Dans cette leçon, A désigne un anneau commutatif unitaire. On note $(a) = aA = \{ax, x \in A\}$ l'idéal engendré par $a \in A$. On suppose connue la notion d'idéal, idéal premier, idéal maximal.

I. Définitions et premières propriétés

1) Anneaux principaux

Def ① : • Un idéal I de A est principal si $I = (a)$ pour un $a \in A$.
• A est dit principal s'il est intègre et si tout idéal de A est principal.

Ex ② : • $\{0\}$ et A sont des idéaux principaux de A
• si $\mathbb{K}$ corps, alors $\mathbb{K}$ est principal.
• $\mathbb{Z}$ est un anneau principal.

Def ③ : • A est noethérien si tout idéal de A est engendré par un nombre fini d'élément
• ceci équivaut à dire que toute suite croissante d'idéaux de A est stationnaire.

Rq ④ : Un anneau principal est noethérien. La réciproque est fausse.

2) Anneaux euclidiens

Def ⑤ : A est euclidien si il est intègre et si il existe $v : A\setminus\{0\} \to \mathbb{N}$ tq si $a, b \in A\setminus\{0\}$, $\exists q, r \in A$ avec $a = bq + r$, $r = 0$ ou $v(r) < v(b)$

prop ⑥ : un anneau euclidien est principal

Ex ⑦ : $A = \mathbb{K}[X]$ où $v = \deg$ est un anneau euclidien.

app ⑧ : soit $M \in \mathcal{M}_n(\mathbb{K})$, et $I = \{P \in \mathbb{K}[X], P(M) = 0\}$ idéal de $\mathbb{K}[X]$ principal, donc I admet un unique générateur unitaire appelé polynôme minimal de M, noté Π_M.

II. Divisibilité et décomposition dans A principal

Def ⑨ : • soient a, b deux éléments de A. On dit que a divise b (noté $a | b$) si $\exists c \in A$ tq $ac = b$
$\Leftrightarrow (b) \subset (a)$
• $a \in A$ est irréductible si $a \neq 0$, $a \notin A^\times$ et si $a = bc$ alors b ou $c \in A^\times$.

prop ⑩ : soit A principal et $p \in A\setminus\{0\}$. on a équivalence entre :
(i) p est irréductible
(ii) (p) est maximal dans A
(iii) (p) est premier
(iv) $A/(p)$ est un corps.

Thm ⑪ : A principal, et soit $a \in A$ non inversible, alors $a = p_1 \dots p_n$ s'écrit comme produit d'éléments irréductibles, cette écriture est unique à association près
(un anneau vérifiant ces propriétés est dit factoriel)
• On appelle système d'irréductibles dans A une famille $\mathcal{P}$ d'éléments irréductibles de A tq tout irréductible de A soit associé à un élément de $\mathcal{P}$ et un seul.

Cor ⑫ : si $a = u p_1^{\alpha_1} \dots p_k^{\alpha_k} \in A\setminus\{0\}$, $u \in A^\times$, $p_1 \dots p_k \in \mathcal{P}$ et $\alpha_i \in \mathbb{N}^*$, les diviseurs de a sont de la forme $b = v p_1^{\beta_1} \dots p_k^{\beta_k}$ où $v \in A^\times$, $\beta_1 \dots \beta_k \in \mathbb{N}$ $\beta_i \leq \alpha_i \ \forall i$

Ex ⑬ : • Les irréductibles de $\mathbb{Z}$ sont les nombres p premier
• Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1
• Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 ou

de degré 2 sans racines réelle.

Les entiers de Gauss

On veut déterminer les $n \in \mathbb{N}$ somme de deux carrés : $n = a^2+b^2$ $a,b \in \mathbb{N}$. On pose $\Sigma = \{ n \in \mathbb{N},\ n = a^2+b^2,\ a,b \in \mathbb{N} \}$.

Def 14 : l'anneau des entiers de Gauss est $\mathbb{Z}[i] = \{a+ib,\ a,b \in \mathbb{Z}\}$

prop 15 : On munit $\mathbb{Z}[i]$ de l'application $N : \begin{array}{l} z \in \mathbb{Z}[i] \longmapsto z\bar{z} \\ a+ib \longmapsto a^2+b^2 \end{array}$

on a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} = \{ z \in \mathbb{Z}[i],\ N(z) = 1 \}$

prop 16 : Σ est stable par multiplication.

prop 17 : $\mathbb{Z}[i]$ est euclidien (donc principal)

DVP 1

prop 18 : soit $p \in \mathbb{N}$ premier, alors :
(i) $p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[i]$
(ii) $p \in \Sigma \iff p = 2$ ou $p \equiv 1\ [4]$

Thm 19 : soit $n \in \mathbb{N}^*$, $n \neq 1$. on écrit $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$
alors $n \in \Sigma \iff v_p(n)$ pair pour $p \equiv 3\ [4]$.

Thm 20 : les irréductibles de $\mathbb{Z}[i]$ sont aux inversibles près :
(i) les entiers $p \equiv 3\ [4]$ $p \in \mathbb{N}$ premiers
(ii) les éléments de la forme $a+ib$ dont la norme a^2+b^2 est un nombre premier.

II. PGCD et PPCM dans un anneau principal

Def 21 : soient $a, b \in A \setminus \{0\}$ (A intègre). ~~Soient~~ on dit que d est un pgcd de a et b si $d | a$, $d | b$ et si $\forall c$ vérifiant $c | a$ et $c | b$, on a $c | d$.
- on dit que m est un ppcm de a et b si $a | m$, $b | m$ et $\forall c$ vérifiant $a | c$, $b | c$, on a $m | c$.

