A désigne un anneau intègre commutatif, $\mathbb{K}$ un corps

$\mathbb{K}_p$ est le corps à p éléments (pour p premier) P est l'ensemble des nombres premiers

I - Anneaux factoriels, principaux et euclidiens

1 - Idéaux

Déf 1: Un idéal est premier si $\forall a,b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$

Ex 1: Dans $\mathbb{Z}$ les idéaux premiers sont $\{0\}$ et $p\mathbb{Z}$, p premier

Dans $\mathbb{K}[X]$ les idéaux premiers sont $\{0\}$ et $\langle P \rangle$, P irréductible

Déf 2: Un idéal I est maximal si I est strictement inclus dans A tel que $I \subset J \subset A$,

$I = J$ ou $J = A$

Ex 2: Dans $\mathbb{Z}$, $p\mathbb{Z}$ pour p premier est maximal

Dans $\mathbb{K}[X]$, $\langle P \rangle$ pour Q irréductible est maximal

Prop 3:

(i) $\frac{A}{I}$ est un anneau intègre $\Leftrightarrow$ I est un idéal premier

(ii) $\frac{A}{I}$ est un corps $\Leftrightarrow$ I est un idéal maximal

Ex 3: Dans $\mathbb{F}_2[X]$, X^2+1 est irréductible, donc $\frac{\mathbb{F}_2[X]}{\langle X^2+1 \rangle}$ constitue un corps à 4 éléments

Déf 4: Un idéal est principal si $\exists a \in A : I = aA = \langle a \rangle$

Déf 5: Deux idéaux I et J sont dits premiers entre eux si et seulement si $I + J = A$

2 - Anneaux factoriels et principaux

Déf 6: A est dit factoriel si :

(i) A est intègre

(ii) Tout élément $a \neq 0$ de A n'étant ni inversible ni nul, se décompose en produit d'irréductibles

(iii) Cette décomposition est unique à l'ordre et à la multiplication par des inversibles près.

Ex 4: $\mathbb{Z}$ et $\mathbb{K}[X]$ sont factoriels

Ex 5: $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel car $9 = 3^2 = (2+i\sqrt{5})(2-i\sqrt{5})$

Prop 6: A est factoriel si $A[X]$ est factoriel

Déf 7: A est un anneau principal si $\forall I \subset A$ (idéal), $\exists a \in A$, $I = aA$

Tout idéal de A est engendré par un seul élément de A

Ex 7: $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux

$\mathbb{K}[X,Y]$ n'est pas principal car $\langle X, Y \rangle$ est un idéal de $\mathbb{K}[X,Y]$

Prop 8: Si A est principal alors A est factoriel

3 - Anneaux euclidiens

Déf 9: Un anneau est euclidien s'il est intègre et s'il existe une application $\nu : A \setminus \{0\} \longrightarrow \mathbb{N}$ appelée stathme euclidien, vérifiant, pour tous $a, b \in A$, $b \neq 0$:

(i) Soit $b \mid a$

(ii) Soit $\exists (q,r) \in A \times A$, $a = bq + r$, $\nu(r) < \nu(b)$

Ex 10: (i) $\mathbb{Z}$, muni du stathme $\nu : \mathbb{Z}^* \to \mathbb{N}$ est euclidien

$p \longmapsto |p|$

(ii) $\mathbb{K}[X]$ muni du stathme $\nu : \mathbb{K}[X] \setminus \{0\} \to \mathbb{N}$ est euclidien

$P \longmapsto \deg(P)$

(iii) $\mathbb{Z}[i]$, muni du stathme $\nu : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$ est euclidien

$a+ib \longmapsto a^2+b^2$

Prop 10: Si A est euclidien alors A est factoriel (donc factoriel)

Prop 20: Si A est un corps alors $A[X]$ est euclidien

Prop 21: $A[X]$ est principal si et seulement si A est un corps

II - Arithmétique dans les anneaux principaux

1 - Théorème de Bézout

Déf 22: Soient $a, b \in A$. On dit que a et b sont premiers entre eux si pour tout $d \in A$ tel que $d \mid a$ et $d \mid b$ alors $d \in A^\times$

Déf 23: (i) On appelle stathme euclidien la propriété : Soient $b, c \in A$, $c \neq 0$ inversible, $a \mid bc \Rightarrow a \mid b$ ou $b \mid c$

(ii) On appelle propriété de Gauss la propriété : Soient $a, b, c \in A$, a et b sont premiers entre eux et $a \mid bc \Rightarrow a \mid c$

(iii) On appelle propriété de Bézout : Soient $a, b \in A$, premiers entre eux, alors $aA + bA = A$

Déf 24: Soient $a, b \in A$. Un PGCD de $\{a, b\}$ est un élément d de A tel que (i) $d \mid a$ et $d \mid b$

