HAX501X – Groupes et anneaux 1

CM18 08/12/2023

Clément Dupont

10. Arithmétique dans un anneau factoriel

10.2 Hérédité de la factorialité

10. Arithmétique dans un anneau factoriel

10.2 Hérédité de la factorialité

Rappel : définition d'un 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 $i = 1, \ldots, r$.*

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.

Le programme d'aujourd'hui

- Pour plus de clarté, on va seulement prouver le théorème dans le cas $A = \mathbb{Z}$

Théorème
L'anneau $\mathbb{Z}[X]$ *est factoriel.*

- On rappelle les inversibles de $\mathbb{Z}[X]$:

$$\mathbb{Z}[X]^\times = \mathbb{Z}^\times = \{-1, 1\}.$$

- On va se servir de la connaissance de $\mathbb{Q}[X]$, qui est un anneau factoriel.
- Attention :

le polynôme $2X - 4 \in \mathbb{Q}[X]$ est irréductible (car de dégré 1)

mais

le polynôme $2X - 4 \in \mathbb{Z}[X]$ n'est pas irréductible car il s'écrit $2 \times (X - 2)$, et ni 2 ni $X - 2$ ne sont inversibles dans $\mathbb{Z}[X]$.

Contenu, polynômes primitifs

Définition

Le **contenu** *d'un polynôme*

$$f = \sum_{n=0}^{N} a_n X^n \ \in \mathbb{Z}[X]$$

est le PGCD des coefficients a_n. On le note $c(f)$. On dit que f est **primitif** *si $c(f) = 1$, c'est-à-dire si les coefficients de f sont premiers entre eux dans leur ensemble.*

Exercice 81

1) Montrer qu'on peut écrire $f = c(f)f_1$ avec $f_1 \in \mathbb{Z}[X]$ primitif.
2) Réciproquement, si on a $f = \lambda f_1$ avec $\lambda \in \mathbb{N}$ et $f_1 \in \mathbb{Z}[X]$ primitif, montrer que $c(f) = \lambda$.

Existence de la décomposition en produit d'irréductibles

- Cette fois c'est l'existence de la décomposition en produit d'irréductibles qui est la plus facile.

Proposition

Tout $f \in \mathbb{Z}[X] \setminus \{0\}$ *peut s'écrire (au signe près) comme un produit d'irréductibles de* $\mathbb{Z}[X]$.

Réduction modulo p

- On passe maintenant à l'unicité de la décomposition en produit d'irréductibles dans $\mathbb{Z}[X]$.
- Avant de continuer, une remarque sera utile. Pour un polynôme

$$f = \sum_{n=0}^{N} a_n X^n \ \in \mathbb{Z}[X]$$

et pour un nombre premier fixé p, on peut réduire tous les coefficients de f modulo p et obtenir un polynôme

$$\overline{f} = \sum_{n=0}^{N} \overline{a_n} X^n \ \in (\mathbb{Z}/p\mathbb{Z})[X]$$

à coefficients dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 82
Montrer que cette opération définit un morphisme d'anneaux

$$\mathbb{Z}[X] \longrightarrow (\mathbb{Z}/p\mathbb{Z})[X] \ , \ \ f \mapsto \overline{f} \ .$$

Montrer que ce morphisme est surjectif et décrire son noyau.

Le lemme de Gauss

- La proposition suivante s'appelle "lemme de Gauss", mais n'a pas vraiment de rapport avec l'autre lemme de Gauss de ce cours.

Proposition (Lemme de Gauss)

Pour $f, g \in \mathbb{Z}[X]$ *on a*

$$c(fg) = c(f)c(g) \ .$$

En particulier, le produit de deux polynômes primitifs est primitif.

Irréductibles de $\mathbb{Z}[X]$

Proposition

Un polynôme non constant $f \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il est primitif et irréductible dans $\mathbb{Q}[X]$.

Remarque

La partie "non triviale" de la proposition pécédente est l'implication

$$(\text{irréductible dans } \mathbb{Z}[X]) \Longrightarrow (\text{irréductible dans } \mathbb{Q}[X]).$$

En pratique, c'est cette implication qui est utile. En effet, il est (de manière peut-être surprenante) plus facile de montrer qu'un polynôme à coefficients **entiers** est irréductible, notamment parce qu'on peut alors réduire les coefficients modulo un nombre premier p bien choisi.

Corollaire

Les irréductibles de $\mathbb{Z}[X]$ sont les nombres premiers (et leurs opposés) et les polynômes primitifs qui sont irréductibles dans $\mathbb{Q}[X]$.

Le lemme d'Euclide dans $\mathbb{Z}[X]$

Proposition (Lemme d'Euclide pour les polynômes à coefficients dans $\mathbb{Z}$)

Soient $f, g \in \mathbb{Z}[X]$, et $h \in \mathbb{Z}[X]$ irréductible. Si $h|fg$ alors $h|f$ ou $h|g$.

Unicité de la décomposition en produit d'irréductibles

Proposition

Dans $\mathbb{Z}[X]$ la décomposition en produit d'irréductibles est unique au signe près et à l'ordre des facteurs près.

Démonstration. En utilisant le lemme d'Euclide (proposition précédente) comme dans le cas de $\mathbb{Z}$. $\square$

- On a fini : on a montré que $\mathbb{Z}[X]$ est un anneau factoriel.