HAX501X – Groupes et anneaux 1

CM15 24/11/2023

Clément Dupont

Divisibilité, polynômes irréductibles

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 $g = fh$.

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 $a \in K^*$.*

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 $X^2 + X + 1$.

Racines

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 :

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

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 :

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

Proposition

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

Idéal de $K[X]$

Définition

Un **idéal** *de $K[X]$ est un sous-ensemble $I \subset K[X]$ qui vérifie*

1) *I est un sous-groupe de $(K[X], +)$.*
2) *I est stable par multiplication par tout élément de $K[X]$: pour tout $f \in K[X]$, pour tout $g \in I$, $fg \in I$.*

Proposition

Soit $f \in K[X]$. Alors l'ensemble des multiples de f, noté

$$(f) = \{fg,\ g \in K[X]\},$$

est un idéal de $K[X]$.

Définition

On appelle (f) **l'idéal de $K[X]$ engendré par f.**

Idéaux et divisibilité

Proposition

Soient $f_1, f_2 \in K[X]$.

1) *On a*
$$(f_1) \subset (f_2) \iff f_2 | f_1.$$

2) *On a*
$$(f_1) = (f_2) \iff \exists\, a \in K^*,\ f_2 = a f_1.$$

Démonstration.

1) Supposons que $(f_1) \subset (f_2)$. Comme $f_1 = f_1 \times 1$, on a $f_1 \in (f_1)$ et donc $f_1 \in (f_2)$, d'où par définition $f_2 | f_1$. Réciproquement, supposons que $f_2 | f_1$, on peut donc écrire $f_1 = f_2 h$ avec $h \in K[X]$. Alors $(f_1) \subset (f_2)$ car pour tout $g \in K[X]$ on a $f_1 g = f_2(hg) \in (f_2)$.
2) Par 1), $(f_1) = (f_2)$ équivaut à : $f_1 | f_2$ et $f_2 | f_1$. C'est équivalent à : $\exists\, a \in K^*, f_2 = a f_1$.

□

Classification des idéaux de $K[X]$

Théorème
Soit I un idéal de $K[X]$. Alors il existe un polynôme $f \in K[X]$ tel que $I = (f)$.

- Par la proposition précédente, f n'est unique qu'à multiplication par un élément de K^* près.
- Si l'on demande que f soit unitaire, alors f devient unique.

Définition
Soit I un idéal de $K[X]$. L'unique polynôme f unitaire tel que $I = (f)$ est appelé le **générateur unitaire** *de I.*

Définition du PGCD

Proposition

Soient $f, g \in K[X]$. Alors l'ensemble

$$(f, g) = \{fu + gv,\ u, v \in K[X]\}$$

est un idéal de $K[X]$.

- On l'appelle l'**idéal de $K[X]$ engendré par f et g.**

Définition

Le générateur unitaire de (f, g) est appelé le **plus grand commun diviseur (PGCD)** *de f et g. On le note $\mathrm{PGCD}(f, g)$ ou $f \wedge g$.*

On a donc :

$$(f, g) = (f \wedge g).$$

Propriétés du PGCD

- On a la propriété importante, pour $f, g, h \in K[X]$:

$$(f + gh) \wedge g = f \wedge g.$$

- Cette propriété explique qu'on peut calculer le PGCD des polynômes par l'**algorithme d'Euclide**.

- On a aussi la proposition suivante qui explique la dénomination "plus grand commun diviseur".

Proposition

Soient $f, g \in K[X]$. Alors $f \wedge g$ est l'unique $h \in K[X]$ unitaire qui vérifie les deux conditions suivantes.

1) $h|f$ *et* $h|g$;
2) *pour tout* $k \in K[X]$, $(k|f$ *et* $k|g) \Longrightarrow k|h$.

Polynômes premiers entre eux

Définition
On dit que deux polynômes $f, g \in K[X]$ *sont* **premiers entre eux** *si* $f \wedge g = 1$.

- Cela revient à dire que les seuls diviseurs communs à f et g sont constants.

Exercice 74
Dans $\mathbb{R}[X]$, calculer le PGCD des polynômes $X^5 + 2X^4 - X^2 + 1$ et $X^4 - 1$.

Définition du PPCM

Proposition

Soient $f, g \in K[X]$. L'ensemble $(f) \cap (g)$ est un idéal de $K[X]$.

- On note que $(f) \cap (g)$ est l'ensemble des polynômes qui sont à la fois des multiples de f et de g.

Définition

Le générateur unitaire de $(f) \cap (g)$ est appelé le **plus petit commun multiple (PPCM)** *de f et g. On le note $\mathrm{PPCM}(f, g)$ ou $f \vee g$.*

- On a donc :

$$(f) \cap (g) = (f \vee g).$$

Le PPCM comme plus petit multiple commun

Proposition

Soient $f, g \in K[X]$. Alors $f \vee g$ est l'unique $h \in K[X]$ unitaire qui vérifie les deux conditions suivantes.

1) $f|h$ *et* $g|h$;
2) *pour tout* $k \in K[X]$, $(f|k$ *et* $g|k) \Longrightarrow h|k$.

Gauss etc.

On laisse au lecteur le soin d'énoncer et démontrer les analogues pour les polynômes des théorèmes classiques de l'arithmétique des entiers :

- le lemme de Gauss (et sa variante) ;
- le lemme d'Euclide ;
- le théorème de Bézout ;
- le théorème de factorisation en produit de polynômes irréductibles.

Exercice 75
Le faire en copiant les preuves du chapitre 1.

Exercice 76
Dans $\mathbb{R}[X]$, déterminer une relation de Bézout pour $X^5 + 2X^4 - X^2 + 1$ et $X^4 - 1$.