(ii) Soit $\Sigma \in A$ tq $\Sigma \mid a$ et $\Sigma \mid b$ alors $\Sigma \mid d$

Déf 25: Soient $a, b \in A$. Un PPCM de $\{a, b\}$ est un élément $m \in A$ tel que (i) $a \mid m$ et $b \mid m$

(ii) Soit $\mu \in A$ tq $a \mid \mu$ et $b \mid \mu$ alors $m \mid \mu$

2- Propriétés

Prop 26 : On a les implications de réciproques

A euclidien $\Rightarrow$ A principal $\Rightarrow$ A factoriel

$\Downarrow$ $\Downarrow$

Bézout $\Rightarrow$ Gauss $\Rightarrow$ Euclide

Prop 27 : Si A est factoriel et vérifie la propriété de Bézout, alors A est principal.

Rq 28 : On a ainsi fait une équivalence d'après la Prop 26.

Ex 29 : On retrouve de fait que $\mathbb{Z}$ et $\mathbb{K}[X]$ vérifient la propriété de Bézout et la structure de Gauss.

Prop 30 : Si A est principal alors $\forall a,b \in A\setminus\{0\}$, $aA + bA = PGCD(a,b)A$

Prop 31 : Si A est un anneau intègre euclidien. Soient $a,b \in A\setminus\{0\}$.

Supposons que $a = bq + r$. Alors $PGCD(a,b) = PGCD(b,r)$

App. 32 : Algorithme d'Euclide généralisé aux anneaux euclidiens

Th 33 : (Théorème chinois) Si A est un anneau factoriel,

Soit $a \in A\setminus\{0\}$, tel que $a = u p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, $u \in A^\times$, $p_1, \dots, p_n$ irréductibles deux à deux.

Alors, l'application

$$\varphi : \frac{A}{aA} \xrightarrow{\sim} \frac{A}{p_1^{\alpha_1}A} \times \cdots \times \frac{A}{p_n^{\alpha_n}A}$$

$$[x]_{aA} \longmapsto \left([x]_{p_1^{\alpha_1}A}, \dots, [x]_{p_n^{\alpha_n}A}\right)$$

est un isomorphisme d'anneaux.

Ex 34 : On a cet isomorphisme (puisque $20 = 2^2 \times 5$) :

$$\frac{\mathbb{Z}}{20\mathbb{Z}} \simeq \frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$$

App. 35 : Résolution d'un système de congruences

Le système de congruences suivant $\begin{cases} x \equiv 2 \ [5] \\ x \equiv -1 \ [7] \end{cases}$ admet pour solution $\{7+4+7k, k \in \mathbb{Z}\}$

II - Applications

1- Entiers de Gauss

Prop 36 : $\mathbb{Z}[i]$ est euclidien pour le stathme $N : \mathbb{Z}[i] \to \mathbb{N}$, $z = a+ib \longmapsto z\bar{z} = a^2+b^2$

Rq 37 : $\forall u,v \in \mathbb{Z}[i]$, $N(uv) = N(u)N(v)$

Prop 38 : $\mathbb{Z}[i]^\times = \{-1, 1, -i, i\}$

Def 39 : $\Sigma = \{n \in \mathbb{N} \mid \exists (a,b) \in \mathbb{N}^2,\ n = a^2+b^2\}$

Prop 40 : Σ est stable par multiplication.

Prop 41 : Si $p \equiv 3 \ [4]$, alors $p \notin \Sigma$

Th 42 : (Théorème des deux carrés)

Soit p premier. $p \in \Sigma \iff p = 2$ ou $p \equiv 1 \ [4]$

2- Algèbre linéaire

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n.

Def 38 : Le morphisme d'évaluation associé à un endomorphisme u

$$ev_u : \mathbb{K}[X] \to \mathcal{L}(E), \quad P \longmapsto P(u)$$

Th 40 : $\ker(ev_u)$ est un idéal de $\mathbb{K}[X]$, il existe un unique polynôme unitaire μ_u tel que $\ker(ev_u) = \langle \mu_u \rangle$. μ_u s'appelle le polynôme minimal de u.

Prop 41 : (Lemme des noyaux)

Soit $Q = P_1 \cdots P_r$ où $P_1, \dots, P_r$ sont deux à deux premiers entre eux.

Alors, pour $u \in End_{\mathbb{K}}(E)$

$$\ker(Q(u)) = \bigoplus_{i=1}^{r} \ker(P_i(u))$$

Th 42 : (Forme normale de Smith)

Si A est euclidien, soit $M \in \mathcal{M}_{m,n}(A)$. Alors $\exists P \in GL_m(A)$ et $\exists Q \in GL_n(A)$:

$$PMQ = \begin{bmatrix} d_1 & & & (0) \\ & \ddots & & \\ & & d_r & \\ (0) & & & (0) \end{bmatrix}$$

où $d_1 \mid \cdots \mid d_r$

App 43 : (Système d'équations diophantiennes linéaires)

Si on considère un système d'équations diophantiennes linéaires $[S] : AX = B$, $A \in \mathcal{M}_{m,n}(\mathbb{Z})$, $B \in \mathbb{Z}^m$, $X \in \mathbb{Z}^n$ est l'inconnue, alors on réduit A sous sa forme normale de Smith D

$PAQ = D$, où D est donc diagonale, $P \in GL_m(\mathbb{Z})$, $Q \in GL_n(\mathbb{Z})$.

