# Algèbre de base

Pierron Théo

ENS Ker Lann

# Table des matières

# Première partie

# Anneaux et modules

# Chapitre 0

# Rappels

## 0.1 Relations d'équivalence et quotients

Soit $X$ un ensemble.

**<u>Définition 0.1</u>** Une relation sur $X$ est une partie $\mathcal{R}$ de $X \times X$ où on écrit $x\mathcal{R}y$ ssi $(x, y) \in \mathcal{R}$. Cette relation est dite :

- réflexive ssi $\forall x \in X$, $x\mathcal{R}x$
- transitive ssi $\forall x, y, z \in X$, $x\mathcal{R}y$ et $y\mathcal{R}z$ implique $x\mathcal{R}z$
- symétrique ssi $\forall x, y \in X$, $x\mathcal{R}y \Rightarrow y\mathcal{R}x$
- antisymétrique ssi $\forall x, y \in X$, $x\mathcal{R}y$ et $y\mathcal{R}x \Rightarrow x = y$

Une relation d'équivalence (resp. d'ordre) est une relation réflexive, transitive et symétrique (resp. antisymétrique).

Lorsque $\mathcal{R}$ est une relation d'équivalence, on note souvent $x \sim y$ pour $x\mathcal{R}y$.

**Exemple 0.1** Soit $f : X \to Y$ une application. Notons $x\mathcal{R}x'$ ssi $f(x) = f(x')$. C'est clairement une relation d'équivalence sur $X$, qu'on appelle relation associée à $f$.

**<u>Définition 0.2</u>** Si $\mathcal{R}$ est une relation d'équivalence sur $X$ et $x \in X$, on note $\overline{x} = \{y \in X, y \sim x\}$ la classe d'équivalence de $x$. On note $X/\mathcal{R}$ l'ensemble des classes d'équivalences de $X$ pour $\mathcal{R}$.

**Proposition 0.1** Chaque classe d'équivalence définit une partition de $X$ par les $\overline{x}$ et, réciproquement, toute partition de $X$ définit une relation d'équivalence sur $X$.

<u>THÉORÈME 0.1</u> *Soit $X$ un ensemble, $\mathcal{R}$ une relation d'équivalence sur $X$. On note*

$$\pi : \begin{cases} X & \to & X/\mathcal{R} \\ x & \mapsto & \overline{x} \end{cases}$$

*Alors $\pi$ est surjectif et la relation d'équivalence qui lui est associée est $\mathcal{R}$.*

*De plus, $\pi$ vérifie la* propriété universelle *: Pour tout ensemble $Y$ et toute application $f : X \to Y$ telle que si $x \sim x'$, $f(x) = f(x')$, il existe une unique application $g : X/\mathcal{R} \to Y$ telle que $f = g \circ \pi$.*

$$\begin{tikzcd} X \arrow[r, "\pi"] \arrow[dr, "f"'] & X/\mathcal{R} \arrow[d, "g"] \\ & Y \end{tikzcd}$$

FIGURE 1 – Propriété universelle

*Démonstration.* Il suffit de vérifier que $g$ définie par $g(\overline{x}) = f(x)$ est bien définie. ∎

**Définition 0.3** On dit que $f$ passe au quotient en une application $g$, et que $g$ est induite par $f$ par passage au quotient.

*Remarque 0.1 À cause de la propriété universelle, l'application $\pi : X \to X/\mathcal{R}$ est déterminée à une unique bijection près.*

*Plus précisément, si $\pi_1 : X \to Y_1$ et $\pi_2 : X \to Y_2$ vérifient la propriété universelle, alors il existe une unique bijection $\alpha : Y_1 \to Y_2$ telle que $\pi_2 = \alpha \circ \pi_1$.*

**Exemple 0.2**

- $X = \mathbb{N}$, $m \sim n$ ssi $2 \mid m - n$. $X/\sim = \{0, 1\}$.
- $X = \mathbb{N}^2$, $(a, b) \sim (c, d)$ ssi $a + d = b + c$. $X/\sim = \mathbb{Z}$.
- $X = \mathbb{Z} \times \mathbb{N}^*$, $(a, b) \sim (c, d)$ ssi $ad = bc$. $X/\sim = \mathbb{Q}$.
- $X = \{(\overrightarrow{u}, \overrightarrow{v}) \in E^2 \text{ unitaires}\}$ avec $E$ un plan euclidien, $(\overrightarrow{u}, \overrightarrow{v}) \sim (\overrightarrow{u'}, \overrightarrow{v'})$ ssi il existe une rotation telle que $r(\overrightarrow{u}) = \overrightarrow{u'}$ et $r(\overrightarrow{v}) = \overrightarrow{v'}$. $X/\sim$ est l'ensemble des angles orientés.
- $X = \mathbb{K}^{n+1} \setminus \{0\}$, $\mathbb{K}$ un corps, $v \sim v'$ ssi $\exists \lambda \in k^*$, $v = \lambda v'$. $X/\sim$ est l'espace projectif de dimension $n$ : $\mathbb{P}^n(\mathbb{K})$.
- $X = \mathscr{L}^p$, $f \sim g$ ssi $f - g$ est nulle en dehors d'un négligeable. $X/\sim = L^p$.
- $X = \{u \in \mathbb{Q}^{\mathbb{N}}, u \text{ de Cauchy}\}$. $u \sim v$ ssi $u - v$ converge vers 0. $X/\sim = \mathbb{R}$.
- $X = \mathbb{R}[T]$, $P \sim Q$ ssi $T^2 + 1 \mid P - Q$. $X/\sim = \mathbb{C}$.

*Remarque 0.2 Si $f : X \to Y$ est une application, l'image $f(X)$ sert à mesurer le défaut de surjectivité de $f$ et $X/\mathcal{R}$ sert à mesurer le défaut d'injectivité de $f$ (avec $\mathcal{R}$ associée à $f$).*

 

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "s"] & Y \\ X/\mathcal{R} \arrow[r, hook, two heads, "f'"] & f(X) \arrow[u, hook, "i"'] \end{tikzcd}$$

FIGURE 2 – Quotient et bijectivité

## 0.2 Loi internes compatibles

**Définition 0.4** Une loi de composition interne sur $X$ est une application :

$$\begin{cases} X \times X & \to & X \\ (x, y) & \mapsto & x * y \end{cases}$$

**Proposition 0.2** Soit $\mathcal{R}$ une relation d'équivalence sur $X$ et $\pi : X \to X/\mathcal{R}$ la surjection canonique. Soit $*$ une loi de composition interne sur $X$. Les conditions suivantes sont équivalentes :

i Pour tous $(x, x', y, y') \in X^4$, $(x \sim x'$ et $y \sim y') \Rightarrow x * y \sim x' * y'$

ii Om existe une loi de composition $\overline{*}$ sur $X/\mathcal{R}$ telle que pour tous $(x, y) \in X$, on ait, $\overline{x}\overline{*}\overline{y} = \overline{x * y}$.

*Démonstration.*

i⇒ ii On définit $c\overline{*}d = \overline{x * y}$ avec $c = \overline{x}$ et $d = \overline{y}$.

ii⇒ i Soient $(x, x', y, y') \in X^4$ tel que $x \sim x'$ et $y \sim y'$.
On a $\overline{x * y} = \overline{x}\overline{*}\overline{y} = \overline{x'}\overline{*}\overline{y'} = \overline{x' * y'}$. ∎

Dans ce cas, on dit que $\mathcal{R}$ et $*$ sont compatibles.

## 0.3 Cas des groupes

Soit $G$ un ensemble et $*$ une loi sur $G$.

