Leçon III : Anneaux principaux. Applications.

$(A,+,\times)$ anneau intègre (commutatif) unitaire

I Anneau principal, euclidien, factoriel. [FRE I]

1) Anneau principal

Def : Un idéal $I \subset A$ est dit principal s'il existe $m \in I$ tq $I = (m)$

- Un idéal $I \subset A$ est dit premier si $\forall a,b \in A, ab \in I \Rightarrow a \in I$ ou $b \in I$
- — elt $c \in A$ — $c \mid ab \Rightarrow c \mid a$ ou $c \mid b$
- Un idéal $I \subset A$ est dit maximal si $\forall$ idéal J tq $I \subset J \subset A$ $J = I$ ou $J = A$
- Un $c \in A$ est dit irréductible si $\forall a \in A$ tq $a \mid c$ $\exists \varepsilon \in A^\times$ tq $a = \varepsilon$ ou $a = \varepsilon c$.

Def : A est principal si il n'est pas un corps et tous ses idéaux sont principaux.

Exemple : $\mathbb{Z}$ (via les sous groupes de $\mathbb{Z}$) / $C^\infty_c(K)$ où $K \subset \mathbb{R}$ ouvert commercé

Def : A principal, soit $a, b \in A$ on définit $d = pgcd(a,b)$, $m = ppcm(a,b)$ à inversible près par $(a,b) = (d)$ $(a) \cap (b) = (m)$ si d inversible on dit que a et b sont premiers entre eux

Prop : $(a)(b) = (ab)$

Thm : (Chinois) A anneau principal si $pgcd(a,b) = 1$ alors $A/(ab) \simeq \frac{A}{(a)} \times \frac{A}{(b)}$

Thm : Bezout A anneau principal alors $\forall a,b \in A$ $pgcd(a,b) = d \Rightarrow \exists u,v \in A$ tq $au + bv = d$

2) Anneau euclidien

Def : • Stathme euclidien sur A est $\varphi : A^* \to \mathbb{N}$ tq $\forall a,b \in A$ $b \neq 0$ $\exists q,r \in A$ tq $a = bq + r$ et $r = 0$ ou $\varphi(r) < \varphi(b)$.

• Un anneau euclidien est un anneau A qui admet l'existence d'un stathme euclidien.

Exemple : $\mathbb{Z}$ euclidien pour $|\cdot|$.

Thm : Si A anneau eucl alors A principal

Remarque : La preuve de ce théorème est une généralisation de la preuve utilisée pour trouver les sous groupes de $\mathbb{Z}$.

Remarque : D'après le théorème précédent, le théorème de Bezout est vrai dans un anneau euclidien. Mais le stathme euclidien fournit l'algorithme d'Euclide pour trouver le pgcd de 2 elts de A et de plus l'algorithme d'Euclide généralisé fournit un procédé constructif pour l'identité de Bezout.

Théorème : Si K corps alors $K[X]$ euclidien avec pour stathme le degré.

Remarque : D'après ce qui précède $K[X]$ principal. Tout idéal de $K[X]$ est donc principal, en particulier les idéaux annulateurs d'une matrice sont tous principaux donc on définit le polynôme minimal d'une matrice comme l'unique générateur unitaire de son idéal annulateur.

Exemple : d'anneau principal mais non euclidien cf. III 2)

3) Anneau factoriel

Def : A anneau factoriel si $\forall a \in A$ $\exists p_1, \dots, p_m \in A$ tq $\forall i$ p_i irréductible et $a = \prod_{i=1}^{m} p_i$ et les p_i uniques à l'ordre des facteurs près et à inversible près.

Théorème : Si A est un anneau principal alors A factoriel.

Théorème : A factoriel, alors $\forall a \in A$ a premier ssi a irréductible

Corollaire : Dans un anneau principal, un idéal est premier ssi il est maximal.

Def : A factoriel. Soit $a, b \in A$ alors $\exists \varepsilon, \varepsilon' \in A^*$, $p_1, \dots, p_m \in A$ irréductibles tq $a = \varepsilon \prod_{i=1}^{m} p_i^{\nu_i}$ $b = \varepsilon' \prod_{i=1}^{m} p_i^{\nu_i'}$ où $\nu_i, \nu_i' \in \mathbb{N}$

dans ce cas on définit à inversible près $\begin{cases} pgcd(a,b) = \prod_{i=1}^{m} p_i^{\min(\nu_i, \nu_i')} \\ ppcm(a,b) = \prod_{i=1}^{m} p_i^{\max(\nu_i, \nu_i')} \end{cases}$

Remarque : Sur un anneau principal, les définitions "factoriel" et "principal" du pgcd et du ppcm coïncident.

Théorème : Si A anneau factoriel alors A[X] factoriel

Corollaire : $\forall m \in \mathbb{N}^*$ si A factoriel alors $A[X_1,\dots X_m]$ factoriel

Exemple : Anneau factoriel non principal
$\mathbb{Z}[X]$ factoriel d'après ce qui précède
non principal : considérer $(2X, X^2)$ [HAU]

Def : A anneau de Bézout si tout idéal de A engendré par 2 elts est principal.

