Anneaux principaux. Applications.

A est un anneau commutatif, unitaire et intègre.

I) Généralités.

Déf : A est principal si tout idéal est monogène.

1) Anneaux euclidiens.

Déf : A est euclidien s'il existe $\varphi : A \to \mathbb{N}$ (stathme) telle que : $\forall (a,b) \in A^2$, $b \neq 0$, $\exists$ $q, r \in A$, $a = bq + r$, $\varphi(r) < \varphi(b)$.

Prop : Les anneaux euclidiens sont principaux.

Exemples : $\mathbb{Z}$, $K[X]$ (K corps) sont euclidiens.

Prop : $A[X]$ principal $\Leftrightarrow$ $A[X]$ euclidien $\Leftrightarrow$ A corps.

Application : $\mathbb{C}[X,Y]/(XY-1)$ est euclidien.

Théorème : A est principal si et seulement si tous les idéaux maximaux de A sont monogènes.

Contre-exemple : $\mathbb{R}[X,Y]/(X^2+Y^2+1)$ est principal mais non euclidien.

2) Divisibilité.

Déf : Soit $(a,b) \in (A \setminus \{0\})^2$. a et b admettent un PGCD (resp. PPCM) si il existe $d \in A$ (resp. $m \in A$) tel que : $\forall c \in A$, $c \mid a$, $c \mid b \Rightarrow c \mid d$ (resp. $\forall c \in A$, $a \mid c$, $b \mid c \Rightarrow m \mid c$)

Prop : Le PGCD et le PPCM sont uniques à multiplication par un inversible près dans un anneau principal : d est un générateur de (a,b) ; m est un générateur de $(a) \cap (b)$.

Déf : a et b sont dit premiers entre eux lorsque leur PGCD vaut 1.

Théorème de Bézout : Soit A principal. a et b sont premiers entre eux ssi $\begin{cases} \exists (u,v) \in A^2, \\ au + bv = 1 \end{cases}$

Lemme de Gauss : $(a,b,c) \in (A \setminus \{0\})$ avec a et b premiers entre eux où A est principal. Alors : $a \mid bc \Rightarrow a \mid c$.

Application : Résolution de $ax + by = c$ avec $(x,y) \in \mathbb{Z}^2$.

3) Théorème chinois.

Théorème : Soit A principal et $(a_1, \dots, a_m) \in A^m$ avec $PGCD(a_i, a_j) = 1$ si $i \neq j$. Alors :

$$\frac{A}{(a_1, \dots, a_m)} \simeq \frac{A}{(a_1)} \times \dots \times \frac{A}{(a_m)}.$$

Applications :

- Résolution de systèmes de congruences :
$$\begin{cases} x \equiv 2 \ [4] \\ x \equiv 3 \ [5] \end{cases} \Rightarrow x \equiv 18 \ [20]$$
- Nombres de Mersenne : $M_q = 2^q - 1$. Pour tout q premier impair, M_q est premier ssi $(2+\sqrt{3})^{2^{q-1}} \equiv -1 \ [M_q]$ (dans une extension contenant une racine de 3).

4) Factorialité.

Prop : Soit $x \in A$ principal avec x non nul non inversible. Il y a équivalence entre :

(i) $x = x_1 x_2 \Rightarrow x_1 \in A^\times$ ou $x_2 \in A^\times$

(ii) $\forall x_2 \neq 0$ $x \mid x_2$ ou $PGCD(x, x_2) = 1$

(iii) (x) est maximal. On dit que x est irréductible.

Déf : Un idéal I est premier si $I \neq A$ et $ab \in I \Rightarrow a \in I$ ou $b \in I$.

Prop : Dans un anneau principal tout idéal premier non nul est maximal.

Déf: A est factoriel si tout élément $a \in A$ s'écrit: $a = p_1 \cdots p_s$ où p_i est irréductible et cette décomposition est unique à permutation et multiplication par un inversible près.