**Définition 0.5** On dit que :

- $*$ est associative ssi pour tout $(x, y, z) \in G^3$, $(x * y) * z = x * (y * z)$
- $*$ est commutative ssi pour tout $(x, y) \in G^2$, $x * y = y * x$
- $e \in G$ est neutre pour $*$ ssi pour tout $x \in G$, $x * e = e * x = x$ (unicité si existence)
- $x' \in G$ est un symétrique de $x \in G$ ssi $x * x' = x' * x = e$ (unicité si existence)

 

**Proposition 0.3** Soit $G$ muni de $*$ et $\mathcal{R}$ une relation d'équivalence sur $G$ compatible avec $*$. Soit $\overline{*}$ la loi induite sur $G/\mathcal{R}$.

Alors si $*$ est associative (resp. commutative, possède un neutre,...) alors $\overline{*}$ aussi.

**Définition 0.6** Un groupe est un ensemble $G$ muni d'une loi $*$ associative, possédant un neutre $e$ epour laquelle tout élément possède un symétrique.

Par convention, dans un groupe, la loi est notée multiplicativement : $x * y \to xy$, $e \to 1$ et $x' \to x^{-1}$. Exception notable pour les groupes abéliens, on note la loi additivement : $x * y \to x + y$, $e \to 0$ et $x' \to -x$.

On renvoie au magnifique cours de THGR pour les définitions usuelles sur les groupes.

**Définition 0.7** Un sous-groupe $H \subset G$ est dit distingué ssi pour tout $h \in H$ et pour tout $g \in G$, $ghg^{-1} \in H$. On note alors $H \lhd G$.

**Exemple 0.3** Soit $G$ un groupe et $H$ un sous-groupe.

$x \sim_d y$ ssi $xy^{-1} \in H$ et $x \sim_g y$ ssi $y^{-1}x \in H$.

$\sim_g$ et $\sim_d$ sont des relations d'équivalence et $H$ est distingué ssi les classes des deux relations sont les mêmes.

**Proposition 0.4** Si $f : G \to H$ est un morphisme de groupes, son image $\mathrm{Im}(f) = f(G)$ est un sous-groupe (non distingué en général, ex : si $H \not\lhd G$, le morphisme d'inclusion n'a pas une image distinguée) de $H$ et son noyau $\mathrm{Ker}(f) = f^{-1}(1_H)$ est un sous-groue distingué de $G$.

Tout sous-groupe distingué est noyau d'un morphisme.

Théorème 0.2 *Soit $G$ un groupe et $N \lhd G$. Il existe un groupe $G/N$ et un morphisme de groupes $\pi : G \to G/N$ surjectif qui vérifie la propriété universelle suivante : pour tout groupe $H$ et tout morphisme $f : G \to H$ tel que $N \subset \mathrm{Ker}(f)$, il existe un unique morphisme $f' : G/N \to H$ tel que $f = f' \circ \pi$.*

*De plus, $N \lhd \mathrm{Ker}\, f$ et $\mathrm{Ker}\, f' = \mathrm{Ker}\, f/N$. On a aussi $\mathrm{Im}\, f = \mathrm{Im}\, f'$.*

*Démonstration.* On note $\sim$ la relation d'équivalence définie par $x \sim y$ ssi $xy^{-1} \in N$. On note $G/N = G/\sim$.

$\sim$ est compatible avec la loi de $G$ donc il y a une loi induite sur $G/N$. ∎

*Remarque 0.3 Avec les mêmes notations, si on dispose d'un morphisme surjectif $\rho : G \to Q$ de noyau $N$, on peut lui appliquer le théorème assure l'existence de $\rho'$ tel que $\rho = \rho' \circ \pi$. On a $\mathrm{Ker}(\rho') = N/N = \{1\}$ et $\mathrm{Im}(\rho') = \mathrm{Im}(\rho) = Q$.*

*Donc $\rho'$ est bijectif.*

 

**Exemple 0.4** $G = GL_n(\mathbb{K})$ et $H = SL_n(\mathbb{K})$. det : $G \to \mathbb{K}^*$ est surjectif de noyau $SL_n$ donc induit une bijection de $G/H$ dans $\mathbb{K}^*$.

**Exemple 0.5** Soit $G$ un groupe, $N \lhd G$, $\pi : G \to G/N$. Si $H \supset N$ est un sous-groupe de $G$, $\pi(H)$ est un sous-groupe de $G/N$.

$\pi$ est une bijection de l'ensemble des sous-groupes de $G$ contenant $N$ sur l'ensemble des sous-groupes de $G/N$.

 

# Chapitre 1

# Théorie générale des anneaux et modules

## 1.1 Anneaux

**Définition 1.1** Un anneau est un triplet $(A, +, \times)$ tel que :
- $(A, +)$ est un groupe commutatif d'élément neutre 0
- $\times$ est associative et possède un neutre 1
- $\times$ est distributive à gauche et à droite sur $+$ : $\forall x, y, z \in A$, $x(y+z) = xy + xz$

L'anneau est dit commutatif ssi $\times$ l'est.

*Remarque 1.1*
- *Il existe des notions (intéressantes) d'anneaux non associatifs, ou non unitaires, ou avec* $1 = 0$.
- *Si* $1 = 0$, $A = \{0\}$.
- $(A, \times)$ *n'est pas un groupe (0 n'a pas d'inverse).*

**Exemple 1.1**
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux commutatifs.
- $\mathbb{Z}[i]$ est un anneau.
- $\mathbb{F}_p$ est un anneau, de même que les $\mathbb{Z}/n\mathbb{Z}$.
- $\mathfrak{M}_n(\mathbb{K})$ est un anneau.
- La $\mathbb{R}$-algèbre des quaternions $\mathbb{H}$ est un anneau.
- Les anneaux de polynômes $\mathbb{K}[X]$, de fonctions $A^E$ ($E$ ensemble, $A$ anneau)

**Définition 1.2** Soient $A$ et $B$ deux anneaux. Un morphisme d'anneaux $f : A \to B$ est un morphisme de groupe $(A, +) \to (B, +)$ et tel que pour tout $(x, y) \in A^2$, $f(xy) = f(x)f(y)$ et $f(1_A) = 1_B$.

*Remarque 1.2* *Pour tout anneau $A$, il existe un unique morphisme d'anneaux $\mathbb{Z} \to A$.*

**Définition 1.3** Un sous-anneau de $A$ est un sous-groupe de $A$ contenant $1_A$ et stable par $\times$.

*Remarque 1.3*
- *Si $f : A \to B$ est un morphisme, alors $f(A)$ est un sous-anneau de $B$. En revanche, le noyau n'est pas un sous-anneau car $f(1) = 1 \neq 0$ donc $1 \notin \operatorname{Ker} f$.*
- *L'intersection d'une famille quelconques de sous-anneaux est un sous-anneau. Par ailleurs, si $S$ est une partie d'un anneau $A$, l'intersection de tous les sous-anneaux de $A$ qui contiennent $S$ est un sous-anneau de $A$ appelé sous-anneau engendré par $S$.*

**Définition 1.4** Soit $A$ un anneau, $S \subset A$. L'ensemble des $x \in A$ qui commutent avec tous les éléments de $S$ est un sous-anneau de $A$ appelé commutant de $S$. Si $S = A$, le commutant est appelé centre de $A$ souvent noté $Z$.

Si $x$ est dans le commutant de $S$, on dit que $x$ centralise $S$. Si $S = A$, $x$ est dit central.

*Remarque 1.4* *Le centre est commutatif.*

**Définition 1.5** Soit $A$ un anneau, $x \in A$.
- $x$ est dit nilpotent ssi il existe $n \neq 0$ tel que $x^n = 0$.
- $x$ est dit inversible à gauche (resp. à droite) ssi il existe $y \in A$ tel que $yx = 1$ (resp. $xy = 1$)
- $x$ est dit régulier (ou non-diviseur de 0 ou simplifiable) à gauche (resp. à droite) ssi pour tout $y \in A$, $xy = 0 \Rightarrow y = 0$.
- $x$ est inversible, régulier, non-diviseur de 0, simplifiable ssi il l'est à gauche et à droite.
- $A$ est une algèbre à division, ou un corps gauche ssi ses éléments non nuls sont inversibles.
- Si de plus $A$ est commutatif, $A$ est intègre ssi ses éléments non nuls sont non-diviseurs de 0
- Une algèbre à division commutative est un corps.