Théorème : A factoriel et de Bézout $\Rightarrow$ A principal

Remarque : le théorème peut se reformuler de la façon suivante : si A est un anneau factoriel où le théorème de Bézout est vérifié alors A principal.

II A-modules où A principal

1) Définitions [FRE1]

Def : $(M,+,\cdot)$ est un A-module si $(M,+)$ gpe commutatif et si $\forall (\alpha,\beta)\in A^2, (m,m')\in M^2$
- $\alpha\cdot(\beta m) = (\alpha\beta)m$
- $(\alpha+\beta)m = \alpha m + \beta m$
- $\alpha(m+m') = \alpha m + \alpha m'$
- $1_A \cdot m = m$.

Exemples : tout K-ev est un K-module.
- tout idéal de A est un A-module.

Def : Soit M un A-module et $(m_i)_{i\in I}\in M^I$, $I\neq\emptyset$
- (m_i) libre si $\forall J\subset I$ fini $\forall (\lambda_j)\in A^J$, $\sum \lambda_j m_j = 0 \Rightarrow \lambda_j = 0 \ \forall j\in J$
- (m_i) génératrice si $\forall m\in M$ $\exists (\lambda_i)_{i\in I}$ à support fini tel que $\sum_{i\in I}\lambda_i m_i = m$.
- (m_i) est une base si (m_i) libre et génératrice

Def : Un A-module est dit de type fini s'il admet une partie génératrice finie
- Un A-module est dit libre s'il admet une base.

Prop-def : Si M est un A-module libre alors toutes les bases de M ont même cardinal, on appelle alors ce cardinal le rang de M.

Remarque : Tout A-module n'admet pas nécessairement une base. Si A principal, un A-module libre de rang n et L' ⊂ L alors L' A-module libre de rang $\leq n$

Exemple : $\mathbb{Z}/3\mathbb{Z}$ vu comme $\mathbb{Z}$-module n'admet pas de base (en fait il n'a pas de famille libre).

Def : $\mathcal{M}_{m,n}(A) := \{$matrices de $A^n \to A^m\}$
$GL_n(A) := \{$elts inversibles de $\mathcal{M}_{n,n}(A)\}$

Prop : $\forall M\in GL_n(A)$, $\det(M)\in A^\times$.

2) Théorème de structure des A-modules de type fini [GOB]

Lemme : Soit $(a_1,\dots a_m)\in A^m$, $\exists T\in GL_m$ tel que $(a_1\dots a_m)T = (d,0\dots 0)$ où d est le pgcd des (a_j).

Théorème : des bases adoptées. Si L est un A-module libre de rang n et L' un sous-module $L'\subset L$ libre de rang $m\leq n$. Alors il existe $(e_1,\dots e_n)$ base de L, $d_1,\dots d_m\neq 0$ de A tq $\forall j\leq m-1$ $d_j \mid d_{j+1}$ et $(d_1e_1,\dots d_me_m)$ base de L'. Les éléments d_i sont uniques à inversible près. DEV

Théorème : de structure. Si M est un A-module de type fini alors $\exists!(m,n)\in\mathbb{N}^2$ et $\exists d_1,\dots d_m\in A$ tq $M \simeq \frac{A}{(d_1)}\times\dots\times\frac{A}{(d_m)}\times A^n$, les d_i étant uniques à inversible près.

Remarque : L'existence dans le théorème de structure se déduit de l'existence dans le théorème des bases adoptées, mêmes remarques l'unicité dans le théorème de structure ne se déduit pas de l'unicité dans le théorème des bases adoptées et nécessite une démonstration ad hoc.

3) Application aux groupes commutatifs. [FRE2]

Un groupe commutatif G peut être vu comme un $\mathbb{Z}$-module
$n\cdot g = g+\dots+g$ n fois.

Def : G est dit de type fini s'il est de type fini pour cette structure de $\mathbb{Z}$-module.

Le Théorème de structure nous donne alors le Théorème suivant :

Théorème : Si G est de type fini alors $\exists!\, d_1 \dots d_m \in \mathbb{N}^*$ tq $d_1 | \dots | d_m$ et $r \in \mathbb{N}$ tq $G \simeq \frac{\mathbb{Z}}{(d_1)} \oplus \dots \frac{\mathbb{Z}}{(d_m)} \oplus \mathbb{Z}^n$

Si de plus G est fini on retrouve le théorème de classification des groupes abéliens finis : $(r = 0)$.

4) Application aux invariants de similitude d'un endomorphisme [FREZ]

Soit $u \in \mathcal{L}(E)$ où E $\mathbb{K}$-ev de dim finie.

On définit une structure de $\mathbb{K}[X]$-module sur E par $P \cdot x = [P(u)](x)$. Pour cette structure E est de type fini et on a

Théorème : $\exists!\, P_1 \dots P_m \in \mathbb{K}[X]$ unitaires tq $P_1 | \dots | P_m$ et $E = \frac{\mathbb{K}[X]}{(P_1)} \times \dots \times \frac{\mathbb{K}[X]}{(P_m)}$. Les P_i sont les invariants de similitude de u.