Théorème: Un anneau principal est factoriel.

Applications:
- Calcul du PGCD / PPCM par réduction.
- Résolution de l'équation de Fermat $x^2 + y^2 = z^2$ dans $\mathbb{N}^3$: $(x,y,z) = d(u^2 - v^2, 2uv, u^2+v^2)$ (facultatif)
- Théorème des zéros de Hilbert : [DVP] Les idéaux maximaux de $\mathbb{C}[X_1, \dots, X_n]$ sont les : $(X - x_1, \dots, X - x_n)$ où $(x_1, \dots, x_n) \in \mathbb{C}^n$.

II) Modules de type fini sur un anneau principal.

Soit A un anneau principal et M un A-module libre de type fini.

1) Facteurs invariants. [DVP]

Théorème: Si $U \in \mathcal{M}_{m,p}(A)$, il existe une famille $(d_1, \dots, d_s) \in A^s$ avec $d_i \mid d_{i+1}$ telle que U soit équivalente à $D = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_s \\ & 0 & \end{pmatrix}$ (où d_i est appelé facteur invariant) avec unicité au sens:

si $U \sim \begin{pmatrix} d'_1 & & 0 \\ & \ddots & \\ 0 & & d'_s \\ & 0 & \end{pmatrix}$ et $d'_i \mid d'_{i+1}$ alors $(d_i) = (d'_i)$.

2) Structure des A-modules de type fini.

Théorème de la base adaptée: Si M est de rang n et N un sous-module de M de rang $m \leq n$, il existe une base $(e_1, \dots, e_n)$ de M et $(d_1, \dots, d_m) \in A^m$ tels que $(d_1 e_1, \dots, d_m e_m)$ soit une base de N.

Théorème: Il existe une unique couple (r, s) et une unique suite $(d_1) \subset \cdots \subset (d_s)$ d'idéaux tels que:

$$M \simeq A^r \oplus \left[\bigoplus_{i=1}^{s} A/(d_i) \right]$$

3) Applications:

a) Structure des groupes abéliens finis.

Théorème: Si G est un groupe abélien fini, il existe une unique suite d'entiers $d_1 | \cdots | d_s$ tels que:

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}.$$

b) Décomposition de Frobénius.

Théorème: Si k est un corps et $M \in \mathcal{M}_n(k)$, en notant $P_1 | \cdots | P_s$ les facteurs invariants de $XI_n - M \in \mathcal{M}_n(k[X])$, M est semblable à une matrice diagonale par blocs dont les blocs diagonaux sont les matrices compagnons des P_i.

c) Réseaux.

Déf: Un réseau R_0 est un sous-groupe additif de E engendrant E comme $\mathbb{R}$-e.v. et sur lequel la topologie de E induit la topologie discrète.

Prop: Tout réseau R_0 s'écrit: $R_0 = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ où $(e_1, \dots, e_n)$ est une base de E.

Application: Soit un convexe C de $\mathbb{R}^n$ symétrique / 0 et L un réseau de volume fondamental $< \frac{\lambda(C)}{2^n}$ (λ : Lebesgue). Alors $C \cap L \neq \{0\}$.

III) Anneaux d'entiers quadratiques.

1) Anneau des entiers.

Soit $d \in \mathbb{Z}$ sans facteur carré. On pose:

$$n : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(\sqrt{d}) \quad \text{et} \quad t : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}$$
$$x + y\sqrt{d} \longmapsto x^2 - dy^2. \qquad \alpha \mapsto \alpha + \bar{\alpha}$$

Déf: $x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ est dit entier si $t(x + y\sqrt{d})$ et $n(x + y\sqrt{d}) \in \mathbb{Z}$.

