HAX501X – Groupes et anneaux 1

CM14 23/11/2023

Clément Dupont

Définition

On se contente ici de considérer des polynômes dont les coefficients sont pris dans un **anneau commutatif** R.

Définition

Soit R un anneau commutatif. Un polynôme à une indéterminée à coefficients dans R est une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de R qui est nulle à partir d'un certain rang (il existe un $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, $a_n = 0$). On le note comme la combinaison linéaire

$$f = \sum_{n=0}^{N} a_n X^n \ ,$$

où l'indéterminée X est un symbole formel.

- L'ensemble des polynômes à coefficients dans R est noté $R[X]$ et est muni d'une structure d'anneau (commutatif).
- On voit R comme un sous-anneau de $R[X]$, qui consiste en les polynômes constants.

Degré

Exercice 71
Lister les polynômes de degré $\leqslant 3$ à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. Même chose pour $\mathbb{Z}/3\mathbb{Z}$.

Il y a $16 = 2^4$ polynômes de degré $\leqslant 3$ à coefficients dans $\mathbb{Z}/2\mathbb{Z}$:

- Degré $-\infty$: $\overline{0}$.
- Degré 0 : $\overline{1}$.
- Degré 1 : X, $X + \overline{1}$.
- Degré 2 : X^2, $X^2 + \overline{1}$, $X^2 + X$, $X^2 + X + \overline{1}$.
- Degré 3 : X^3, $X^3 + \overline{1}$, $X^3 + X$, $X^3 + X + \overline{1}$, $X^3 + X^2$, $X^3 + X^2 + \overline{1}$, $X^3 + X^2 + X$, $X^3 + X^2 + X + \overline{1}$.

Il y a $81 = 3^4$ polynômes de degré $\leqslant 3$ à coefficients dans $\mathbb{Z}/3\mathbb{Z}$...

Degré, et conséquences

Proposition

Soit R un anneau intègre. Pour $f, g \in R[X]$ on a :

$$\deg(fg) = \deg(f) + \deg(g).$$

Proposition

Si R est un anneau intègre alors $R[X]$ est aussi un anneau intègre.

Proposition

Soit R un anneau intègre. Les inversibles de $R[X]$ sont les polynômes constants inversibles dans R :

$$R[X]^\times = R^\times.$$

Fonction polynomiale

- À un polynôme $f \in R[X]$ on associe la **fonction polynomiale** correspondante, qu'on note par le même symbole
$$f : R \to R\ ,\ x \mapsto f(x).$$
- Elle est définie, pour $f = \sum_{n=0}^{N} a_n X^n$, par $f(x) = \sum_{n=0}^{N} a_n x^n$.
- Noter que la première somme est une somme "formelle" qui est juste une notation pour les polynômes, alors que la deuxième somme est une vraie somme dans l'anneau R. (Évidemment, la notation pour les polynômes est choisie pour imiter la notation pour les fonctions polynomiales...)

Attention : polynômes vs fonctions polynomiales

- Soit p un nombre premier et considérons le polynôme

$$X^p - X \ \in \ (\mathbb{Z}/p\mathbb{Z})[X].$$

- Ce polynôme n'est pas nul (il est de degré p) mais la fonction polynomiale associée est nulle par le petit théorème de Fermat :

$$\forall x \in \mathbb{Z}/p\mathbb{Z},\, x^p - x = \overline{0}.$$

- Il est donc important, en général, de faire la distinction entre polynôme et fonction polynomiale.

- On verra ci-dessous que si R est un **corps infini** alors il n'y a pas de risque à confondre polynôme et fonction polynomiale.