On a :

$$[S] \iff P^{-1}DQ^{-1}X = B$$

$$\iff DY = PB, \text{ où } Y = Q^{-1}X$$

On résout cette équation facilement car D est diagonale, et on calcule $X = QY$.

3 - Irréductibilité de polynômes

Soit A factoriel

Notation Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. On définit le contenu de P, noté $c(P)$, par

$$c(P) = \text{PGCD}\{a_0, \dots, a_n\}$$

Si $c(P) = 1$, on dit que P est primitif.

Proposition : P est un élément irréductible dans $A[X] \iff$
P est irréductible dans $\text{Frac}(A)[X]$ et P est primitif.

Th 43 (Critère d'Eisenstein)

Soit $P \in A[X]$, $P = a_n X^n + \dots + a_1 X + a_0$. Soit $p \in A$ irréductible tel que (i) $p \nmid a_n$
(ii) $\forall i \in [\![0, n-1]\!]$, $p \mid a_i$
(iii) $p^2 \nmid a_0$

alors P est irréductible dans $\text{Frac}(A)[X]$ et dans $A[X]$ si $c(P) = 1$.

Ex (i) $P = X^3 + 3X + 2 \in \mathbb{Z}[X]$ est irréductible
(i) Comme P irréductible est impossible, on essaie si $P = X^2 - 4 \in \mathbb{Z}[X]$
$p = 2$, $p \nmid 1$, $p \mid -4$ et $p^2 \nmid -4$, mais $P = (X-2)(X+2)$ n'est pas irréductible

Th 50 (Réduction)

Soit $p \in A$ irréductible et soit $B = A/pA$. Soit $\varphi : A[X] \to B[X]$ le morphisme de réduction des coefficients modulo p. Soit $P \in A[X]$ non constant. On suppose que
(i) $\deg(\varphi(P)) = \deg(P)$
(ii) $\varphi(P)$ est irréductible dans $\text{Frac}(B)[X]$
Alors P est irréductible dans $\text{Frac}(A)[X]$ et dans $A[X]$ si P est primitif.

Ex 51 Soit $P = X^4 + 4 \in \mathbb{Z}[X]$, soit $\varphi : \mathbb{Z}[X] \to \mathbb{F}_3[X]$ $(\mathbb{F}_3 = \frac{\mathbb{Z}}{3\mathbb{Z}})$
$\varphi(P) = X^4 + \overline{1}$, est irréductible dans $\mathbb{F}_3[X] = \text{Frac}(\mathbb{F}_3)[X]$.
Donc P est irréductible dans $\mathbb{Z}[X]$

4 - Anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un quotient de fractions

Def : On dit que a est congru à b modulo n ($n \neq 0$) si $n \mid a - b$ et on note $a \equiv b \ [n]$ ou de manière équivalente $\overline{a} = \overline{b}$ dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ou encore dans $\mathbb{Z}$, $a + n\mathbb{Z} = b + n\mathbb{Z}$ (appelé classe d'équivalence)

Prop : (i) On a $\overline{a} = 0$ dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ si $n \mid a$
(ii) $\overline{a} \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ si $a \wedge n = 1$

Cor : $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps si $p \in \mathbb{P}$

Rq : On le note parfois $\mathbb{F}_p$

Appli : (i) $\forall n \in \mathbb{N}^*$, $\frac{5^{n+1} + 6^{n+1}}{5^n + 6^n}$ est irréductible

(ii) $\forall n \in \mathbb{N}^*$, $\frac{7^{n+1} + 3 \times 0^{n+1}}{7^n + 3 \times 0^n}$ est irréductible

(iii) Soient $(\lambda, \mu, \alpha, \beta) \in \mathbb{N}^{*4}$, $n \in \mathbb{N}^*$ et $F_n = \frac{\lambda \alpha^{n+1} + \mu \beta^{n+1}}{\lambda \alpha^n + \mu \beta^n}$ DVPT 2

Alors F_n est irréductible ssi $\lambda \wedge \mu = \lambda \wedge \beta = \mu \wedge \alpha = \alpha \wedge \beta$
$= (\alpha - \beta) \wedge (\lambda + \mu) = 1$ [illegible]

Références :
D. Perrin, Cours d'algèbre
FGN, Anneaux A=ENS, Algèbre 1