122 Anneaux principaux
Applications

Refs : [Per] Perrin, Cours d'Algèbre. [OA] BMP : Objectif agrégation
[Cal2] Calais, Éléments de théorie des Anneaux [Gou1] Gourdon, Algèbre.
[Lan] Lang, Algèbre.
Devts : Thm 33+34 (deux cas) Facteurs invariants.
Ex 29 ($\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$)

Cadre : A un anneau commutatif unitaire, K un corps.

I. Notion de Principalité

1) Idéaux d'un anneau.

[Per] 42,43

Def 1 : On appelle idéal de A tout sous ensemble de A qui se réalise comme noyau d'un morphisme d'Anneaux $A \to B$. On dit qu'un idéal I de A est principal (ou monogène) s'il existe $x \in A$ tel que $I = \{ax \mid a \in A\}$, on note $I = (x)$.

Ex2 : Tout idéal de $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$ est principal.

Ex3 : L'idéal $(2, X)$ de $\mathbb{Z}[X]$ n'est pas principal

Prop-def 4 : Soit $I \subseteq A$ un idéal, on a équivalence entre
- A/I est intègre
- Si $ab \in I$, alors $a \in I$ ou $b \in I$ (pour $a, b \in A$)

Si l'une de ces conditions est réalisée, on dit que I est intègre

Ex5 : L'idéal $(n) = n\mathbb{Z}$ de $\mathbb{Z}$ est premier si et seulement si $n = 0$ ou n est premier.

Prop-def 6 : Soit $I \subseteq A$ un idéal, on a équivalence entre
- A/I est un corps
- Si $I \subsetneq J \subseteq A$ est un idéal, alors $J = A$ ou I (et $I \neq A$).

Si l'une de ces conditions est réalisée, on dit que I est maximal.

Ex7 : Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ pour p premier.

Théo 8 : Tout idéal de A est inclus dans un idéal maximal.

2) Anneaux principaux.

[Per] 49

Def 9 : L'anneau A est dit principal s'il est intègre et si tout idéal de A est principal.

Ex10 : L'anneau $\mathbb{Z}$ est principal, ainsi que $K[X]$, mais pas $\mathbb{Z}[X]$, ni $\mathbb{Z}/n\mathbb{Z}$ pour n non premier.

[OA]

Appl 11 : Soit E un K-espace vectoriel de dimension finie, $f \in \mathcal{L}(E)$. On a un morphisme d'évaluation $K[X] \to \mathcal{L}(E)$ qui envoie $P(X)$ sur $P(f)$, il s'agit d'une application linéaire, dont le noyau est non trivial. Comme $K[X]$ est principal, cet idéal est monogène, on appelle polynôme minimal de f le générateur unitaire de cet idéal.

[OA]

Appl 12 : Si $K \to L$ est une extension de corps, et $\alpha \in L$ est algébrique sur K. Le même raisonnement sur l'évaluation des polynômes en α donne l'existence du polynôme minimal de α.

Def 13 : Soit $p \in A$, on dit que p est irréductible si $p \notin A^\times$ et si $p = ab$, alors on a $a \in A^\times$ ou $b \in A^\times$.

Ex14 : Les irréductibles de $\mathbb{Z}$ sont les nombres premiers, à ± 1 près.

Prop 15 : Si A est principal, on a les équivalences
$I = (p)$ est premier $\Leftrightarrow$ p est irréductible $\Leftrightarrow$ $(p) = I$ est maximal

Prop 16 : Si A est un corps, alors $A[X]$ est principal

Rq 17 : On obtient une preuve simple que $\mathbb{Z}[X]$ n'est pas principal

[Cal2]

Prop 18 : Si $S \subseteq A$ est une partie multiplicative et si A est principal alors $S^{-1}A$ est principal

Appl 19 : L'anneau des décimaux est principal, de même que $\mathbb{Q}$.

3) Cas des anneaux euclidiens.