*Remarque 1.5*
- *Si $x$ possède un inverse à gauche, il est régulier à gauche.*
- *La définition de régularité à gauche porte sur $\gamma_x : y \mapsto xy$ alors que l'inversibilité à gauche porte sur $\delta_x : y \mapsto yx$.*
- *L'ensemble des inversibles de $A$ est un groupe pour $\times$ noté $A^*$ ou $A^\times$.*

**Exemple 1.2** Anneaux intègres :

 

- $\mathbb{Z}$
- $\mathbb{Z}/n\mathbb{Z}$ est intègre ssi $n$ est premier ou $n = 0$.
- $C^0(\mathbb{R}, \mathbb{R})$ n'est pas intègre.
- L'ensembles des fonctions holomorphes $\mathcal{H}(U)$ sur un ouvert $U$ non vide et connexe est intègre.
- Si $A$ est intègre, $A[X]$ aussi.

Corps :

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- Si $\mathbb{K}$ est un corps, $\mathbb{K}(X) = \mathrm{Frac}(\mathbb{K}[X])$ est aussi un corps. On a $\mathcal{M}(U) = \mathrm{Frac}(\mathcal{H}(U))$ (fonctions méromorphes).

**Exemple 1.3** Soit $\mathbb{K}$ un corps, $E$ un $\mathbb{K}$-ev, $A = \mathscr{L}(E)$. $f$ est régulier à gauche ssi $f$ est injectif ssi $f$ est inversible à gauche.

De même, $f$ est régulier à droite ssi $f$ est surjectif ssi $f$ est inversible à droite.

## 1.2 Quelques exemples d'anneaux

### 1.2.1 Anneaux de polynômes

Soit $A$ un anneau non commutatif. On note $A[X]$ l'ensemble des polynômes à coefficients dans $A$, ie l'ensemble des suites presques nulles, muni de l'addition terme à terme et du produit de Cauchy.

On note $X$ la suite presque nulle $(\delta_{1,n})_{n\in\mathbb{N}}$. $X$ est alors central.

Si $F = (f_n)_n$, on définit le degré

$$\deg(F) = \begin{cases} \max\{n, f_n \neq 0\} & \text{si } \exists n, f_n \neq 0 \\ -\infty & \text{sinon} \end{cases}$$

et le coefficient dominant de $F$ (noté $\mathrm{cd}(F)$) par $f_{\deg(F)}$ si $\deg(F) \neq \infty$ et 0 sinon.

**Proposition 1.1** On a $\deg(FG) \leqslant \deg(F) + \deg(G)$ avec égalité si $\mathrm{cd}(F)$ est régulier à gauche ou si $\mathrm{cd}(G)$ est régulier à droite.

<u>Théorème 1.1</u> *Soient $F, G$ deux polynômes tels que $\mathrm{cd}(G)$ soit inversible. Alors :*

- *Il existe un unique couple $(Q, R) \in A[X]^2$ tel que $F = GQ + R$ et $\deg(R) < \deg(G)$.*
- *Il existe un unique couple $(Q', R') \in A[X]^2$ tel que $F = Q'G + R'$ et $\deg(R') < \deg(G)$.*

*Démonstration.* Notons $aX^m$ et $bX^n$ les monômes dominants de $F$ et $G$.

 

$\exists$ : Si $m < n$, on prend $Q = 0$ et $R = F$. Sinon, on fait une récurrence sur $m$. Le cas précédent l'initialise. Ensuite, on observe que $\mathrm{cd}(Gb^{-1}aX^{m-n}) = aX^m$.
On a $\deg(F - Gb^{-1}aX^{m-n}) < m$ donc par hypothèse de récurrence, il existe un couple $(Q^*, R^*)$ tel que $F - Gb^{-1}aX^{m-n} = GQ^* + R^*$ et $\deg(R^*) < \deg(G)$ donc $F = G(\underbrace{b^{-1}aX^{m-n} + Q^*}_{Q}) + R^*$.

! : Si on a deux couples $(Q_1, R_1)$ et $(Q_2, R_2)$ qui marchent, alors $G(Q_1 - Q_2) = R_2 - R_1$.
Comme $\mathrm{cd}(G)$ est régulier à gauche, on a $\deg(G) + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) < \deg(G)$ donc $Q_1 = Q_2$ et $R_1 = R_2$. ∎

**Exemple 1.4** Soit $Z$ le centre de $A$. Le centre de $A[X]$ est $Z[X]$.

Soit $F \in A[X]$ et $\alpha \in A$. Si $F = \sum\limits_{n \geqslant 0} f_n X^n$, on définit $F_g(\alpha) = \sum\limits_{n \geqslant 0} \alpha^n f_n$.

Le reste de la division euclidienne à gauche de $F$ par $X - \alpha$ est $F_g(\alpha)$. (En effet, $F - F_g(\alpha) = \sum\limits_{n \geqslant 0} (X^n - \alpha^n) f_n$ et $X - \alpha \mid X^n - \alpha^n$)

*Remarque 1.6 Si tous les coefficients de $F$ commutent avec tous les coefficients de $G$ alors $Q = Q'$ et $R = R'$.*

### 1.2.2 Anneaux et matrices

Soit $R$ un anneau de centre $Z$ et $n \geqslant 1$. On note $\mathfrak{M}_n(R)$ l'anneau des matrices carrées de taille $n$ muni des lois habituelles.

Cet anneau n'est pas commutatif dès que $n \neq 1$ ou $R$ non commutatif.

Son centre est l'ensemble $Z\,\mathrm{Id}$.

Il y a un isomorphisme canonique entre $\mathfrak{M}_n(R[X])$ et $\mathfrak{M}_n(R)[X]$ via :

$$\left(\sum_{p=0}^{n} m_{i,j}^{(p)} X^p\right)_{i,j} \mapsto \sum_{p=0}^{n} m_p X^p$$

où $m_p = (m_{i,j}^{(p)})_{i,j}$.

### 1.2.3 Produit d'anneaux, anneaux de fonctions

Soit $(A_i)_{i \in I}$ une famille d'anneaux avec $I$ un ensemble. Le produit des $A_i$ est l'anneau $\prod\limits_{i \in I} A_i$.

 

Ses éléments sont des familles $(a_i)_{i\in I}$, produit cartésien d'ensembles avec $a_i \in A_i$, muni des lois d'addition et de multiplication coordonnée par coordonnée. Pour chaque $j \in I$, on a une projection $\pi_j : (a_i)_i \to a_j$ qui est un morphisme d'anneau.

Le produit $A$ muni de ses projections vérifie la propriété universelle suivante : Pour tout anneau $B$ et toute famille de morphismes $(f_i)_{i\in I} : B \to A_i$, il existe un unique $f : B \to A$ tel que pour tout $i \in I$, $\pi_i \circ f = f_i$.

$$\begin{tikzcd}
 & & A_j \\
B \arrow[r, "f"] \arrow[urr, "f_j"] \arrow[drr, "f_k"'] & A \arrow[ur, "\pi_j"'] \arrow[r] \arrow[dr, "\pi_k"] & \cdots \\
 & & A_k
\end{tikzcd}$$

FIGURE 1.1 – Factorisation des morphismes dans un produit d'anneaux

Si tous les $A_i$ sont égaux à un même anneau $A$, leur produit est l'anneau $A^I$ des fonctions de $I$ dans $A$.

**Exemple 1.5** Soit $I$ un ensemble. On a un isomorphisme d'anneaux :

$$\begin{cases} (\mathcal{P}(I), \Delta, \cap) & \to & I^{\mathbb{Z}/2\mathbb{Z}} \\ A & \mapsto & 1_A \end{cases}$$

### 1.2.4 Espaces $\mathscr{L}^p$ et $L^p$ avec $p \geqslant 1$

Si $p = 2$, l'inégalité de Hölder implique que $\mathscr{L}^p$ et $L^p$ sont des anneaux.