Polynômes à plusieurs indéterminées

- On peut aussi définir des anneaux de polynômes avec un nombre r d'indéterminées $X_1, \ldots, X_r$ à coefficients dans un anneau commutatif R, notés $R[X_1, \ldots, X_r]$.
- Un élément de cet anneau est une application $\mathbb{N}^r \to R \ , \ (n_1, \ldots, n_r) \mapsto a_{n_1, \ldots, n_r}$ telle que $a_{n_1, \ldots, n_r} \neq 0$ seulement pour un nombre fini de multi-indices $(n_1, \ldots, n_r)$. On le représente par la combinaison linéaire **finie** :

$$f = \sum_{(n_1, \ldots, n_r) \in \mathbb{N}^r} a_{n_1, \ldots, n_r} X_1^{n_1} \cdots X_r^{n_r} \ .$$

- Les lois $+$ et $\times$ sont définies de manière évidente.
- On note que les indéterminées commutent deux à deux : $X_i X_j = X_j X_i$ et que l'anneau $R[X_1, \ldots, X_r]$ est commutatif.

Exercice 72
Dans l'anneau $(\mathbb{Z}/3\mathbb{Z})[X, Y]$, développer $(X + \overline{2}Y)^3$.

Deux remarques

Remarque

On a un isomorphisme d'anneaux naturel

$$R[X,Y] \simeq (R[X])[Y]$$

qui consiste à voir un polynôme en deux indéterminées X, Y comme un polynôme en une indéterminée Y dont les coefficients sont des polynômes en X. Plus généralement on a un isomorphisme d'anneaux naturel $R[X_1, \ldots, X_r] \simeq (R[X_1, \ldots, X_{r-1}])[X_r]$. Cette remarque permet parfois de prouver des propriétés des anneaux de polynomes à **plusieurs** indéterminées en se ramenant par récurrence au cas d'une seule indéterminée.

Remarque

On peut définir des anneaux de polynômes avec un ensemble quelconque (notamment infini) d'indéterminées ; dans ce cas, chaque polynôme donné ne fait intervenir qu'un nombre **fini** d'indéterminées.

Algèbre sur un corps

Définition
*Soit K un corps. Une K-***algèbre** *(ou* **algèbre sur** *K) est un quadruplet $(A, +, ., \times)$ où :*

(1) $(A, +, .)$ *est un K-espace vectoriel ;*

(2) $(A, +, \times)$ *est un anneau ;*

(3) *les lois . et $\times$ sont compatibles :*
$\forall a, b \in K\,,\ \forall x, y \in A\,,\ (a.x) \times (b.y) = (ab).(x \times y).$

Des exemples de K-algèbres :

- Le corps K lui-même est une K-algèbre.
- On a l'algèbre $K^{\mathbb{N}}$ des suites d'éléments de K.
- L'anneau de polynômes $K[X]$ est une K-algèbre.
- L'anneau des matrices $\mathrm{M}_n(K)$ est une K-algèbre (non commutative si $n \geqslant 2$).
- Pour V un K-espace vectoriel on a la K-algèbre des endomorphismes K-linéaires de V, notée $\mathrm{End}(V)$, non commutative si $\dim(V) \geqslant 2$.

Corps des fractions d'un anneau intègre

- Soit A un anneau intègre. On veut se donner la possibilité de considérer des "fractions" d'éléments de A.
- On définit pour cela sur l'ensemble $A \times A \backslash \{0\}$ la relation :

$$(a,b) \sim (a',b') \iff ab' = a'b \ .$$

- L'intuition qu'il faut avoir est que le couple (a,b) va jouer le rôle de la fraction $\frac{a}{b}$; de ce point de vue-là cette relation est naturelle puisqu'on a envie de considérer que $\frac{a}{b}$ et $\frac{a'}{b'}$ sont le même élément si $ab' = a'b$.

Proposition

La relation $\sim$ sur $A \times A \backslash \{0\}$ est une relation d'équivalence.

- On note $\mathrm{Frac}(A)$ le quotient de $A \times A \backslash \{0\}$ par la relation d'équivalence $\sim$.
- On note $\frac{a}{b}$ la classe d'équivalence d'un couple (a,b) dans $\mathrm{Frac}(A)$.