[Per] 50,51

Def 20 : Un anneau intègre A est dit euclidien s'il est muni d'une application (le stathme) $v : A \setminus \{0\} \to \mathbb{N}$ telle que, pour $a, b \in A^*$, il existe $q, r \in A$ avec $a = bq + r$ et ($r = 0$ ou $v(r) < v(b)$).

Ex21 : $\mathbb{Z}$, muni de la valeur absolue, est euclidien

Théo 22 : Un anneau euclidien est principal

Prop 23 : Soit $P \in A[X]^*$, de coefficient dominant inversible, et $F \in A[X]$. Il existe $Q, R \in A[X]$ tels que $F = PQ + R$ et
$$d^\circ R < d^\circ P \text{ ou } R = 0$$

Cor 24 : Si K est un corps, alors $K[X]$ est euclidien et principal

Cor 25 : L'anneau $A[X]$ est principal si et seulement si A est un corps.

Cor 26 : L'anneau $K[X_1, \dots, X_n]$ est principal si et seulement si $n = 1$.

Ex 27 : L'anneau $K[[X]]$ est euclidien. Ses inversibles sont les séries $\sum a_n X^n$ avec $a_0 \neq 0$.

Prop 28 : Avec les notations de la proposition, si A est euclidien, alors c'est aussi le cas de $S^{-1}A$

[Per] 54

Ex 29 : Pour $\alpha = \frac{1}{2}(1 + i\sqrt{19})$, l'anneau $\mathbb{Z}[\alpha]$ est principal et non euclidien. DVP.

4) Application : Théorème des deux carrés.

[Perr] 55-58

Déf 30 : On définit l'anneau des entiers de Gauss comme
$$\mathbb{Z}[i]=\{a+ib \mid a,b\in\mathbb{Z}\}$$
On définit $N:\mathbb{Z}[i]\setminus\{0\}\longrightarrow\mathbb{N}$ par $N(a+ib)=a^2+b^2$.

Prop 31 : L'anneau $\mathbb{Z}[i]$ muni de N est un anneau euclidien

Déf 32 : On pose $\Sigma = N(\mathbb{Z}[i])\cup\{0\}$ l'ensemble des entiers s'écrivant comme somme de deux carrés.

DVP

Théo 33 : Soit p un nombre premier, on a les équivalences
$p\in\Sigma \iff p\equiv 2$ ou $p\equiv 1[4] \iff p$ est réductible dans $\mathbb{Z}[i]$.

Théo 34 (Théorème des deux carrés) Soit $n\in\mathbb{N}^*$, alors $n\in\Sigma$ si et seulement si pour tout $p\equiv 3[4]$ premier divisant n, $v_p(n)$ pair.

II. Arithmétique dans les anneaux principaux

1) Divisibilité, factorialité.

[Perr] 46, 47

Déf 35 : Soient $a,b\in A$, on dit que a divise b, noté $a|b$, si $b\in(a)$, i.e $(b)\subseteq(a)$.

Déf 36 : On définit l'association comme la relation d'équivalence
$a\mathcal{R}b \iff a|b$ et $b|a \iff (a)=(b)$

Prop 37 : Si A est intègre, alors $a\mathcal{R}b \iff \exists u\in A^\times \mid a=bu$.

Prop 38 : Si A est principal, pour $a,b\in A$, on pose $\mathrm{pgcd}(a,b)$ tout générateur de l'idéal $((a),(b))$, et $\mathrm{ppcm}(a,b)$ tout générateur de $(a)\cap(b)$.

[Perr] 61

Ex 40 : Dans $\mathbb{Z}[i\sqrt5]$, 3 et $2+i\sqrt5$ n'ont pas de ppcm et 9 et $6+3i\sqrt5$ n'ont pas de pgcd

On suppose désormais A intègre

[Perr] 67-69

Déf 41 : On appelle système de représentants des irréductibles de A un ensemble P d'irréductibles tel que tout irréductible de A admette un unique associé dans P.

Ex 42 : Les nombres premiers sont un système de représentants des irréductibles de $\mathbb{Z}$.