Si $p = 1$ et qu'on se place sur $\mathbb{R}$, on peut munir $L^1$ du produit de convolution. On obtient un anneau non unitaire. (Ça marche aussi pour $\mathscr{L}^1$.)

## 1.3 Idéaux

**Définition 1.6** Soit $A$ un anneau. Un idéal à gauche est un sous groupe $I$ de $(A, +)$ stable par multiplication à gauche par les élements de $A$.

Un idéal bilatère est un idéal à gauche et à droite. On dit que $A$ est simple ssi il n'a pas d'idéal bilatère différent de $\{0\}$ et $A$.

*Remarque 1.7 Le seul idéal qui est un anneau est $A$.*

**Définition 1.7** Pour tout $S \subset A$, l'intersection des idéaux de $A$ qui la contiennent est un idéal, c'est le plus petit qui contient $S$. On l'appelle idéal engendré par $S$.

Soit $(I_\lambda)_\lambda$ une famille d'idéaux à gauche. On appelle somme des $I_\lambda$ et on note $\sum\limits_\lambda I_\lambda$, l'idéal à gauche engendré par la réunion des $I_\lambda$.

Soient $I_1, \cdots, I_n$ des idéaux bilatères. On appelle produit des $I_k$ l'idéal engendré par les produits $i_1 \dots i_n$.

**Exemple 1.6**

- Dans $\mathbb{Z}$, on montre que tout idéal est principal ie est engendré par un seul élément. On a de plus $(a)+(b) = (a \wedge b)$, $(a) \cap (b) = (a \vee b)$ et $(a)(b) = (ab)$.
- Si $B \in A^E$ et $x \in E$, alors $\{f \in B, f(x) = 0\}$ est un idéal bilatère.
- Soit $A$ un anneau et $I, J$ deux idéaux à gauche. Alors

$$(I \colon J)_A = \{a \in A, aJ \subset I\}$$

  Si $I = 0$, on note $\mathrm{Ann}(J) = (0 \colon J) = \{a \in A, aJ = \{0\}\}$ l'idéal annulateur de $J$.
- Soit $E$ un $\mathbb{K}$-ev, $F$ un sev de $E$, $A = L(E)$.
  $\{f \in A, F \subset \mathrm{Ker}(f)\}$ est un idéal à gauche de $A$ et $\{f \in A, \mathrm{Im}(f) \subset F\}$ est un idéal à droite de $A$.

**Proposition 1.2** Soit $f : A \to B$ un morphisme d'anneaux.

La préimage d'un idéal à gauche de $B$ est un idéal à gauche.

Si $f$ est surjectif, l'image d'un idéal à gauche de $A$ est un idéal à gauche.

*Démonstration.*

- Soit $I$ un idéal à gauche. On pose $J = f(I)$.
  Soit $x, y \in J$. Par surjectivité, $x = f(x')$ et $y = f(y')$ et on a $x + y = f(x' + y')$ donc $x + y \in J$.
  Soit $x \in J$ et $a \in B$, on a $x = f(x')$ et $a = f(a')$ donc $ax = f(a'x') \in J$
- Soit $I$ un idéal de $B$. On pose $J = f^{-1}(I)$.
  Soit $x, y \in J$ et $a \in A$. $f(x+y) = f(x) + f(y) \in I$ donc $x + y \in J$. De plus, $f(ax) = f(a)f(x) \in I$ donc $J$ est un idéal. ∎

**Proposition 1.3** Tout idéal bilatère est noyau d'un morphisme de source $A$ (théorème de quotient).

<u>Théorème 1.2</u> De quotient *Soit $A$ un anneau, $I$ un idéal bilatère. Il existe un anneau $A/I$ et un morphisme $\pi : A \to A/I$ tel que pour tout anneau $B$ et tout morphisme $f : A \to B$ dont le noyau contient $I$, il existe un unique morphisme $f' : A/I \to B$ tel que $f = f' \circ \pi$.*

 

*Le morphisme $\pi$ est surjectif de noyau $I$. On a de plus* $\mathrm{Im}(f) = \mathrm{Im}(f')$ *et* $\mathrm{Ker}(f') = \mathrm{Ker}(f)/I$.

*Démonstration.* On considère la relation d'équivalence sur $A$ définie par $x \sim y$ ssi $x - y \in I$. On vérifie que cette relation est compatible avec $+$ et $\times$. ∎

*Remarque 1.8 Si $f : A \to B$ est un morphisme surjectif de noyau $I$. La propriété universelle donne un $f' : A/I \to B$ qui est un isomorphisme qui identifie $B$ à $A/I$.*

**Exemple 1.7** $A' = A^E$, $I = \{f \in A', f(x) = 0\}$ où $x \in E$ est fixé.

Le morphisme d'évaluation en $x$ est surjectif de noyau $I$, donc induit un isomorphisme de $A'/I$ sur $A$.

**Proposition 1.4** Il y a une bijection entre les idéaux de $A$ qui contiennent $I$ et les idéaux de $A/I$.

**Proposition 1.5** Soit $A$ un anneau et $I \subset J$ deux idéaux bilatères. Il y a un isomorphisme canonique entre $(A/I)/(J/I)$ et $A/J$.

*Démonstration.* On applique la propriété universelle de $A/I$ à la projection canonique $f : A \to A/J$, ce qui nous donne $f' : A/I \to A/J$.

On applique à $f'$ la propriété universelle de $(A/I)/(J/I)$ et on a le résultat. ∎

**Exemple 1.8**

- Si $m \mid n$, on a $(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}$.
- $A = \mathbb{R}[T]$, $I = (T^2 + 1)$ et

$$f : \begin{cases} \mathbb{R}[T] & \to & \mathbb{C} \\ P & \mapsto & P(i) \end{cases}$$

  induit un isomorphisme $f' : \mathbb{R}[T]/(T^2 + 1) \to \mathbb{C}$.
  $f'$ est surjectif car $a + ib \in \mathbb{C}$ est l'image de $\overline{a + bT}$.
  $f'$ est injectif car si $P \in \mathrm{Ker}(f)$, $P(i) = 0$ donc $P = (T^2+1)Q + R$ avec $\deg(R) < 2$. On a $R(i) = a + bi = 0$ donc $a = b = 0$ donc $T^2 + 1 \mid P$. Ainsi, $\mathrm{Ker}(f) = I$ donc $\mathrm{Ker}(f') = I/I = \{0\}$.
- $A$ l'anneau des suites de Cauchy de $\mathbb{Q}^{\mathbb{N}}$, $I$ l'idéal de celles qui convergent vers 0. Par complétude de $\mathbb{R}$, lim est un morphisme surjectif de noyau 0 qui induit donc un isomorphsime $A/I \to \mathbb{R}$.

 

## 1.4 Idéaux des anneaux commutatifs

On suppose $A$ commutatif.

**Définition 1.8** Un idéal $I \subset A$ est dit premier ssi $A/I$ est intègre, ie pour tout $x, y \in A$, $xy \in I \Rightarrow x \in I$ ou $y \in I$.

**Définition 1.9** Un idéal $I \subset A$ est dit maximal ssi $A/I$ est un corps, ie pour tout $x \in A \setminus I$, il existe $y \in A$ tel que $xy - 1 \in I$. C'est équivalent à dire qu'il n'y a aucun idéal strict $J$ de $A$ tel que $I \subsetneq J$.

En effet, si ce n'est pas le cas, $A/I$ a un idéal strict $(J/I)$ donc $J/I = \{0\}$.

**Lemme 1.2.1 Zorn**
Soit $E$ un ensemble partiellement ordonné. On appelle chaîne de $E$ tout sous-ensemble qui est totalement ordonnée. On dit que $E$ est inductif ssi toute chaîne de $E$ admet une borne supérieure dans $E$.

