122 : Anneaux principaux. Applications.

111 [103]

Cadre : A anneau commutatif unitaire intègre

I Premières définitions, premier exemple

1) Définitions

[ESC]

déf 1 : Un idéal I de A est principal lorsqu'il est engendré par un unique élément $a \in A$, noté $I = (a)$.
A est principal lorsqu'il est intègre et que tous ses idéaux sont principaux.

ex 2 : $\mathbb{Z}$, $k[X]$ où k est un corps.

déf 3 : Soit I un idéal de A.

- I est premier si $I \subsetneq A$ et que $\forall x, y \in A$, $xy \in I \Rightarrow x \in I$ ou $y \in I$.
- I est maximal s'il est maximal au sens de l'inclusion parmi les idéaux stricts de A.

propo 4 : (Caractérisation) Soit I un idéal de A.

- I est premier ssi A/I est intègre.
- I est maximal ssi A/I est un corps.

Application 5 : - un idéal maximal est premier.
- idéaux premiers et maximaux de $\mathbb{Z}$.

déf 6 : • $a \in A$ est irréductible si $a \in A - (A^\times \cup \{0\})$ et que : $\forall b, c \in A$; $a = bc \Rightarrow b \in A^\times$ ou $c \in A^\times$.
• $a \in A$ est premier si $a \neq 0$ et que (a) est premier.

propo 7 : Dans un anneau intègre, premier $\Rightarrow$ irréductible

propo 8 : Dans un anneau principal, tout élément irréductible engendre un idéal maximal et est premier.

2) Un exemple important : les anneaux euclidiens

[PER]

déf 9 : A est euclidien s'il existe $j : A^* \to \mathbb{N}$ une fonction, dite jauge euclidienne, vérifiant :
$\forall (a,b) \in A \times A - \{0\}$, $\exists (q,r) \in A^2 \mid a = bq + r$ et $\begin{cases} r = 0 \\ j(r) < j(b) \end{cases}$ ou

ex 10 : $\mathbb{Z}[i]$, $\mathbb{Z}[X]$.

propo 11 : Un anneau euclidien est principal.

propo 12 : A euclidien. Il existe $x \in A - A^\times$ tel que, si $\pi : A \to A/(x)$ est la projection canonique, $\pi|_{A^\times \cup \{0\}}$ soit surjective.

[PER]

Application 13 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal non euclidien

théorème 14 $A[X]$ est principal ssi $A[X]$ est euclidien ssi A est un corps.

Rque 15 : Existence d'algorithme pour effectuer les calculs dans les anneaux euclidiens.

II Arithmétique dans les anneaux principaux

1) Divisibilité - PGCD - PPCM

[ESC]

déf 16 : Soient $a, b \in A$.

- $m \in A$ est un ppcm de a et b si $(a) \cap (b) = (m)$.
- $d \in A$ est un pgcd de a et b si $(a, b) = (d)$.

Rques 17 : - pgcd et ppcm sont définis à inversibles près.
- Si A est principal, on a toujours l'existence.
- généralisation à des familles finies.

[GO]

propo 18 : (Caractérisation) A principal, $a, b, d, m \in A$.
• $d = \text{pgcd}(a, b)$ ssi $\exists a', b', u, v \in A \mid d = au + bv$ et $a = da'$, $b = db'$.

• $m = \text{ppcm}(a,b)$ ssi $m = a'b'd$. On a $md = ab$.

<u>Application 19</u>: $\text{pgcd}(ka,kb) = k\,\text{pgcd}(a,b)$

<u>déf 20</u>: A principal. $a,b \in A$ sont dits <u>premiers entre eux</u> si 1 est un pgcd de a et b.

<u>Théorème de Bezout</u>: A principal. $a,b \in A$ $(a,b \neq 0)$ sont premiers entre eux ssi $\exists (u,v) \in A^2 \mid au + bv = 1$.

<u>Lemme de Gauss</u>: A principal, $a,b,c \in A - \{0\}$. Si a et b sont premiers entre eux et que $a \mid bc$ alors $a \mid c$.