Structure de corps sur $\mathrm{Frac}(A)$

Proposition

Les formules

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \textit{et} \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

définissent des lois de composition internes sur $\mathrm{Frac}(A)$*, qui font de* $\mathrm{Frac}(A)$ *un corps.*

Définition

On appelle $\mathrm{Frac}(A)$ *le* **corps des fractions** *de l'anneau intègre* A*.*

- Dans le cas $A = \mathbb{Z}$ on retrouve le corps $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.
- Dans le cas $A = K[X]$, avec K un corps, on retrouve le corps $\mathrm{Frac}(K[X]) = K(X)$, le corps des fractions rationnelles en une indéterminée à coefficients dans K.
- On a plus généralement le corps des fractions rationnelles en plusieurs indéterminées $K(X_1, \ldots, X_r) = \mathrm{Frac}(K[X_1, \ldots, X_r])$.

Intersection de sous-anneaux

Proposition

Soit A un anneau, soit $(B_i)_{i \in I}$ une famille de sous-anneaux de A indexée par un ensemble I. Alors l'intersection

$$B = \bigcap_{i \in I} B_i$$

est un sous-anneau de A.

On rappelle la définition :

$$\bigcap_{i \in I} B_i = \{x \in A \mid \forall i \in I, \, x \in B_i\}.$$

- Notamment, si B et B' sont deux sous-anneaux de A, alors l'intersection $B \cap B'$ est un sous-anneau de A.

Sous-anneau engendré par une partie

Soit A un anneau et soit $S \subset A$ un sous-ensemble (pas nécessairement un sous-anneau).

Définition

Le **sous-anneau de A engendré par** S*, noté* $\langle S \rangle$*, est l'intersection de tous les sous-anneaux de* A *qui contiennent* S*.*

Remarque

La notation $\langle \cdots \rangle$ dépend donc du contexte : sous-groupe engendré par une partie, ou sous-anneau engendré par une partie.

C'est bien un sous-anneau de A par la proposition précédente. On a clairement $S \subset \langle S \rangle$, et pour tout sous-anneau B de A on a l'équivalence :

$$S \subset B \iff \langle S \rangle \subset B.$$

On dit donc que $\langle S \rangle$ est le plus petit (pour l'inclusion) sous-anneau de A qui contient S.

Sous-anneau engendré par une partie... concrètement

Proposition

Le sous-anneau $\langle\, S \,\rangle$ est l'ensemble des éléments de A qu'on peut obtenir en faisant des combinaisons $\mathbb{Z}$-linéaires de produits d'éléments de S, c'est-à-dire l'ensemble des sommes

$$\sum_{i=1}^{N} n_i \, x_{i,1} x_{i,2} \cdots x_{i,r_i}$$

avec $N \in \mathbb{N}$, les $n_i \in \mathbb{Z}$, les $r_i \in \mathbb{N}$ et les $x_{i,j} \in S$.

Ici on prend les conventions qu'une somme indexée par l'ensemble vide dans un anneau A est égale à 0_A, et qu'un produit indexé par l'ensemble vide dans un anneau A est égal à 1_A.

Cas particuliers

- Lorsque $S = \{s_1, \ldots, s_k\}$ est finie, on note simplement.

$$\langle\, S \,\rangle = \langle\, s_1, \ldots, s_k \,\rangle.$$

- La description est particulièrement simple quand il y a un seul générateur.

Proposition

Soit A un anneau, soit $s \in A$. Alors le sous-anneau de A engendré par s a la description concrète suivante :

$$\langle\, s \,\rangle = \left\{ \sum_{i=0}^{N} a_i s^i \,,\, N \in \mathbb{N},\, a_0, \ldots, a_N \in \mathbb{Z} \right\}.$$

Divisibilité

On se place dans $K[X]$, avec K un corps.

Définition
Soient $f, g \in K[X]$. On dit que f **divise** *g et on note*

$$f|g$$

s'il existe $h \in K[X]$ tel que $g = fh$.

- Si $f|g$ et $g \neq 0$ alors $\deg(f) \leqslant \deg(g)$.
- $(f|g \text{ et } g|f) \iff \exists\, a \in K^*,\ f = ag$.

Polynômes irréductibles

Définition

Un polynôme $f \in K[X]$ est dit **irréductible** *s'il n'est pas constant et que ses seuls diviseurs sont tous de la forme $a \in K^*$ ou af avec $a \in K^*$.*

- Dit autrement, f est irréductible si f n'est pas constant et que pour tous $g, h \in K[X]$,
$$f = gh \quad \Longrightarrow \quad g \in K^* \text{ ou } h \in K^*.$$
- Tout polynôme f de degré 1 est irréductible.