Tout ensemble inductif non vide admet des éléments maximaux.

**Définition 1.10** On appelle bon ordre sur $E$ un ordre tel que toute partie non vide de $E$ admette un plus petit élément.

**Proposition 1.6** Tout ensemble peut être muni d'un bon ordre (équivalent à l'axiome du choix).

THÉORÈME 1.3 KRULL *Tout anneau commutatif possède un idéal maximal.*

*Démonstration.* On va montrer que si $I \subset A$ est un idéal strict, il existe un idéal maximal qui contient $I$.

Soit $E$ l'ensemble des idéaux stricts de $A$ qui contiennent $I$. On sait que $E$ est non vide puisqu'il contient $I$.

De plus, si on munit $E$ de l'ordre partiel défini par l'inclusion, il est inductif : soit $(I_\lambda)_\lambda$ une famille d'idéaux totalement ordonnée, alors l'idéal somme $J$ est une borne supérieure. en effet, il est clair que $J$ est le plus petit idéal de $A$ contenant tous les $I_\lambda$ et $I$ est stricte car si $1 \in I$, il existe $\lambda$ tel que $1 \in I_\lambda$ donc $I_\lambda = A$. Contradiction. Le lemme de Zorn assure alors le résultat. ∎

COROLLAIRE 1.1 *Tout anneau commutatif possède un morphisme surjectif vers un corps.*

*Démonstration.* Soit $I$ un idéal maximal, la projection canonique $A \to A/I$ répond à la question. ∎

**Lemme 1.3.1**
Soit $A$ un anneau commutatif. L'ensemble $\mathrm{Nil}(A)$ des éléments nilpotents de $A$ est un idéal.

 

*Démonstration.* Si $x \in \mathrm{Nil}(A)$ et $a \in A$, il existe $n$ tel que $x^n = 0$. Par commutativité, $(ax)^n = a^n x^n = 0$ donc $ax \in \mathrm{Nil}(A)$.

Si $x, y \in \mathrm{Nil}(A)$, il existe $m, n$ tel que $x^m = y^n = 0$. Par le binôme, on obtient que $(x+y)^{n+m-1} = 0$. ■

<u>Théorème 1.4</u> *Dans un anneau commutatif $A$, $\mathrm{Nil}(A)$ est l'intersection de tous les idéaux premiers de $A$.*

*Démonstration.*

$\subset$ Si $x^n = 0$, pour tout idéal $I$ premier, on a $x^n = 0 \in I$ donc $x \in I$.

$\supset$ Soit $x \in A$ non nilpotent. La partie $S = \{x^n, x \in \mathbb{N}\}$ ne contient pas 0. Soit $E$ l'ensemble des idéaux de $A$ qui ne rencontrent pas $S$, ordonné par l'inclusion. $E$ est non vide car contient $\{0\}$. $E$ est inductif car si $(I_\lambda)_\lambda$ est une chaîne de $E$, leur réunion est un idéal qui ne rencontre pas $S$.

Il existe donc un élément maximal $\mathfrak{p}$ de $E$. Montrons que $\mathfrak{p}$ est premier. Soit $\alpha, \beta \in A$ tel que $\alpha \notin \mathfrak{p}$ et $\beta \notin \mathfrak{p}$.

Les idéaux $\mathfrak{p} + (\alpha)$ et $\mathfrak{p} + (\beta)$ contiennent $\mathfrak{p}$ strictement. Comme $\mathfrak{p}$ est maximal parmi les ensembles qui ne rencontrent pas $S$, $\mathfrak{p} + (\alpha)$ et $\mathfrak{p} + (\beta)$ rencontrent $S$. Il existe donc $u, v \in \mathfrak{p}$, $e, f \in A$ et $m, n \in \mathbb{N}$ tel que $u + e\alpha = x^m$ et $v + f\beta = x^n$.

On a $uv + uf\beta + ve\alpha + ef\alpha\beta = x^{m+n} \in S$. Or $(uv, uf\beta, ve\alpha) \in \mathfrak{p}^3$. On ne peut pas avoir $\alpha\beta \in \mathfrak{p}$ sinon $\mathfrak{p}$ rencontrerait $S$. Donc $\mathfrak{p}$ est premier. ■

Corollaire 1.2 *Soit $A$ un anneau commutatif. Alors $A$ est réduit (ie n'a pas d'élément nilpotent non nul) ssi il s'injecte dans un produit de corps.*

*Remarque 1.9 Ce corollaire est à mettre en parallèle avec $A$ intègre ssi il s'injecte dans un corps.*

*Démonstration.* S'il existe un morphisme injectif $f : A \hookrightarrow \prod_{i \in I} K_i$, et si $a \in A$ est nilpotent, il existe $n$ tel que $a^n = 0$ donc $f(a)^n = 0$. Si $f(a) = (x_i)_i$, on a $x_i^n$ donc comme $K_i$ est un corps, $x_i = 0$ donc $a = 0$ par injectivité.

Réciproquement, si $A$ est réduit, pour chaque idéal premier $\mathfrak{p} \subset A$, on note $K_{\mathfrak{p}} = \mathrm{Frac}(A/\mathfrak{p})$. On a un morphisme d'anneaux

$$\begin{cases} A & \to & \prod_{\mathfrak{p}} A/\mathfrak{p} = \prod_{\mathfrak{p}} K_p \\ a & \mapsto & (\pi_{\mathfrak{p}}(a))_{\mathfrak{p}} \end{cases}$$

Ce morphisme est injectif car si l'image de $a$ est 0, cela signifie que $a \in \mathrm{Ker}(\pi_{\mathfrak{p}})$ pour tout $\mathfrak{p}$. Donc $a \in \mathrm{Nil}(A) = 0$. ■

 

## 1.5 Modules

**Définition 1.11** Soit $A$ un anneau. Un $A$-module à gauche est un groupe commutatif $M$ muni d'une application $\cdot : A \times M \to M$ telle que :
- Pour tout $a \in A$, $m, m' \in M$, $a(m + m') = am + am'$.
- Pour tout $a, b \in A$, $m \in M$, $(a + b)m = am + bm$.
- Pour tout $a, b \in A$, $m \in M$, $(ab)m = a(bm)$.
- Pour tout $m \in M$, $1m = m$

*Remarque 1.10*
- *Il y a une notion de module à droite.*
- *Pour tout anneau $A$, il existe un anneau $A^0$ ou $A^{opp}$ appelé anneau opposé de $A$ tel que $A^0 = A$, $+^0 = +$ et $a \times^0 b = ba$.*
- *Un morphisme d'anneaux $A \to B^0$ est une application $f : A \to B$ additive, qui envoie $1$ sur $1$ et vérifie $f(ab) = f(b)f(a)$. On appelle $f : A \to B$ un antimorphisme. On a donc une correspondance entre les modules à gauche et à droite.*

**Exemple 1.9**
- Le groupe additif $(A, +)$ d'un anneau $A$ est muni d'une structure de module sur $A$.
- Si $A$ est un corps, le module est un espace vectoriel.
- Si $A = \mathbb{Z}$, on a en fait une structure sous-jacente de groupe commutatif.
- Si $E$ est un $k$-espace vectoriel, tout $u \in L(E)$ définit une structure de $k[X]$ module sur $E$ :

$$\begin{cases} k[X] \times E & \to & E \\ (P, v) & \mapsto & P(u)(v) \end{cases}$$

  On note $E_u$ ce module.
- Si $A$ est un anneau et $I$ un ensemble, alors $A^I$ est muni d'une structure de $A$-module composante par composante.
- Un morphisme d'anneaux $f : A \to B$ munit $B$ d'une structure de $A$-module via $ab = f(a)b$.