Déf 43 : L'anneau A est dit factoriel si,
(E) Pour $a\neq0$, a se décompose comme $a=u\prod_{p\in P}p^{v_p(a)}$ où $u\in A^\times$, $v_p(a)\in\mathbb{N}$ presque tous nuls et P est un système de représentants des irréductibles
(U) Cette décomposition est unique
L'entier $v_p(a)$ est la valuation p-adique de a.

Ex 44 : $\mathbb{Z}$ est factoriel, $\mathbb{C}[X]$ est factoriel, $\mathbb{Z}[i\sqrt5]$ n'est pas factoriel : 9 admet deux décompositions 3×3 et $(2-i\sqrt5)(2+i\sqrt5)$.

[Perr] 67-69

Prop 45 : Soit A intègre vérifiant (E). On a équivalence entre
i) A vérifie (U).
ii) Lemme d'Euclide : Si p est irréductible, alors (p) est premier
iii) On a l'équivalence p est irréductible $\iff (p)$ est premier
iv) Lemme de Gauss : Si a divise bc et a et b sont premiers entre eux, alors a divise c

Prop 46 : Tout anneau principal est factoriel

Prop 47 : Dans un anneau factoriel, les pgcd et ppcm existent.

Déf 35 bis : Soient $a,b\in A$, on dit que a et b sont premiers entre eux si 1 et les inversibles sont les seuls diviseurs communs de a et b

Rq 48 : Dans un anneau factoriel, on ne peut utiliser la description de pgcd et ppcm de la prop 37, cependant, pour $a=u\prod_{p\in P}p^{v_p(a)}$ et $b=u'\prod_{p\in P}p^{v_p(b)}$, on peut définir
$$\mathrm{pgcd}(a,b)=\prod_{p\in P}p^{v_p a\wedge v_p b} \qquad \mathrm{ppcm}=\prod_{p\in P}p^{v_p a\vee v_p b}.$$

Théo 49 : Si A est factoriel, $A[X]$ aussi

Prop 50 : Si A est principal on a le théorème de Bézout : si a et b sont premiers entre eux, alors $\exists \lambda,\mu\in A \mid \lambda a+\mu b=1$

Ex 51 : Dans un anneau factoriel, ce fait tombe en défaut : dans $K[X,Y]$, X et Y sont 1^{ers} entre eux.

[Gou1] p175

Prop 52 (Lemme des noyaux) Soit E un K-ev de dim finie, $u\in\mathcal{L}(E)$, et $P=P_1\dots P_r\in K[X]$ avec $P_i\wedge P_j=1$ pr $i\neq j$. Alors $\mathrm{Ker}\,P(u)=\bigoplus_{i}\mathrm{Ker}\,P_i(u)$.

Cor 53 : Un endomorphisme $u\in\mathcal{L}(E)$ est diagonalisable ssi son polynôme minimal est simplement scindé.

2) Théorème des restes chinois.

[Perr] 241-243

Théo 54 : Soit A un anneau commutatif unitaire, I et J des idéaux tels que $(I,J)=A$. On a un isomorphisme $A/(I\cap J)\simeq A/I\times A/J$.

Cor 55 : Soit A principal, $a_1,\dots,a_n$ des éléments premiers entre eux, on a un isomorphisme
$$A/(a_1\dots a_n)\simeq A/a_1\times\dots\times A/a_n$$
envoyant $x[a_1\dots a_n]$ sur $(x[a_1],\dots,x[a_n])$.

Ex 56 : Le système $\begin{cases}x\equiv2[4]\\x\equiv3[5]\\x\equiv1[9]\end{cases}$ admet comme sol $x=118+180k$ $(k\in\mathbb{Z})$ en calc mod 180.

[Per2] 161

Appl 57 : Avec les notations de la prop 52, en notant Π_u son polynôme minimal, si on a une décomposition en produits de facteurs premiers entre eux deux à deux $\Pi_u = P_1 \dots P_r$, alors

$$K[u] = K[X]/(\Pi_u) \simeq K[X]/(P_1) \times \dots \times K[X]/(P_r)$$

On retrouve alors le résultat du corollaire 53.