Remarque : Matriciellement, les (P_i) caractérisent les classes de similitude de GL_n.

III Anneau des entiers quadratiques. [GOB]

1) Définitions

Def : Si K extension de corps $\mathbb{Q}$, on dit que K quadratique si $\dim_{\mathbb{Q}}(K) = 2$. Donc ce sera $\exists d \in \mathbb{Z}$ sans facteur carré tel que $K = \mathbb{Q}(\sqrt{d})$. si $d > 0$ on parle d'extension réelle, si $d < 0$ on parle d'extension imaginaire.

Prop : $(1, \sqrt{d})$ base de $\mathbb{Q}(\sqrt{d})$

Def : $x = a + b\sqrt{d}$. conjugué : $\bar{x} = a - b\sqrt{d}$
. trace : $t(x) = x + \bar{x} = 2a$
. norme : $N(x) = x\bar{x} = a^2 - b^2 d$

Prop : la conjugaison est un automorphisme de $\mathbb{Q}(\sqrt{d})$
la trace est une forme $\mathbb{Q}$-linéaire
la norme est un morphisme de groupes : $\mathbb{Q}(\sqrt{d})^* \longrightarrow \mathbb{Q}^*$

Def : $z \in \mathbb{Q}(\sqrt{d})$ est un entier quadratique si $t(z) \in \mathbb{Z}$ et $N(z) \in \mathbb{Z}$
On note $\mathcal{O}(d)$ leur ensemble.

Remarque : $u \in \mathcal{O}(d)^*$ ssi $N(u) = \pm 1$.

Théorème : si $d \equiv 2$ ou $3\ [4]$ alors $\mathcal{O}(d) = \mathbb{Z}[\sqrt{d}]$
si $d \equiv 1\ [4]$ alors $\mathcal{O}(d) = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$

Les cas $d > 0$ et $d < 0$ sont très différents :

- $d > 0$ alors $\mathcal{O}(d)$ groupe additif réel non monogène donc dense dans $\mathbb{R}$.
- $d < 0$ alors $\mathcal{O}(d)$ est un réseau de $\mathbb{C}$ de base
  $(1, \sqrt{d})$ si $d \equiv 2$ ou $3\ [4]$ $\quad$ $(1, \frac{1+\sqrt{d}}{2})$ si $d \equiv 1\ [4]$
  maille ... $\quad$ maille ...
  rectangle $\square$ ... $\quad$ losange $\diagup\!\!\square$ ...

2) Caractère euclidien, principal pour $d < 0$

Prop : N est un stathme euclidien sur $\mathcal{O}(d)$ si
- $d \equiv 2$ ou $3\ [4]$ et $d = -1, -2$
ou
- $d \equiv 1\ [4]$ et $d = -3, -7, -11$

Prop : - $d < -2$ et $d \equiv 2$ ou $3\ [4]$ alors $\mathcal{O}(d)$ non principal
- $d < -7$ et $d \equiv 1\ [8]$ alors $\mathcal{O}(d)$ non principal

Remarque : le cas $d \equiv 5\ [8]$ est plus compliqué.

Exemple : $d = -19\ (\equiv 5\ [8])$ $\mathcal{O}(d) = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est un anneau principal non euclidien. [CHAU]]DEV

3) Théorème des 2 carrés.

Théorème : Soit $d \in \mathbb{Z}$ sans facteur carré tq $\mathcal{O}(d)$ principal.
$p > 0$ premier impair. Les conditions suivantes sont équivalentes :
a) d carré modulo p
b) p non premier de $\mathcal{O}(d)$
c) $\exists \pi \in \mathcal{O}(d)$ tq $p = \pm N(\pi)$
d) $\exists a, b \in \mathbb{Z}$ tq $4p^2 = \pm(a^2 - db^2)$

Si l'on est ainsi alors π et $\bar{\pi}$ premiers dans $\mathcal{O}(d)$ et $p = \pi\bar{\pi}$
est la décomposition en produit de facteurs premiers de $\mathcal{O}(d)$.
Les $z \in \mathcal{O}(d)$ tq $p = \pm N(z)$ sont de la forme $z = u\pi$ ou $u\bar{\pi}$ où $u \in \mathcal{O}(d)^*$.

En appliquant cela à $\mathbb{Z}[i]$ euclidien

Théorème : p premier > 2 est somme de 2 carrés ssi $p \equiv 1\ [4]$

Théorème des 2 carrés : $m \in \mathbb{Z}$ $m = \prod_{i=1}^{n} p_i^{\alpha_i} \prod_{j=1}^{k} q_j^{\gamma_j}$ où $p_i \equiv 1\ [4]$, $q_j \equiv 3\ [4]$ premiers
m est somme de 2 carrés ssi les γ_j sont pairs.