**Définition 1.12**
- Un morphisme de $A$-module entre deux $A$ modules $M$, $N$ est un morphisme de groupes commutatifs $f : M \to N$ tel que pour tout $x \in M$ et $a \in A$, $f(ax) = af(x)$.
- Le noyau $\mathrm{Ker}(f)$ (resp. l'image $\mathrm{Im}(f)$) est le noyau (resp. l'image) du morphisme de groupe $f$.
- Une application $n$-multilinéaire (alternée) est une $f : M_1 \times \ldots \times M_n \to N$ tel que pour tout $i$ et $(x_j)_{j \neq i}$, $f(x_1, \ldots, x_{i-1}, \cdot, x_{i+1}, \ldots, x_n)$ est $A$-linéaire (et s'annule dès que deux variables sont égales).

 

**Exemple 1.10** Si $A$ est un anneau commutatif, l'ensemble $\hom_A(M, N)$ des morphismes de $A$-modules de $M$ dans $N$ est muni d'une structure naturelle de $A$-module.

**Définition 1.13** Un sous-$A$-module d'un module $M$ est un sous-groupe $N \subset M$ tel que pour tout $a \in A$ et $x \in N$, $ax \in N$.

**Exemple 1.11** Les sous-$A$-modules de $A$ sont ses idéaux.

**Proposition 1.7**

- Si $f : M \to N$ est un morphisme, $\mathrm{Ker}(f) \subset M$ est un sous-module, de même que $\mathrm{Im}(f) \subset N$.
- Soit $M$ un $A$-module, $S \subset M$ une partie. L'intersection des sous-modules de $M$ qui contiennent $S$ est un sous-module. C'est le plus petit sous-module de $M$ qui contient $S$. C'est aussi l'ensemble des sommes finies de termes de la forme $as$ avec $a \in A$ et $s \in S$
- Si $M$ est un $A$-module et $I \subset A$ un idéal, alors le sous-module engendré par les éléments de la forme $ix$ avec $i \in I$ et $m \in M$ est noté $IM$. C'est un sous-module de $M$.
- Soit $M$ un module, $N, P$ des sous-modules. On définit $(P : N)_A = \{a \in A, aN \subset P\}$ qui est un idéal de $A$ et $\mathrm{Ann}(M) = (0 : M)$ l'annulateur de $M$. Par exemple, si $A = \mathbb{Z}$, $M = \mathbb{Z}/n\mathbb{Z}$, $\mathrm{Ann}_{\mathbb{Z}}(M) = n\mathbb{Z}$.
  Si on prend $A = \mathbb{Z}/n\mathbb{Z}$, $\mathrm{Ann}_{\mathbb{Z}/n\mathbb{Z}}(M) = \{0\}$. De plus, si $n \mid m$, on a $\mathrm{Ann}_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) = n\mathbb{Z}/m\mathbb{Z}$.

THÉORÈME 1.5 *Soit $M$ un $A$-module à gauche et $N \subset M$ un sous-$A$-module. Il existe un $A$-module $M/N$ est un morphisme surjectif de $A$-modules $\pi : M \to M/N$ tel que pour tout $A$-module $P$ et tout morphisme $f : M \to P$ tel que $N \subset \mathrm{Ker}(f)$, il existe un unique morphisme $f' : M/N \to P$ tel que $f = f' \circ \pi$.*

*De plus,* $\mathrm{Im}(f') = \mathrm{Im}(f)$ *et* $\mathrm{Ker}(f') = \pi(\mathrm{Ker}(f))$.

*Remarque 1.11 Par conséquent, tout morphise $f : M \to P$ surjectif de noyau $N$ induit un isomorphisme $f' : M/N \to P$.*

Soit $A$ un anneau, $(M_i)_i$ une famille de $A$-modules.

**Définition 1.14**

- Le produit direct est l'ensemble $M = \prod_{i \in I} M_i$ muni de la structure de $A$-module définie par la somme terme à terme et la produit par un scalaire terme à terme.
- La somme directe $M' = \bigoplus_{i \in I} M_i$ est le sous-module de $\prod_{i \in I} M_i$ dormé des familles $(x_i)_i$ telles que $x_i = 0$ pour tout $i$ sauf un nombre fini.

 

**Exemple 1.12** $k[X] = \bigoplus\limits_{n \geqslant 0} k$ et $k[\![X]\!] = \prod\limits_{n \geqslant 0} k$.

**Proposition 1.8** Le produit direct est muni de morphismes surjectifs de $A$-modules

$$\pi_j : \begin{cases} \prod\limits_{i \in I} M_i & \to & M_j \\ (x_i)_i & \mapsto & x_j \end{cases}$$

La somme directe est munie de morphismes injectifs de $A$-modules

$$\alpha_j : \begin{cases} M_j & \to & M' = \bigoplus\limits_{i \in I} M_i \\ x & \mapsto & (x_i)_i \text{ où } \begin{cases} x_j & = x \\ x_i & = 0 \end{cases} \end{cases}$$

<u>Théorème 1.6</u> Propriété universelle du produit *Pour tout module $N$ sur $A$ et toute famille de morphismes $f_k : N \to M_j$, il existe un unique morphisme $f' : N \to M$ tel que $f_j = \pi \circ f'$.*

$$\begin{tikzcd}
 & & M_l \\
N \arrow[rru, "f_l"] \arrow[r, dashed, "f'"] \arrow[rrd, "f_k"'] & M \arrow[ru, "\pi_l"'] \arrow[rd, "\pi_k"] & \\
 & & M_k
\end{tikzcd}$$

Figure 1.2 – Propriété universelle du produit

<u>Théorème 1.7</u> Propriété universelle de la somme directe *Pour tout $A$-module $N$ et toute famille de morphismes $g_j : M_j \to N$, il existe un unique morphisme $g : M \to N$ tel que $g_j = g \circ \alpha_j$.*

$$\begin{tikzcd}
 & & M_l \arrow[lld, "g_l"'] \arrow[ld, "\alpha_l"] \\
N & M \arrow[l, dashed, "g"'] & \\
 & & M_k \arrow[llu, "g_k"] \arrow[lu, "\alpha_k"']
\end{tikzcd}$$

Figure 1.3 – Propriété universelle de la somme

*Remarque 1.12 La somme directe est le sous-module du produit engendré par les $\alpha_j(M_j)$.*

## 1.6 Algèbres

On fixe un anneau commutatif $R$ qui va jouer le rôle d'anneau des scalaires.

**Définition 1.15** Une $R$-algèbre est un anneau (non nécessairement commutatif) $A$ muni d'une structure de $R$-module telle que la multiplication $m : A \times A \to A$ est $R$-bilinéaire.

Cela signifie que pour tout $a, b \in A^2$, les applications

$$\gamma_a : \begin{cases} A & \to & A \\ x & \mapsto & ax \end{cases} \text{ et } \delta_b : \begin{cases} A & \to & A \\ x & \mapsto & xb \end{cases}$$

sont linéaires.

**Proposition 1.9** Soient $R, A$ deux anneaux avec $R$ commutatif. La donnée d'une structure de $R$-algèbre sur $A$ est équivalente à la donnée d'un morphisme d'anneaux $f : R \to A$ telle que $f(R) \subset Z(A)$.

*Démonstration.* Soit $A$ une $R$-algèbre. On définit $f : R \to A$ par $f(r) = r1_A$. On a $f(R) \subset Z(A)$ car

$$f(r)a = (r1_A)a = r(1a) = r(a1) = a(r1) = af(r)$$

Réciproquement, soit $f : R \to A$ un morphisme d'anneaux tel que $f(R) \subset Z(A)$. On munit $A$ d'une structure de $R$-module par $ra = f(r)a$.

On vérifie que ces constructions sont inverses l'une de l'autre. ■

*Remarque 1.13 Si $M$ est une matrice qui n'est pas une homothétie, le morphisme d'inclusion $\mathbb{Z}[M] \subset \mathfrak{M}_n(k)$ ne vérifie pas la propriété sur le centre. De même pour $k[M] \subset \mathfrak{M}_n(k)$.*

**Définition 1.16** On peut définir comme précédemment les morphismes de $R$-algèbres, les sous-$R$-algèbres et la $R$-algèbre engendrée.