III. Modules sur les anneaux principaux.

1) Généralités sur les modules.

On fixe A un anneau commutatif unitaire.

Def 58 : Un A-module à gauche est un groupe abélien M, muni d'une loi externe $A \times M \to M$, (on note $a.x$ l'image de (a,x)) telle que

[Gal2] 55-67

- $\forall a,b \in A$, $m \in M$, $(ab)m = a(bm)$ et $(a+b)m = am+bm$
- $\forall a \in A$, $m,n \in M$, $a(m+n) = am+an$, et $1m = m$.

Ex 59 : Un groupe abélien est exactement un $\mathbb{Z}$-module, si A est un corps, on retrouve la définition d'un espace vectoriel.

Def 59 : Soit M, N deux A-modules, $f : M \to N$ un morphisme de groupes, on dit que f est A-linéaire si $\forall a \in A, m \in M$, $f(am) = af(m)$.

Def 60 : Soit M un A-module, un sous-module de M est un A-module N muni d'une application A-linéaire injective $N \to M$.

Def 61 : Soit M un A-module et N un sous module, le quotient de groupes M/N est naturellement muni d'une loi de A-module et la projection canonique $M \to M/N$ est A-linéaire.

Def 62 : Un A-module M est dit libre s'il admet une base (au sens de l'algèbre linéaire). Il est dit de type fini s'il admet une famille génératrice finie.

Théo 63 : Tout A module (resp de type fini) est quotient d'un A-module libre (resp libre et de type fini).

2) Cas des anneaux principaux.

Ici A est principal, les modules sont sur A.

[Com] 146 155

Prop 64 : Si M est un module libre, alors le cardinal d'une base est déterminé par M, on l'appelle la dimension de M. Si N est un sous module de M, alors N est lui aussi libre, de dimension inférieure à celle de M.

Cor 65 : Un sous module d'un module de type fini est de type fini.

Def 66 : Un élément $m \in M$ un module est dit de torsion si il existe $a \in A$ tel que $am = 0$. Les éléments de torsion de M en forment un sous module, noté M_{tor}.

Théo 67 : Soit M un A-module. Alors M/M_{tor} est libre, et M_{tor} admet un supplémentaire libre dans M, dont la dimension est uniquement déterminée par M, on l'appelle le rang de M.

On voit retrouver le théorème de structure qu'on avait pour les groupes abéliens, on reconnaît le dictionnaire associé.

[Com] 146 155

Soit M un A-module, pour $x \in E$, l'application $a \mapsto ax$ est une application linéaire de A (vu comme A-module) dans M, son noyau est un idéal de A, principal, un gen de cet idéal est appelé "période" de x. Un élément de (m) est appelé un exposant de x.

Def 68 : Pour M un A-module et $p \in A$ irréductible, on pose $M(p)$ l'ensemble des éléments de M admettant une puissance de p comme exposant. Il s'agit d'un sous module de M. Un p-sous module de M est un sous module inclus dans $M(p)$.

Fixons à présent P un système de représentants des irréductibles de A.

DVP

Théo 69 : Si M est un A-module de torsion finiment engendré (égal à M_{tor}). Alors M est isomorphe à la somme directe $\bigoplus_{p \in P} M(p)$. Tout sous module de la forme $M(p)$ est lui même isomorphe à la somme directe

$$M(p) \simeq A/(p^{\nu_1}) \oplus \dots \oplus A/(p^{\nu_s})$$

Avec $1 \leq \nu_1 \leq \dots \leq \nu_s$, cette suite est unique.

Théo 70 : Si M est un module de torsion finiment engendré non trivial. Alors M est isomorphe à une somme directe (de facteurs non triviaux)

$$A/(q_1) \oplus \dots \oplus A/(q_r)$$

où $q_1 \dots q_r \in A$ sont non nuls et $q_1 | q_2 \dots | q_r$. Cette suite d'idéaux $(q_1) \dots (q_r)$ est uniquement déterminée avec cette propriété, on l'appelle la suite des invariants de M.

On retrouve le théorème de structure des groupes abéliens de type fini.