unique comme

$$a = u * \prod_{p \in \mathbb{P}} p^{v_p(a)} \text{ où : } u \in A^* \text{ et } v_p(a) \in \mathbb{N}, \text{ tous nuls sauf un nombre fini}$$

Exercices :

1. $b|a \iff (\forall p \in \mathbb{P}) \;\; v_p(b) \leq v_p(a)$.
2. $\operatorname{pgcd}(a,b) \sim \prod_{p \in \mathbb{P}} p^{\min(v_p(a), v_p(b))}$ et $\operatorname{ppcm}(a,b) \sim \prod_{p \in \mathbb{P}} p^{\max(v_p(a), v_p(b))}$.

Proposition (lemme de Gauss pour les anneaux factoriels)

Tout anneau factoriel possède la propriété de Gauss.

Démonstration : par la décomposition en irréductibles (exercice). □

5. Lien entre élément premier et élément irréductible

Soit $(A, +, 0, *, e)$ un anneau commutatif intègre. On a déjà vu que :

1. 0 est premier mais n'est pas irréductible.
2. (0) est un idéal premier.
3. (0) idéal maximal $\iff$ A est un corps.
4. a premier non nul $\implies$ a irréductible.
5. (a) maximal non nul $\implies$ a irréductible.

Proposition

1. *Si de plus, A possède la propriété de Gauss :*

$$(\forall a \in A \setminus \{0\}) \qquad a \text{ premier} \iff a \text{ irréductible}$$

2. *Si A est principal :*

$$(\forall a \in A \setminus \{0\}) \qquad (a) \text{ maximal} \iff a \text{ irréductible}$$

Démonstration : (exercices). □

6. A euclidien $\Longrightarrow$ A principal

Théorème

$$A \text{ euclidien} \implies A \text{ principal}$$

Démonstration : Soient A euclidien de stathme δ et I idéal de A.

- Si $I = (0)$, il est (évidemment) principal.
- Sinon, il existe $\alpha \in I \setminus \{0\}$ tel que $\delta(\alpha)$ minimal. Montrons que $I = (\alpha)$:

$$(\forall x \in I)(\exists (q,r) \in A \times A) \quad \begin{cases} x = \alpha * q + r \\ r = 0 \ \text{ ou } \delta(r) < \delta(\alpha) \end{cases}$$

Comme $r = x - \alpha * q \in I$ et $\delta(\alpha)$ minimal, on doit avoir $r = 0$. □

7. A principal $\Longrightarrow$ A factoriel

Soit $(A, +, 0, *, e)$ un anneau principal.

Lemme

Toute suite croissante d'idéaux de A est stationnaire.

Démonstration : Soit $(a_0) \subset (a_1) \subset \cdots$ une telle suite. $\bigcup_{n\in\mathbb{N}}(a_n)$ est un idéal de A (exercice). Donc $\bigcup_{n\in\mathbb{N}}(a_n) = (\alpha)$ et il existe $N \in \mathbb{N}$ tel que $(\forall n \geq N) \quad (a_n) = (\alpha)$. □

Corollaire

Pour tout $a \in A$, $a \neq 0$, $a \notin A^*$, on a l'alternative :

- *soit a irréductible ;*
- *soit $a = p * b$ avec p irréductible et $b \notin A^*$.*

Démonstration : exercice. □

A principal $\Longrightarrow$ A factoriel

Théorème

$$A \textit{ principal} \implies A \textit{ factoriel}$$

Démonstration :

• existence de la décomposition en irréductibles : par le lemme précédent et son corollaire.

• unicité à équivalence près : soient deux décompositions de a en irréductibles, $a = u * p_1^{\alpha_1} * \cdots * p_n^{\alpha_n}$ et $a = v * q_1^{\beta_1} * \cdots * q_m^{\beta_m}$. Par récurrence sur $l = n + m$ et en utilisant le lemme de Gauss (possible car principal $\Longrightarrow$ Bézout $\Longrightarrow$ Gauss), on montre qu'elles sont équivalentes (exercice).

□

8. A corps $\iff$ $A[X]$ principal

Théorème

$$A \text{ corps} \iff A[X] \text{ principal}$$

Démonstration :
($\Longrightarrow$) si A est un corps, $A[X]$ est euclidien, donc principal.
($\Longleftarrow$) si $A[X]$ est principal, il est intègre, donc A est aussi intègre. X est donc irréductible.
Comme $A[X]$ est principal, (X) est maximal et donc $A[X]/(X)$ est un corps.
Par ailleurs, $A[X]/(X)$ est isomorphe à A.

□

Corollaire

$$A \text{ corps} \iff A[X] \text{ euclidien}$$

Exemple : $\mathbb{Z}[X]$ n'est ni euclidien, ni principal.

9. A factoriel $\Longrightarrow$ $A[X]$ factoriel

Soit $(A, +, 0, *, e)$ un anneau factoriel.
Pour tout $P \in A[X]$, $P \neq 0$, on définit son contenu, noté $c(P)$, par

$$P = \sum_{k=0}^{\deg(P)} a_k X^k \quad \Longrightarrow \quad c(P) \overset{\text{déf}}{=} \operatorname{pgcd}(a_0, \ldots, a_{\deg(P)})$$

P est dit primitif si $c(P) \sim e$.

Lemme (Gauss)

$$(\forall P, Q \in A[X] \setminus \{0\}) \qquad c(PQ) \sim c(P) * c(Q)$$

Démonstration : exercice. □

Les irréductibles de $A[X]$

Proposition (irréductibles de $A[X]$ lorsque A est factoriel)

Lorsque A est factoriel, les irréductibles de $A[X]$ sont

1. *les irréductibles de A ;*
2. *les polynômes $P \in A[X]$, $\deg(P) \geq 1$, primitifs et irréductibles dans $Frac(A)[X]$.*

Démonstration : exercice. □

Théorème (Gauss)

$$A \text{ factoriel} \implies A[X] \text{ factoriel}$$

Démonstration : utilise le fait que $\mathrm{Frac}(A)[X]$ est factoriel (car euclidien). □