Rq 22 : les pgcd et ppcm sont définies à associations près.
- Dans un anneau quelconque, rien n'assure l'existence de ces deux éléments.

prop 23 : - un générateur de $(a) \cap (b)$ dans A principal est un ppcm de a et b
- un générateur de $(a) + (b)$ est un pgcd de a et b.

Rq 24 : ceci se généralise à une famille finie d'éléments de A

cor 25 (Bezout) : Soient $a_1 \dots a_n$ des éléments de A principal et d diviseur de $a_1, \dots, a_n$. Alors d est un pgcd de $a_1 \dots a_n$ ssi $\exists\ u_1 \dots u_n \in A$ tq $d = a_1 u_1 + \dots + a_n u_n$.
- Des éléments sont dit premiers entre eux dans leur ensemble si leurs pgcd dans A sont dans $A^\times$.

cor 26 : soit A principal, $a,b,c \in A$. si $\text{pgcd}(a,b) = 1$ (à association près) et si $a | bc$, alors $a | c$ (Gauss).

prop 27 : si A principal, $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ et $b = v \prod_{p \in \mathcal{P}} p^{v_p(b)}$
alors $\text{ppcm}(a,b) = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$
et $\text{pgcd}(a,b) = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$

en particulier : $ab = \text{pgcd}(a,b)\, \text{ppcm}(a,b)$ à association près

Calcul dans le cas euclidien A euclidien

Thm 28 : si $a,b \in A\setminus\{0\}$, soit (r_i) : la suite d'éléments de A définis par $r_0 = a$, $r_1 = b$ puis pour $i \geq 2$ $r_i = rem(r_{i-2}, r_{i-1})$ où $rem(x,y)$ est le reste dans la division euclidienne de x par y. Alors cette suite est stationnaire à 0 ($\exists n \in \mathbb{N}$, $r_{n+1} = 0$ et $r_n \neq 0$) et $pgcd(a,b) = r_n$.

Thm 29 (Euclide étendu) si $a,b \in A\setminus\{0\}$ on définit

$$W_0 = \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix}, \quad W_1 \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix} \quad \text{et} \quad W_i = \begin{pmatrix} r_i \\ u_i \\ v_i \end{pmatrix}$$

où $\forall i \geq 2$ $\begin{cases} r_i = rem(r_{i-2}, r_{i-1}) \\ u_i = u_{i-2} - q_i u_{i-1} \\ v_i = v_{i-2} - q_i v_{i-1} \end{cases}$ (q_i quotient dans la division euclidienne de r_{i-1} par r_{i-2})

alors $\forall i$, $r_i = a u_i + b v_i$ (en particulier, $pgcd(a,b) = au_n + bv_n$)

application 30 : $pgcd(X^m - 1, X^n - 1) = X^{pgcd(m,n)} - 1$.

Facteurs invariants

Thm 31 : soit A un anneau principal, $m,n \in \mathbb{N}^*$. Soit $M \in M_{n,m}(A)$, alors il existe $P \in Gl_n(A)$, $Q \in Gl_n(A)$, et une suite $(d_i)_{i=1}^{r}$ de $A\setminus\{0\}$ tq $d_1 | \dots | d_r$ et

$$A = P \left(\begin{array}{c|c} d_1 \ddots d_r & 0 \\ \hline 0 & 0 \end{array} \right) Q.$$ Si de plus $d_1' \dots d_r'$ est une autre telle suite, on a $d_i = u_i d_i'$ $\forall i$ où $u_i \in A^\times$.

on appelle la suite $d_1 \dots d_r$ les facteurs invariants de A.

DVP ②

Lemme chinois

prop 32 : A anneau commutatif unitaire. I, J des idéaux de A avec $I + J = A$.

alors $\psi : A/(I\cap J) \longrightarrow A/I \times A/J$ est un isomorphisme d'anneaux.
$\hat{x} \longmapsto (\bar{x}, \dot{x})$

cor 33 : soient A principal et $m,n \in A$ premier entre eux. alors $\psi : A/(mn) \longrightarrow A/(m) \times A/(n)$ est un isom d'anneaux.
$\hat{x} \longmapsto (\bar{x}, \dot{x})$

et $\psi^{-1} : A/(m) \times A/(n) \longrightarrow A/(mn)$
$(\bar{a}, \dot{b}) \longmapsto \hat{x}$ où $x = vna + umb$ avec u,v tq $1 = um + vn$.

Ex 34 : $\begin{cases} x \equiv 2 [4] \\ x \equiv 3 [5] \\ x \equiv 1 [9] \end{cases}$ admet pour solutions les x de la forme $x = 838 + k180$ où $k \in \mathbb{Z}$

Lemme des noyaux

Lemm 35 : soit E ev sur $\mathbb{K}$ un corps, $P_1, \dots, P_r \in \mathbb{K}[X]$ premiers entre eux deux à deux, et $u \in \mathcal{L}(E)$
alors $\ker(P_1 \dots P_r(u)) = \bigoplus_{i=1}^{r} \ker(P_i(u))$

app 36 (Dunford) : Soit $f \in \mathcal{L}(E)$ de polynome caractéristique scindé sur $\mathbb{K}$. il existe un unique couple $(d,n) \in \mathcal{L}(E)^2$ tq
(i) d diagonalisable, n nilpotente
(ii) $f = d + n$, $n\circ d = d\circ n$ et d, n sont des polynômes en f.

Développements :

① Théorème des deux carrés [15] à [19]

② Algorithme des facteurs invariants [31]
(Existence)