<u>Application 21</u>: Il existe une infinité de nombres premiers.
· lemme des noyaux.

<u>Algorithme d'Euclide étendu</u>: A euclidien, $a,b \neq 0$. Par divisions euclidiennes successives, renvoie $d = \text{pgcd}(a,b)$ et $u,v \in A$ tels que $au + bv = d$

<u>Rque 22</u>: existence assurée dans un anneau principal, calcul effectif dans un anneau euclidien

2) Théorème chinois (ici, A principal) [...]

<u>Théorème chinois</u>: Soient $x,y \in A$ premiers entre eux. Alors $\varphi : \begin{cases} A/(xy) \to A/(x) \times A/(y) \\ y = \pi_{xy}(a) \mapsto \pi_x(a), \pi_y(a) \end{cases}$ est un isomorphisme d'anneaux.
(où π_* désigne la projection canonique $A \to A/(*)$.)

<u>Applications 23</u> • résolution de systèmes de congruences: $\begin{cases} a \equiv s \bmod x \\ a \equiv t \bmod y \end{cases}$ Solution: si $ux + vy = 1$, $\bar{x} \equiv s \bmod x$, $\bar{y} \equiv t \bmod y$ alors $a = ux\bar{y} + vy\bar{x}$ convient.

• Cryptosystème RSA

• Algorithme de Berlekamp pour la factorisation de polynômes.

3) Factorialité [PER]

<u>déf 24</u>: $a,b \in A$ sont <u>associés</u> si $a \mid b$ et $b \mid a$ $(\Leftrightarrow \exists u \in A^\times,\ a = bu)$ Notation : $a \sim b$.

• <u>Un système de représentants d'irréductibles</u> est un ensemble P d'irred tel que $\forall p$ irred, $\exists!\, q \in P$, $p \sim q$.

• A est <u>factoriel</u> si A est intègre et que $\forall a \in A \setminus \{0\}$, a s'écrit de façon unique $u \prod_{p \in P} p^{v_p(a)}$ $u \in A^\times$, $v_p(a) \in \mathbb{N}$ tous nuls sauf un nombre fini.

<u>prop 25</u>: Un anneau principal est factoriel.

<u>conseq</u>: décomposition unique selon le système

<u>ex 26</u>: nombres premiers dans $\mathbb{Z}$, polynômes unitaires irred dans $k[X]$.

III) Modules de type fini sur un anneau principal [OA]

ici, A est principal.

1) Théorèmes de structure

<u>Thm [Facteurs invariants]</u> Soit $U \in \mathcal{M}_{mn}(A)$ il existe $(d_1, \dots, d_s) \in A - \{0\}$ tels que $d_s \mid \dots \mid d_1$ et que U soit équivalente à $D = \begin{pmatrix} d_s & & & \\ & \ddots & & \\ & & d_1 & \\ & & & 0 \end{pmatrix}$.

<u>Rque</u>: preuve algorithmique dans le cas euclidien: algorithme des facteurs invariants (DVP)

<u>lemme</u>: Soit M un A-module libre de rang m, N un sous-module de M, alors N est libre de rang $\leq m$.

<u>Application 27</u>: [thm de la base adaptée] Mêmes notations. Il existe une base $(e_1, \dots, e_m)$ de M, $s \in [\![0,n]\!]$ et $(d_1, \dots, d_s) \in A - \{0\}$ tels que $d_s \mid \dots \mid d_1$ et $(d_1 e_1, \dots, d_s e_s)$ est une base de N.