FACULTATIF

Prop. : Les entiers de $\mathbb{Q}(\sqrt{d})$ forment un sous-anneau de $\mathbb{Q}(\sqrt{d})$ noté ensuite A_d

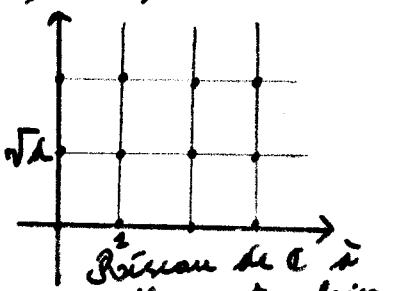
Théorème : (i) Si $d \equiv 1 [4]$, $A_d = \mathbb{Z}\left[\frac{1-\sqrt{d}}{2}\right]$.

(ii) Si $d \equiv 2, 3 [4]$, $A_d = \mathbb{Z}[\sqrt{d}]$.

Remarque : Si $d > 0$, A_d est un sous-groupe de $\mathbb{R}$ $\neq \frac{1}{2}\mathbb{Z}$ donc A_d est dense.

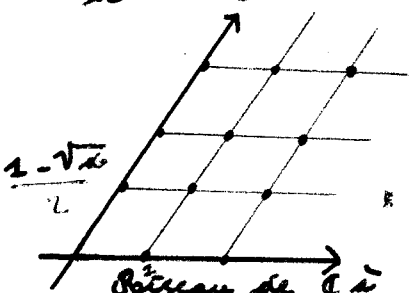
Si $d < 0$, A_d est un réseau de $\mathbb{C}$:

$d \equiv 2, 3 [4]$



Réseau de $\mathbb{C}$ à maille rectangulaire

$d \equiv 1 [4]$



Réseau de $\mathbb{C}$ à maille losange

2) **Caractère euclidien / non principal.**

Prop. : (i) Si $d \equiv 2, 3 [4]$, $|n|$ est un stathme pour A_d ssi $d = -1$ ou $d = -2$

(ii) Si $d \equiv 1 [4]$, $|n|$ est un stathme pour A_d ssi $d = -3, -7$ ou -11.

Théorème : On suppose que $d < 0$.

Si $d \notin \{-1, -2, -7\}$. A_d n'est jamais principal si $d \equiv 2, 3 [4]$ ou $d \equiv 1 [8]$.

Le cas $d \equiv 5 [8]$ est plus complexe :

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ est principal mais non euclidien

3) **Théorème des deux carrés** [DVP]

Théorème : $\mathbb{Z}[i]$ est euclidien et tout entier $n \in \mathbb{N}$ s'écrit comme somme de deux carrés d'entiers si et seulement si ses facteurs premiers congrus à 3 modulo 4 sont d'exposant pair.

IV) Autres applications.

a) **Algorithme de Berlekamp.**

Par application du théorème chinois, si $q = p^n$ $\uparrow$ premier : $\mathbb{F}_q[X]/(P) \simeq \mathbb{F}_q[X]/(P_1) \times \dots \times \mathbb{F}_q[X]/(P_s)$

où $P \in \mathbb{F}_q[X]$ permet d'obtenir une factorisation de P.

b) **Résultant.** $(P, Q) \in K_p[X] \times K_q[X]$

On pose : $R(P,Q) : K_{q-1}[X] \times K_{p-1}[X] \longrightarrow K_{p+q-1}[X]$

$(U, V) \longmapsto UP + VQ$

$\det(R(P,Q))$ fournit l'existence de facteurs communs entre P et Q.

c) **Décomposition de Dunford effective.**

Si K est algébriquement clos de caractéristique nulle, alors il existe un algorithme de calcul de la décomposition de Dunford de $u \in \mathcal{L}(K^n)$. Elle repose sur l'application de la méthode de Newton dans $K[X]/\chi_u(X)$:

$$\begin{cases} x_0 = \overline{X} \\ x_{n+1} = x_n - \dfrac{Q(x_n)}{Q'(x_n)} \end{cases}$$

où $Q = P_1 \dots P_r$ si $\chi_u = P_1^{q_1} \dots P_r^{q_r}$.