*Remarque 1.14 Si $A$ est une $R$-algèbre, tout idéal (de l'anneau) est automatiquement un sous-$R$-module.*

 

# Chapitre 2

# Modules libres de type fini

## 2.1 Modules libres

**<u>Définition 2.1</u>** Soit $A$ un anneau, $I$ un ensemble. Le $A$-module libre (standard) de base $E$ est le module $A^{(I)} = \bigoplus_{i \in I} A$. On note $e_i$ l'élément de $A^{(I)}$ dont la seule composante non nulle est celle d'indice $i$, qui vaut 1.

*Remarque 2.1* *On peut voir $A^{(I)}$ comme l'ensemble des applications $I \to A$ à support fini. $e_i$ correspond alors à l'indicatrice de $i$.*

*Soit $M$ un $A$-module et $(x_i)_i$ une famille d'éléments de $M$. D'après la propriété universelle de la somme directe, il existe un unique morphisme de $A$-modules $\varphi_x : A^{(I)} \to M$ tel que $\varphi_x(e_i) = x_i$ (appliquer la propriété universelle à $g_i : a \mapsto ax_i$). $\varphi_x$ envoie $(a_i)_i$ (à support fini) sur $\sum_{\text{finie}} a_i x_i$. Son image est le sous-module de $M$ engendré par les $x_i$.*

**<u>Définition 2.2</u>** $(x_i)_i$ est une famille génératrice (resp. libre, base) de $M$ ssi $\varphi_x$ est surjectif (resp. injectif, bijectif).

$M$ est libre ssi il possède une base.

**Exemple 2.1** Si $k$ est un corps, $k[X]$ est libre de base $\{1, X, X^2, \ldots\}$ et $k[\![X]\!]$ est aussi libre (par Zorn, avec un « il existe une base ») mais pas pour la famille $\{1, X, X^2, \ldots\}$.

$\mathbb{Z}[X]$ est libre comme $\mathbb{Z}$-module de base $\{X^i, i \in \mathbb{N}\}$, mais $\mathbb{Z}[\![X]\!]$ n'est pas libre sur $\mathbb{Z}$ (pour aucune base).

Pour $A = \mathbb{Z}$, $\mathbb{Z}$ est libre, $\mathbb{Z}/n\mathbb{Z}$ ne l'est pas et $\mathbb{Q}$ non plus. En effet, si $n \in \mathbb{Z}^*$, la multiplication à gauche par $n$ est surjective. Or pour tout $A$ et tout $A$-module $M \neq 0$ libre, si $a$ est non inversible, le morphisme $x \mapsto ax$ n'est pas surjectif car $M$ possède une base $(e_i)_{i \in I \neq \varnothing}$ et $e_i$ n'est pas de la forme

$ax = a\sum_{j=1}^{n} a_{j_n} e_{j_n}$ puisque sinon on aurait, par unicité de la décomposition sur une base : $aa_i = 1$.

## 2.2 Modules libres de type fini

**Définition 2.3** Soit $A$ un anneau, $M$ un $A$-module. On dit que $M$ est un $A$-module de type fini ssi il existe $x_1, \dots, x_n \in M$ qui engendrent $M$.

**Exemple 2.2**

- Si $A = \mathbb{K}$ un corps, type fini est équivalent à dimension finie.
- Si $A = \mathbb{Z}$, $\mathbb{Z}^n$ et $\mathbb{Z}/n\mathbb{Z}$ sont de type fini mais pas $\mathbb{Q}$.
- $A[X]$ n'est pas un $A$-module de type fini, mais attention, c'est une $A$-algèbre de type fini (engendrée par $X$)
- $A^{(I)}$ est de type fini ssi $I$ est fini.

*Remarque 2.2* *$M$ est de type fini ssi il existe $n \geqslant 0$ et un morphisme injectif $\varphi_x : A^n \to M$.*

**Lemme 2.0.1**
Si $A$ est commutatif et $M$ est un $A$-module libre de type fini, il existe un unique entier positif $r \geqslant 0$ tel que $M \simeq A^r$.

*Démonstration.* Si $M$ est libre, $M \simeq A^{(I)}$ par un ensemble $I$. Comme $M$ est de type fini, $I$ est fini.

Notons $r = \text{Card}(I)$, on a alors $M \simeq A^r$. Par le théorème de Krull, il existe un idéal maximal $\mathfrak{m} \subset A$. On note $k = A/\mathfrak{m}$ le quotient.

L'isomorphisme $A^r \simeq A^s$ passe au quotient et donne un isomorphisme de corps $(A/\mathfrak{m})^r \to (A/\mathfrak{m})^s$. Ce sont des espaces vectoriels de dimensions finies $r$ et $s$, on a donc $r = s$. ∎

*Remarque 2.3* *Pour un anneau non commutatif, $A = L(E)$ pour $\dim(E) = \infty$. On montre que $A \simeq A^2$. On en déduit que $A \simeq A^n$ pour tout $n$, en appliquant $X \mapsto X \oplus A$.*

**Définition 2.4** Dans le cas commutatif, le $r$ du lemme est appelé rang de $M$ comme $A$-module.

On va par la suite s'occuper du cas des morphismes entre $A$-modules libres de type fini avec $A$ commutatif. Soient $M, N$ deux tels modules, de rangs respectifs $p$ et $n$. Soit $f$ un morphisme $M \to N$. Prenons des bases $B = (e_1, \dots, e_p)$ et $C = (f_1, \dots, f_n)$.

 

Le morphisme $f$ est entièrement caractérisé par les valeurs $f(e_j)$ qu'on peut écrire sur $C$ : $f(e_j) = \sum_{i=1}^{n} u_{i,j} f_i$. On peut donc écrire la matrice de $f$ entre les bases $B$ et $C$.

L'application

$$\begin{cases} \hom_A(M,N) & \to & \mathfrak{M}_{n,p}(A) \simeq A^{np} \\ f & \mapsto & \mathcal{M}_{B,C}(f) \end{cases}$$

est un isomorphismes de $A$-modules qui dépend de $B$ et $C$.

## 2.3 Calcul matriciel sur $A$ commutatif

On renomme $A$ en $R$.

Soit $A \in \mathfrak{M}_n(R)$ une matrice carrée. On définit

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

**Lemme 2.0.2**
$\det(A^t) = \det(A)$

*Démonstration.*

$$\det(A^t) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i} = \sum_{\tau \in \mathfrak{S}_n} \varepsilon(\tau) \prod_{j=1}^{n} a_{j,\tau(j)}$$

avec $\tau = \sigma^{-1}$ et $i = \tau(j)$. ■

**<u>Définition 2.5</u>** Soit $f : M^n \to N$ une application multilinéaire. On dit que $f$ est alternée ssi pour tout $i, j$, $(x_i = x_j \Rightarrow f(x_1, \dots, x_n) = 0)$.

