Cadre : A sera un anneau unitaire commutatif

I) Anneaux Principaux - Structures

Déf 1 : Un idéal I de A est principal s'il est engendré par un seul élément : $\exists x \in I$ tel que $I = (x) = xA$.

Ex 2 : Dans $\mathbb{Z}$, $\forall n \in \mathbb{Z}$, $(n) = n\mathbb{Z}$ est principal.

Déf 3 : A est principal si A est intègre, et si tout idéal de A est principal.

Ex 4 : $\mathbb{Z}$ et $\mathbb{D} = \{\frac{a}{10^n}, a \in \mathbb{Z}, n \in \mathbb{N}\}$ sont principaux. Tout corps K est principal : ses seuls idéaux sont (0) et (1).

C-Ex 5 : $\mathbb{Z}[X]$ n'est pas principal, car $(2, X)$ n'est pas un idéal principal de $\mathbb{Z}[X]$.

Déf 6 : A est noethérien si tout idéal I de A est engendré par un nombre fini d'éléments.

Prop 7 : A est noethérien ssi toute suite croissante d'idéaux $I_1 \subset \dots \subset I_n$ est stationnaire.

Thme 8 : (Thme de la base de Hilbert)
A noethérien $\Rightarrow A[X]$ noethérien
$\Rightarrow A[X_1, \dots X_n]$ noethérien

C-Ex 9 : $K[X_1, \dots, X_n, \dots]$ n'est pas noethérien.

Prop 10 : A principal $\Rightarrow A$ noethérien.

C-Ex 11 : $\mathbb{Z}[X]$ et $K[X,Y]$ sont noethériens, mais ne sont pas principaux.

Déf 12 : $p \in A \setminus \{0\}$ est irréductible si $p \notin A^*$ et si $\forall a, b \in A$, $p = ab \Rightarrow a \in A^*$ ou $b \in A^*$

Ex 13 : Dans $\mathbb{Z}$, les irréductibles sont les nombres premiers

Déf 14 : A est factoriel si A est intègre, et si $\forall a \in A \setminus \{0\}$, $\exists u \in A^*$ et $p_1, \dots p_r \in A$ irréductibles, uniques à permutation et à inversible près, tel que $a = u p_1 \dots p_r$

Prop 15 : A factoriel $\Rightarrow A[X]$ factoriel

Prop 16 : A principal $\Rightarrow A$ factoriel

C-Ex 17 : $K[X,Y]$ est factoriel mais pas principal

C-Ex 18 : $\mathbb{Z}[i\sqrt{5}]$ est noethérien, mais pas factoriel, car $3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}) = 9$
$K[X_1, \dots X_n, \dots]$ est factoriel mais pas noethérien.

Déf 19 : A est euclidien si A est intègre, et si A est muni d'un stathme $\nu : A \setminus \{0\} \to \mathbb{N}$ tel que $\forall a, b \in A \setminus \{0\}$, $\exists q, r \in A$ tel que $a = bq + r$ avec $r = 0$ ou $\nu(r) < \nu(b)$

Ex 20 : $\mathbb{Z}$ muni de $|.|$ est euclidien.
$K[X]$ muni du degré est euclidien.

Prop 21 : $A[X]$ est euclidien ssi A est un corps

Prop 22 : A euclidien $\Rightarrow A$ principal

C-Ex 23 : $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ et $\mathbb{R}[X,Y]/(X^2+Y^2+1)$ sont principaux mais pas euclidiens.

Prop 24 : $A[X]$ est principal ssi A est un corps.

App 25 : Soit K un corps et B un anneau.
$\forall \beta \in B$, posons $ev_\beta : P \in K[X] \longmapsto P(\beta) \in B$.
$\ker(ev_\beta)$ est un idéal de l'anneau principal $K[X]$, donc $\exists \mu_\beta \in K[X]$ tel que $\ker(ev_\beta) = (\mu_\beta)$. On définit ainsi μ_β comme étant le polynôme minimal de β.

