HAX501X – Groupes et anneaux 1

CM17 07/12/2023

Clément Dupont

Divisiblité dans un anneau intègre

Soit A un anneau intègre (et donc notamment commutatif).

Définition

Soient $a, b \in A$. On dit que a **divise** *b et on écrit*

$$a|b$$

s'il existe $c \in A$ tel que $b = ac$.

Proposition

On a :

$$a|b \quad \Longleftrightarrow \quad b \in (a) \quad \Longleftrightarrow \quad (b) \subset (a)\ .$$

Éléments associés

Définition

Soient $a, b \in A$. *On dit que* a *et* b *sont* **associés** *s'il existe un inversible* $u \in A^\times$ *tel que* $b = au$.

Proposition

Soient $a, b \in A$. *On a :*

$$a \text{ et } b \text{ associés} \iff a|b \text{ et } b|a \iff (a) = (b) .$$

De plus, la relation d'association ("être associés") est une relation d'équivalence sur A.

Éléments irréductibles

Définition
On dit qu'un élément $x \in A$ non nul est **irréductible** *si x n'est pas inversible et qu'on ne peut pas écrire $x = ab$ avec a et b non inversibles.*

Exercice 80
Dans un corps, quels éléments sont irréductibles ?

- Il n'y en a aucun car un élément d'un corps est soit nul soit inversible.

PGCD dans un anneau principal

On fixe A un anneau **principal** (donc notamment intègre).

Définition

Soit A un anneau principal et soient $a, b \in A$. On dit qu'un élément $d \in A$ est **un PGCD** *de a et b si $(a, b) = (d)$.*

Proposition

Soient $a, b \in A$. Alors $a \wedge b$ est l'unique (à association près) $d \in A$ qui vérifie les deux conditions suivantes.

1) *$d|a$ et $d|b$;*
2) *pour tout $e \in A$, $(e|a$ et $e|b) \Longrightarrow e|d$.*

Proposition

Soient $a, b, c \in A$. Alors à association près on a $(a + bc) \wedge b = a \wedge b$.

- Dans le cas où A est un anneau euclidien, cette proposition implique qu'on peut calculer $a \wedge b$ grâce à l'**algorithme d'Euclide**.

PPCM dans un anneau principal

Définition

Soit A un anneau principal et soient $a, b \in A$. On dit qu'un élément $m \in A$ est **un PPCM** *de a et b si $(a) \cap (b) = (m)$.*

Proposition

Soient $a, b \in A$. Alors $a \vee b$ est l'unique (à association près) $m \in A$ qui vérifie les deux conditions suivantes.

1) *$a|m$ et $b|m$;*
2) *pour tout $n \in A$, $(a|n$ et $b|n) \Longrightarrow m|n$.*

Gauss, Euclide, Bézout

On laisse au lecteur le soin de démontrer, en copiant les preuves du chapitre 1, que dans un anneau principal A ou a les théorèmes classiques suivants :

- le lemme de Gauss (et sa variante) ;
- le lemme d'Euclide ;
- le théorème de Bézout ;

Le théorème de factorisation en produit d'éléments irréductibles est aussi vrai, mais un peu plus subtil, comme on va le voir maintenant.

Anneau factoriel

Définition

Soit A un anneau intègre. On dit que A est un anneau **factoriel** *s'il y a existence et unicité de la décomposition en produit d'irréductibles dans A, c'est-à-dire plus précisément si :*

(1) *pour tout $a \in A \setminus \{0\}$ il existe un nombre fini $x_1, \ldots, x_r$ d'éléments irréductibles de A et un inversible $u \in A^\times$ tels que $a = u\, x_1 \cdots x_r$;*

(2) *si pour $a \in A \setminus \{0\}$ on a des écritures $a = u\, x_1 \cdots x_r$ et $a = v\, y_1 \cdots y_s$ avec les x_i, y_j irréductibles et u, v inversibles alors $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ et des éléments inversibles $u_i \in A^\times$ tels que $y_i = u_i x_{\sigma(i)}$ pour tout $i = 1, \ldots, r$.*

Principal implique factoriel

On va prouver le théorème suivant.

Théorème
Tout anneau principal est factoriel.

- On laisse au lecteur le soin de prouver la partie (2) de la définition (unicité) en utilisant le lemme d'Euclide, comme dans le cas de $\mathbb{Z}$ et de $K[X]$.
- La partie subtile concerne la partie (1), c'est-à-dire l'**existence** de la factorisation en produit d'éléments irréductibles dans un anneau principal.