<u>Rque</u>: version "faible" du théorème de la base incomplète

[COM]

[DA]

[DEM]

[PAP]

2) Applications

thm [Structure des groupes abéliens de type fini] Soit G un gpe abélien de type fini. Alors $G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r$ où $r, k \in \mathbb{N}$, $m_i | m_{i+1}$ entiers non nuls, ne dépendent que de G et sont dits invariants de G.

rque 28 : Soit k un corps, E un k-ev et $u \in \mathcal{L}(E)$. On peut munir E d'une structure de $k[X]$-module via
$P \cdot x = P(u)(x)$, $P \in k[X]$, $x \in E$. On la note (E, u).
Si $\dim E < +\infty$, (E, u) est de type fini.

déf/prop 29 : Mêmes notations : il existe une unique famille $(P_1, \dots, P_s)$ de polynômes unitaires tels que $P_s | \dots | P_1$ et $(E, u) \underset{k[X]\text{-mod}}{\simeq} \bigoplus_{k=1}^{s} k[X]/(P_k)$.
$(P_1, \dots, P_s)$ sont les invariants de similitude de u.

Application 30 : Réduction de Frobenius
Il existe une base $\mathcal{B}$ de E telle que $\mathrm{Mat}_{\mathcal{B}}\, u = \begin{pmatrix} C_{P_1} & & \\ & \ddots & \\ & & C_{P_s} \end{pmatrix}$.

IV Applications aux codes correcteurs

But : détecter voire corriger les erreurs liées aux canaux de transmission.

déf 31 : Un code sur $\mathbb{F}_q$ de longueur n est un sous-ensemble $C \subseteq \mathbb{F}_q^n$. $\mathbb{F}_q$ est l'alphabet, n la longueur du code C et les éléments de C sont les mots du code.

déf 32 : Un code linéaire de longueur n et de dimension k sur $\mathbb{F}_q$ est un sous-espace vectoriel C de $\mathbb{F}_q^n$ de dimension k.

déf 33 : Pour $(x, y) \in (\mathbb{F}_q^n)^2$, on définit :
- le poids du mot x : $w(x) = \#\{i \in [\![1, n]\!] \mid x_i \neq 0\}$.
- la distance de x à y : $d(x, y) = w(x - y)$
- la distance minimale d'un code linéaire C :

$d_C = \min\{d(x, y) \mid (x, y) \in C^2, x \neq y\} = \min\{w(x) \mid x \in C^*\}$

prop 34 : Un code linéaire de distance minimale d peut détecter jusqu'à $d-1$ erreurs, corriger jusqu'à $\left\lfloor \frac{d-1}{2} \right\rfloor$ erreurs.

prop 35 [Borne du singleton] Soit C un code linéaire de dim k, taille n. Alors $d_C \leqslant n - k + 1$.

déf 36 : Un code linéaire C est cyclique si :
$\forall (x_1, \dots, x_n) \in C$, $(x_n, x_1, \dots, x_{n-1}) \in C$.

Rque 37 : on identifie alors chaque mot $(c_0, \dots, c_{n-1}) = m$ du code C au polynôme $m(X) = \sum_{i=0}^{n-1} c_i X^i \in \mathbb{F}_q[X]$.
Alors on a $(c_{n-1}, c_0, \dots, c_{n-2}) \sim \sum_{i=0}^{n-1} c_i X^{i+1} + c_{n-1}(1 - X^n)$
d'où,

Prop 38 : Un code linéaire C est cyclique ssi c'est un idéal de $\mathbb{F}_q[X]/(X^n - 1)$.

Rque 39 : $\mathbb{F}_q[X]/(X^n - 1)$ possède une structure d'anneau principal.

App 40 : Construction d'un code cyclique et décodage dans le cas BCH.

DVP

[DEM-PAP]

Références :

- Perrin, Cours d'algèbre
- Escoffier, Toute l'algèbre de la licence
- Goblot, Algèbre commutative
- Objectif Agreg (III)
- Tomazure, Cours d'algèbre
- Papini, Algèbre discrète & codes correcteurs } (IV)
- Combes, Algèbre et géométrie

Autres développements possibles :
(liste non exhaustive)

- $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ principal non euclidien (Perrin)
- Théorème de la base adaptée (Goblot)
- $\mathbb{C}[X,Y]/(Y-X^2)$ et $\mathbb{C}[X,Y]/(XY-1)$ principaux (Francinou, Gianella, exercices de maths pour l'agreg tome Algèbre)
- D'autres exo de (↙)