II) Arithmétique dans les anneaux principaux

Déf 26 : On note $a | b$ si $\exists c \in A$ tel que $b = ac$ ou si $(b) \subset (a)$ $\quad a, b \in A$

Déf 27 : On dit que $a, b \in A$ sont associés si $a | b$ et $b | a$, ou si $(a) = (b)$. Si A est intègre, $a, b \in A$ sont associés

ssi $\exists u \in A^*$ tel que $a = ub$

Thm 28: (Lemme d'Euclide)
Soit A factoriel. $\forall a,b \in A$, $\forall p \in A$ irréductible,
$p \mid ab \Rightarrow p \mid a$ ou $p \mid b$

Prop 29:
Soit A factoriel, $p \in A$ est irréductible ssi (p) est premier

Prop 30: Soit A principal. $p \in A$ est irréductible ssi (p) est premier, ssi (p) est maximal.

Déf 31: $a,b \in A \setminus \{0\}$ sont premiers entre eux si
$\forall d \in A$, $d \mid a$ et $d \mid b \Rightarrow d \in A^*$

Thme 32: (lemme de Gauss)
Soit A factoriel, $\forall a,b \in A \setminus \{0\}$ premiers entre eux, et
$\forall c \in A$, $a \mid bc \Rightarrow a \mid c$

Déf 33: Soient $a,b \in A \setminus \{0\}$. On appelle pgcd de a et b tout $d \in A$ tel que $d \mid a$, $d \mid b$ et $\forall c \in A$ tel que $c \mid a$ et $c \mid b$, alors $c \mid d$.
On appelle ppcm de a et b tout $m \in A$ tel que $a \mid m$, $b \mid m$ et $\forall c \in A$ tel que $a \mid c$ et $b \mid c$, alors $m \mid c$

Rq 34: Le pgcd et le ppcm n'existent pas toujours. S'ils existent, ils sont définis à inversible près.

C-Ex 35: Dans $\mathbb{Z}[i\sqrt{5}]$, le pgcd de 9 et $6+3i\sqrt{5}$ n'existe pas, car $9 = 3\times 3 = (2+i\sqrt{5})(2-i\sqrt{5})$ et $6+3i\sqrt{5} = 3(2+i\sqrt{5})$.

Prop 36: Si A est factoriel, le pgcd et le ppcm existent, et $\forall a,b \in A \setminus \{0\}$, $\text{pgcd}(a,b)\cdot\text{ppcm}(a,b) = ab$ (a inversible près)
Si A est principal, $(a)+(b) = (\text{pgcd}(a,b))$
$(a)\cap(b) = (\text{ppcm}(a,b))$

Thm 37: (Bezout)
Soit A principal. $\forall a,b \in A \setminus \{0\}$, $\exists u,v \in A$ tel que
$au + bv = \text{pgcd}(a,b)$
et $\text{pgcd}(a,b) = 1 \Leftrightarrow \exists u,v \in A$ tel que $au + bv = 1$

C-Ex 38: Dans $\mathbb{Z}[X]$, $\text{pgcd}(2,X) = 1$
Mais $\forall U,V \in \mathbb{Z}[X]$, $2U + XV \neq 1$

Thm 39: (Lemme des noyaux)
Soient E un espace vectoriel et $u \in \mathcal{L}(E)$
$\forall P = P_1 \cdots P_r \in K[X]$, $P_1, \dots, P_r$ 2 à 2 premiers entre eux,
on a $\text{Ker}(P(u)) = \bigoplus \text{Ker}(P_i(u))$
Si P annule u, alors $E = \bigoplus \text{Ker}(P_i(u))$.

Thme 40: (Thme Chinois)
Soient $I_1, \dots, I_r$ des idéaux de A 2 à 2 étrangers, i.e
$\forall i,j \in [\![1,r]\!]$, $I_i + I_j = (1) = A$
Alors $A/\prod I_i \simeq \prod A/I_i$
En particulier, si A est principal, et $p_1, \dots, p_r$ 2 à 2 premiers entre eux, $A/(p_1 \cdots p_r) \simeq \prod A/(p_i)$

Prop 41: Soit A euclidien. Soient $a,b \in A \setminus \{0\}$. Par division euclidienne, $\exists q,r \in A$ tel que $a = bq + r$, $r = 0$ ou $\nu(r) < \nu(b)$
et $\text{pgcd}(a,b) = \text{pgcd}(b,r)$

App 42: (Algorithme d'Euclide)
Dans A euclidien, on peut calculer algorithmiquement le pgcd de 2 éléments par divisions euclidiennes successives

III) Applications et Exemples

1) Anneaux d'entiers de corps quadratique

Déf 43: Soit $d \in \mathbb{Z} \setminus \{0,1\}$ sans facteur carré.
En notant $\sqrt{d} = i\sqrt{|d|}$ si $d < 0$, on définit :

$\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} \,/\, x, y \in \mathbb{Q}\}$
et on définit A_d l'ensemble des entiers algébriques de $\mathbb{Q}[\sqrt{d}]$, i.e l'ensemble des éléments de $\mathbb{Q}[\sqrt{d}]$ dont le polynôme minimal appartient à $\mathbb{Z}[X]$.