Remarque
La réciproque de ce théorème est fausse, comme on va le voir dans le prochain paragraphe. En effet, on verra que les anneaux $\mathbb{Z}[X]$ et $K[X,Y]$, pour K un corps, sont factoriels, alors qu'il ne sont pas principaux (voir TD). Pour résumer, on a donc les implications suivantes, qui ne sont pas des équivalences :

$$\text{euclidien} \Longrightarrow \text{principal} \Longrightarrow \text{factoriel.}$$

Suites croissantes d'idéaux

Proposition

Soit A *un anneau principal. Soit* $(I_n)_{n\in\mathbb{N}}$ *une suite d'idéaux de* A *tels que* $I_n \subset I_{n+1}$ *pour tout* n*. Alors cette suite est stationnaire : il existe un* $N \in \mathbb{N}$ *tel que pour tout* $n \geqslant N$*,* $I_n = I_N$*.*

- Cette condition dit qu'il ne peut pas y avoir de suite strictement croissante d'idéaux de A.
- Cette condition s'appelle la **condition de chaîne ascendante** et un anneau qui satisfait cette propriété est appelé **noethérien**.
- On vient donc de montrer que tout anneau principal est noethérien.
- Un exemple d'un anneau non noethérien : un anneau de polynômes sur une infinité de variables $K[X_1, X_2, X_3, \ldots]$: la suite d'idéaux $I_n = (X_1, \ldots, X_n)$ est strictement croissante.

Emmy Noether (1882-1935)

Existence de la décomposition en produit d'irréductibles

Théorème
Soit A un anneau principal. Alors pour tout élément $a \in A \setminus \{0\}$ il existe un nombre fini $x_1, \ldots, x_r$ d'éléments irréductibles de A et un inversible $u \in A^\times$ tels que $a = u\, x_1 \cdots x_r$.

Divisibilité dans un anneau factoriel

- A désigne un anneau **factoriel** (et donc notamment intègre).
- On fait un choix, pour simplifier les notations, d'un élément irréductible p_i dans chaque classe d'association, pour i dans un certain ensemble d'indices $\mathcal{I}$.
- Un élément $a \neq 0$ dans A a donc une écriture **unique** sous la forme

$$a = u \prod_{i \in \mathcal{I}} p_i^{m_i}$$

avec u inversible et les $m_i \in \mathbb{N}$ presque tous nuls (tous nuls sauf un nombre fini).

Proposition

Soient deux éléments $a, a' \in A \setminus \{0\}$ *écrits comme ci-dessus*

$$a = u \prod_{i \in \mathcal{I}} p_i^{m_i} \quad \textit{et} \quad a' = u' \prod_{i \in \mathcal{I}} p_i^{m'_i}.$$

Alors on a :

$$a | a' \iff \forall i \in \mathcal{I},\ m_i \leqslant m'_i.$$

PGCD et PPCM dans un anneau factoriel

Soient $a, b \in A$ non nuls, écrits sous la forme ci-dessus,

$$a = u \prod_{i \in \mathcal{I}} p_i^{m_i} \qquad \text{et} \qquad b = v \prod_{i \in \mathcal{I}} p_i^{n_i}.$$

Définition

On définit le **PGCD** *de* a *et* b*, noté* $\mathrm{PGCD}(a, b)$ *ou* $a \wedge b$*, par la formule*

$$a \wedge b = \prod_{i \in \mathcal{I}} p_i^{\min(m_i, n_i)}.$$

On définit le **PPCM** *de* a *et* b*, noté* $\mathrm{PPCM}(a, b)$ *ou* $a \vee b$*, par la formule*

$$a \vee b = \prod_{i \in \mathcal{I}} p_i^{\max(m_i, n_i)} \; .$$

Propriétés du PGCD et du PPCM

Proposition

Soient $a, b \in A \setminus \{0\}$. Alors $a \wedge b$ est l'unique (à association près) $x \in A$ qui vérifie les deux conditions suivantes.

1) $x|a$ *et* $x|b$;
2) *pour tout* $y \in A$, $(y|a$ *et* $y|b) \Longrightarrow y|x$.

Proposition

Soient $a, b \in A \setminus \{0\}$. Alors $a \vee b$ est l'unique (à association près) $x \in A$ qui vérifie les deux conditions suivantes.

1) $a|x$ *et* $b|x$;
2) *pour tout* $y \in A$, $(a|y$ *et* $b|y) \Longrightarrow x|y$.

Proposition

Les produits

$$ab \qquad \text{et} \qquad (a \wedge b)(a \vee b)$$

sont associés dans A.

Éléments premiers entre eux

Définition

On dit que a et b sont **premiers entre eux** *si $a \wedge b = 1$.*

- Cela revient à dire qu'il n'y a aucun élément irréductible qui divise à la fois a et b. C'est aussi équivalent à dire que les seuls diviseurs communs à a et b sont les éléments inversibles de A.

Remarque

Il y a tout de même un résultat très utile en arithmétique qui est vrai dans un anneau principal mais pas dans tout anneau factoriel : le théorème de Bézout !

Hérédité de la factorialité

But de la fin du cours : démontrer le théorème suivant.

Théorème

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

Corollaire

Soit A un anneau factoriel (par exemple $A = \mathbb{Z}$ ou $A = K$ un corps). Alors pour tout entier n, l'anneau $A[X_1, \ldots, X_n]$ est factoriel.

Démonstration. Par récurrence : $A[X_1, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n]$. $\square$

Remarque

Les anneaux $\mathbb{Z}[X]$ et $K[X, Y]$, pour K un corps, ne sont pas principaux (voir TD). Ce sont donc des exemples d'anneaux factoriels non principaux.