Définition d'un idéal

Dans toute cette section A est un anneau **commutatif**.

Définition

Un **idéal** *de A est un sous-ensemble $I \subset A$ qui vérifie :*

1) *I est un sous-groupe de $(A, +)$.*
2) *I est stable par multiplication par tout élément de A : pour tout $x \in I$, pour tout $a \in A$, $ax \in I$.*

On a déjà rencontré cette notion dans deux cas :

- Pour $A = \mathbb{Z}$, tout sous-groupe I de $\mathbb{Z}$ est automatiquement un idéal de $\mathbb{Z}$. En effet, pour tout $x \in I$ et pour tout $k \in \mathbb{Z}$, $kx \in I$. La notion d'idéal se confond donc (dans ce cas particulier) avec la notion de sous-groupe.
- Pour $A = K[X]$ avec K un corps, on a vu la notion d'idéal dans la section précédente.

Exemple

Exemples triviaux : $\{0\}$ et A sont des idéaux de A.

Warning

Remarque

Ne surtout pas confondre la notion d'idéal et la notion de sous-anneau, qui sont différentes et qui jouent des rôles très différents dans la théorie des anneaux. En général, un idéal I ne contient pas 1_A.

Exercice 77

Soit I un idéal de A. Montrer que $1_A \in I$ si et seulement si $I = A$.

Idéal engendré par des éléments

Proposition

Soient $x_1, \ldots, x_r \in A$. *Alors l'ensemble*

$$(x_1, \ldots, x_r) = \{a_1 x_1 + \cdots + a_r x_r,\ a_1, \ldots, a_r \in A\}$$

est un idéal de A. *Pour tout idéal* I *de* A *on a*

$$x_1, \ldots, x_r \in I \quad \Longleftrightarrow \quad (x_1, \ldots, x_r) \subset I.$$

Définition

On appelle $(x_1, \ldots, x_r)$ *l'***idéal de** A **engendré par** $x_1, \ldots, x_r$.

Idéaux et morphismes

Proposition

Soient A et B deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Alors $\ker(f)$ est un idéal de A.

Proposition

Soient A et B deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Soit J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A.

- Pour $J = \{0\}$ on retrouve le fait que $f^{-1}(\{0\}) = \ker(f)$ est un idéal de A.

Exercice 78

Montrer qu'en général l'image **directe** d'un idéal par un morphisme d'anneaux n'est pas un idéal.

Idéaux principaux

Le cas particulier des idéaux engendrés par un seul élément $x \in A$ est important :

$$(x) = \{ax,\ a \in A\}.$$

Définition
Un idéal (x) engendré par un seul élément est dit **principal**.

On a rencontré les idéaux principaux dans deux cas :

- Pour $A = \mathbb{Z}$ et $n \in \mathbb{Z}$ on a $(n) = n\mathbb{Z}$.
- Pour $A = K[X]$ avec K un corps, on a rencontré les idéaux principaux (f) dans la section précédente.

Dans les deux cas les idéaux principaux nous ont aidé à développer les notions de PGCD et de PPCM, et donc toute l'arithmétique.

Anneaux principaux

Définition

Soit A un anneau. On dit que A est **principal** *si A est intègre et que tout idéal de A est principal.*

- Les anneaux $\mathbb{Z}$ et $K[X]$, pour K un corps, sont principaux.
- On verra en TD que les anneaux $\mathbb{Z}[X]$ et $K[X,Y]$, pour K un corps, ne sont pas principaux.

Anneaux euclidiens

Définition

Soit A un anneau intègre. Une **jauge euclidienne** *est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ qui vérifie : pour tous $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ avec*

$$a = bq + r \quad \text{et} \quad (r = 0 \ \text{ ou } \ \nu(r) < \nu(b)) \ .$$

On appelle une telle identité une **division euclidienne** *de a par b pour la jauge euclidienne ν. On dit que A est un* **anneau euclidien** *s'il possède une jauge euclidienne.*

- Notons qu'on ne demande pas d'avoir unicité de la division euclidienne.

Exemple

- L'anneau $\mathbb{Z}$ est euclidien, une jauge euclidienne est donnée par la valeur absolue : $\nu(m) = |m|$. (On pourra remarquer que pour cette jauge euclidienne, il n'y a pas unicité de la division euclidienne.)
- L'anneau $K[X]$ est euclidien si K est un corps, une jauge euclidienne est donnée par le degré : $\nu(f) = \deg(f)$.

Euclidien implique principal

La proposition suivante est la version “abstraite” de deux énoncés importants qu'on a vus dans ce cours :

- $\mathbb{Z}$ est un anneau principal : tous les idéaux de $\mathbb{Z}$ sont de la forme (n). (C'est-à-dire : tous les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$.)
- Pour K un corps, $K[X]$ est principal : tous les idéaux de $K[X]$ sont de la forme (f).

C'est l'outil numéro un pour montrer qu'un anneau est principal.

Théorème
Tout anneau euclidien est principal.

- En TD on se servira de ce théorème pour montrer que l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est un anneau principal.

Remarques

Remarque

Il existe des anneaux principaux qui ne sont pas euclidiens, mais ce n'est pas si facile à prouver en pratique. On n'en verra pas en exercice. Pour votre culture, un exemple d'un tel anneau est le sous-anneau de $\mathbb{C}$ donné par

$$A = \left\{ a + b\frac{1+i\sqrt{19}}{2} \mid a, b \in \mathbb{Z} \right\} .$$

(Vérifiez que c'est bien un sous-anneau de $\mathbb{C}$: il y a un petit calcul à faire.)

Remarque

Les anneaux $\mathbb{Z}[X]$ et $K[X, Y]$, pour K un corps, ne sont pas principaux (voir TD). Ils ne sont donc pas euclidiens.