Prop 44 : A_d est un anneau intègre

Thme 45 : Soit $d \in \mathbb{Z} \setminus \{0,1\}$ sans facteurs carré
Si $d \equiv 2$ ou 3 [4], alors $A_d = \mathbb{Z}[\sqrt{d}]$
Si $d \equiv 1$ [4], alors $A_d = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

Lemme 46 : On appelle anneau des entiers de Gauss $A_1 = \mathbb{Z}[i]$
Alors $\mathbb{Z}[i]$ est euclidien pour le stathme $N(a+ib) = a^2+b^2$
Et $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$

Thme 47 : (Thme des deux carrés)
Soit $p \in \mathbb{N}$ un nombre premier.
Notons $\Sigma = \{n \in \mathbb{N} \,/\, n = a^2+b^2,\ a,b \in \mathbb{N}\}$
Alors $p \in \Sigma$ ssi $p \equiv 1$ ou 2 [4]
De façon générale, $n \in \Sigma$ ssi $\forall p \mid n$, $p \equiv 1$ ou 2 [4] ou $\mathrm{ord}_p(2)$ est pair [DCV]

Coro 48 : Les irréductibles de $\mathbb{Z}[i]$ sont, à inversible près, les entiers p premiers avec $p \equiv 3$ [4].
et les $x \in \mathbb{Z}[i]$ tel que $N(x) \in \mathbb{N}$ est premier.

Prop 49 : De façon générale, $A_d^* = \{x \in A_d,\ N(x) = 1\}$
et A_d est euclidien pour le stathme $N(a+b\sqrt{d}) = a^2 - db^2$
ssi $d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13\}$

2| Modules sur un anneau principal

Thme 50 : (Forme Normale de Smith)
Soit A un anneau principal et $M \in \mathcal{M}_{n,q}(A)$
Alors il existe $P \in SL_n(A)$, $Q \in SL_m(A)$, et $a_1 \dots a_r \in A$ avec $a_1 \mid a_2 \mid \dots \mid a_r$ tel que
$$PMQ = \Delta = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} \quad \text{avec } D = \mathrm{diag}(a_1, \dots a_r)$$
où les $a_1, \dots a_r$ sont uniques à inversible près. [DCV]

Coro 51 : (Thme de la base adaptée)
Soit F un A-module libre de type fini, et M un sous A-module de F de type fini.
Alors il existe $\mathcal{F} = (f_1, \dots f_n)$ base de F, et $a_1, \dots a_r \in A$ avec $a_1 \mid a_2 \mid \dots \mid a_r$ tel que $(a_1 f_1, \dots a_r f_r)$ soit une base de M (qui est alors libre)

Coro 52 : (Thme de Structure des A-modules)
Soit M un A-module de type fini.
Alors il existe $a_1, \dots a_r \in A$ avec $a_1 \mid \dots \mid a_r$, et $q \in \mathbb{N}$ tel que $M \simeq A^q \oplus A/(a_1) \oplus \dots \oplus A/(a_r)$
où $q, (a_1), \dots (a_r)$ sont uniques.

App 53 : (Thme de Structure des groupes abéliens)
Soit G un groupe abélien de type fini. G peut être vu comme un $\mathbb{Z}$-module de type fini, donc il existe $q \in \mathbb{N}$, $a_1, \dots a_r \in \mathbb{Z}$ avec $a_1 \mid \dots \mid a_r$ tel que
$$G \simeq \mathbb{Z}^q \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/a_r\mathbb{Z}$$

Références : Perrin, "Cours d'algèbre"
Berhuy, "Algèbre : le grand combat"
Diaz-Toca, Lombardi, Quitté, "Modules sur les anneaux commutatifs"