Remarque

- Dans $\mathbb{C}[X]$, les polynômes irréductibles sont les polynômes de degré 1.
- Dans $\mathbb{R}[X]$, les polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant < 0 (c'est-à-dire de la forme $aX^2 + bX + c$ avec $b^2 - 4ac < 0$).
- Dans $\mathbb{Q}[X]$ il existe des polynômes irréductibles de n'importe quel degré. Par exemple on peut montrer que le polynôme $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$ pour tout $n \in \mathbb{N}^*$.

Division euclidienne

Théorème

Soit $f \in K[X]$ *et* $g \in K[X] \setminus \{0\}$*. Alors il existe des polynômes* $q, r \in K[X]$ *avec* $\deg(r) < \deg(g)$ *tels que*

$$f = gq + r \ .$$

Le couple (q, r) *est unique.*

Exercice 73

Dans $\mathbb{R}[X]$, calculer la division euclidienne de $X^4 - X^2 + 7$ par $X^2 + X + 1$.

Le cas d'une racine

Définition

Soit $f \in K[X]$*. On dit que* $a \in K$ *est une* **racine** *de* f *si* $f(a) = 0$*.*

Proposition

Soit $f \in K[X]$*. On a l'équivalence :*

$$f(a) = 0 \iff (X - a) \mid f.$$

Démonstration. Considérer la division euclidienne de f par $X - a$. □

Remarque

La proposition précédente est vraie même si l'on remplace K par n'importe quel anneau commutatif R (pouvez-vous le montrer ?). Ce n'est pas le cas de la proposition suivante.

Le cas de plusieurs racines

Proposition

Soit $f \in K[X]$*, et soient* $a_1, \ldots, a_n$ *des éléments deux à deux distincts de* K*. On a l'équivalence :*

$$f(a_1) = \cdots = f(a_n) = 0 \iff (X - a_1)\cdots(X - a_n) \mid f.$$

Démonstration. Par récurrence sur n en utilisant la proposition précédente. □

Proposition

Un polynôme $f \in K[X]$ *non nul de degré* $\leqslant n$ *a au plus* n *racines.*

Démonstration. Si f a $n+1$ racines $a_1, \ldots, a_{n+1}$ deux à deux distinctes, alors par la proposition précédente, $(X - a_1)\cdots(X - a_{n+1})$ divise f, et donc comme f est non nul, f est de degré $\geqslant n+1$. C'est impossible : contradiction. □

Warning

Remarque

La proposition précédente est fausse pour les polynômes à coefficients dans un anneau (commutatif) général.

- Par exemple, le polynôme $X^2 - X \in (\mathbb{Z}/6\mathbb{Z})[X]$ a 4 racines : $\overline{0}$, $\overline{1}$, $\overline{3}$, $\overline{4}$.

Exercice 74

Vérifier que dans $(\mathbb{Z}/6\mathbb{Z})[X]$ le polynôme $X^2 - X$ est divisible par X, par $X - \overline{1}$, par $X - \overline{3}$, et par $X - \overline{4}$. (Mais il n'est pas divisible par le produit de ces 4 polynômes !)

Polynômes vs fonctions polynomiales

Proposition

Supposons que K est infini. Soient $f, g \in K[X]$ telles que les fonctions polynomiales associées à f et g sont égales. Alors les polynômes f et g sont égaux.

Démonstration. Tous les éléments de K sont des racines de $f - g$. Comme K est infini, la proposition précédente implique que le polynôme $f - g$ est nul, et donc que $f = g$. $\square$

- Cela justifie que pour $K = \mathbb{R}$ ou $K = \mathbb{C}$ on se permette de ne pas faire de différence entre polynômes et fonctions polynomiales.

Remarque

La proposition précédente est fausse si le corps K est fini.

- Exemple : $K = \mathbb{Z}/p\mathbb{Z}$, $f = X^p$ et $g = X$.