**Lemme 2.0.3**
det définit deux formes linéaires alternées $(A^n)^n \to A$ en les lignes et les colonnes de $A$.

*Démonstration.* On regarde le cas des colonnes.

$$\begin{aligned} &\det(A^1, \dots, A^{i-1}, \alpha B + \beta C, A^{i+1}, \dots, A^n) \\ &= \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a^1_{\sigma(1)} \dots (\alpha b_{\sigma(i)} + \beta c_{\sigma(i)}) \dots a^n_{\sigma(n)} \\ &= \alpha \det(A^1, \dots, A^{i-1}, B, \dots, A^n) + \beta \det(A^1, \dots, A^{i-1}, C, \dots, A^n) \end{aligned}$$

 

Ce calcul montre que det est $R$-linéaire en la $i^{\mathrm{e}}$ colonne. Soit $\tau = (u\,v)$ une transposition, avec $u \neq v$. On va montrer que $\det(A) = 0$ si la $u^{\mathrm{e}}$ et la $v^{\mathrm{e}}$ ligne sont égales. On écrit $\mathfrak{S}_n = \mathfrak{A}_n \sqcup \mathfrak{A}_n\tau$. On sépare la somme en deux sommes indicées par $\mathfrak{A}_n$ et on remarque que :

$$a_{1,\sigma\tau(1)} \dots a_{n,\sigma\tau(n)} = a_{u,\sigma\tau(u)} a_{v,\sigma\tau(v)} \dots = a_{1,\sigma(1)} \dots a_{n,\sigma(n)}$$

On a donc

$$\begin{aligned}\det(A) &= \sum_{\sigma\in\mathfrak{A}_n} a_{1,\sigma(1)} \dots a_{n,\sigma(n)} + \sum_{\sigma\in\mathfrak{A}_n} - a_{1,\sigma(1)} \dots a_{n,\sigma\tau(n)} \\ &= \sum_{\sigma\in\mathfrak{A}_n} a_{1,\sigma(1)} \dots a_{n,\sigma(n)} - \sum_{\sigma\in\mathfrak{A}_n} a_{1,\sigma(1)} \dots a_{n,\sigma(n)} \\ &= 0\end{aligned}$$

■

<u>Théorème 2.1</u> $\det(AB) = \det(BA)$.

*Démonstration.* Soit $F_n$ l'ensemble des fonctions de $[\![1,n]\!]$ dans lui même. Si $B \in \mathfrak{M}_n(R)$, $\tau \in F_n$. Notons $B_\tau = (b_{\tau(i),j})_{i,j}$.

Si $\tau$ n'est pas injective, $B_\tau$ deux lignes égales donc $\det(B_\tau) = 0$. On a alors

$$\begin{aligned}\det(AB) &= \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} \sum_{k=1}^{n} a_{i,k} b_{k,\sigma(i)} = \sum_{\sigma\in\mathfrak{S}_n} \sum_{\tau\in F_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\tau(i)} b_{\tau(i),\sigma(i)} \\ &= \sum_{\tau\in F_n} \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\tau(i)} b_{\tau(i),\sigma(i)} = \sum_{\tau\in F_n} \prod_{i=1}^{n} a_{i,\tau(i)} \underbrace{\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} \beta_{\tau(i),\sigma(i)}}_{=\det(B_\tau)=0 \text{ si } \tau\notin\mathfrak{S}_n} \\ &= \sum_{\tau\in\mathfrak{S}_n} \prod_{i=1}^{n} a_{i,\tau(i)} \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} \beta_{\tau(i),\sigma(i)} \\ &= \sum_{\tau\in F_n} \prod_{i=1}^{n} a_{i,\tau(i)} \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma\tau) \prod_{i=1}^{n} \beta_{i,\sigma(i)} \qquad (\sigma \leftarrow \sigma\tau^{-1}, i \leftarrow \tau^{-1}(i)) \\ &= \det(A)\det(B)\end{aligned}$$

■

**<u>Définition 2.6</u>** Soit $A \in \mathfrak{M}_n(R)$. Soient $i,j \in [\![1,n]\!]^2$. On note $M_{i,j}$ la matrice de taille $(n-1,n-1)$ obtenue en enlevant la $i^{\mathrm{e}}$ ligne et la $j^{\mathrm{e}}$ colonne de $A$. On appelle

- mineur d'indice $(i,j)$ le déterminant $m_{i,j} = \det(M_{i,j})$
- cofacteur d'indice $(i,j)$ la quantité $\mu_{i,j} = (-1)^{i+j} m_{i,j}$
- comatrice la matrice des cofacteurs $\widetilde{A} = (\mu_{i,j})_{i,j}$

 

**Proposition 2.1**

- Développement par rapport à la $i^{\text{e}}$ ligne :

$$\det(A) = \sum_{j=1}^{n} a_{i,j}\mu_{i,j}$$

- Développement par rapport à la $j^{\text{e}}$ colonne :

$$\det(A) = \sum_{i=1}^{n} a_{i,j}\mu_{i,j}$$

<u>Théorème 2.2</u> *Pour tout* $A \in \mathfrak{M}_n(\mathbb{R})$, $A\widetilde{A}^t = \widetilde{A}^t A = \det(A) I_n$.

*Démonstration.* Découle des formules précédentes. ∎

Corollaire 2.1 *$A$ est inversible ssi* $\det(A) \in R^\times$.

*Démonstration.*

⇒ $AB = I_n$ implique $\det(A)\det(B) = \det(AB) = \det(I_n) = 1$.

⇐ Si $\det(A) \in R^\times$, la formule précédente montre que $(\det(A))^{-1}\widetilde{A}^t$ convient. ∎

<u>Théorème 2.3</u> Cayley-Hamilton *Soit* $\chi(T) = \det(TI_n - A)$ *le polynôme caractéristique de $A$. Alors* $\chi(A) = 0$.

*Démonstration.* Soit $S = R[A]$ la sous-$R$-algèbre engendrée par $A$. C'est l'algèbre des polynômes en $A$ à coefficients dans $R$. Cette algèbre est commutative car $A$ commute avec tout polynôme en $A$.

On veut diviser $\chi(T) \in R[T]$ par $T - A \in S[T]$. On va donc considérer $\chi(T)I_n$ au lieu de $\chi(T)$. Le théorème de division euclidienne dans $S[T]$ assure que

$$\chi(T) = (T - A)Q(T) + R(T)$$

avec $\deg(R) < 1$. On a de plus $\chi(T) = (T - A)\widetilde{T - A}^t$. Cette écriture est une division euclidienne de $\chi(T)$ à gauche par $T - 1$ dans $\mathfrak{M}_n(R)[T]$, de même que la formule précédente. On a donc $\widetilde{T - A}^t = Q(T) \in S[T]$ et $R(T) = 0$.

En particulier, la formule $\chi(T) = (T - A)\widetilde{T - A}^t$ vit dans $S[T]$ qui est commutatif. On dispose alors du morphisme d'anneaux d'évaluation en $A$ : $P(T) \to P(A)$. On applique ce morphisme à cette formule et $\chi(A) = (A - A)\widetilde{A - A}^t = 0$. ∎

**Proposition 2.2** Soit $A \in \mathfrak{M}_n(R)$ et $f : R^n \to R^n$ l'endomorphisme $R$-linéaire associé. Posons $\det(f) = \det(A)$. Alors

 

1. $f$ est surjectif ssi $\det(f) \in R^\times$ ssi $f$ bijectif.
2. $f$ est injectif ssi $\det(f) \nmid 0$.

*Remarque 2.4* *Il existe des $f$ injectifs non surjectifs. En rang $1$, il suffit de prendre $A = (a) \in \mathfrak{M}_1(R)$, $f : x \mapsto ax$.*

*On a $f$ surjective ssi il existe $x$ tel que $ax = 1$ ssi $a = \det(f) \in R^\times$ et $f$ injectif ssi $a \nmid 0$ par définition.*

 

# Chapitre 3

# Anneaux factoriels et principaux

À partir de maintenant, tous les anneaux sont commutatifs.

## 3.1 Anneaux nœthériens

POLY !

## 3.2 Divisibilité, anneaux factoriels

**Définition 3.1** On dit que $a \in A$ divise $b \in A$ ssi il existe $c \in A$ tel que $b = ac$.

On dit que $a$ et $b$ sont associés ssi $a \mid b$ et $b \mid a$. On note $a \sim b$.

*Remarque 3.1 La relation $\mid$ est réflexive et transitive mais pas antisymétrique. $\sim$ est une relation d'équivalence. Dans $A/\sim$, $\mid$ induit donc une relation d'ordre compatible à la multiplication.*

*Si $A$ est intègre et $a \sim b$, alors $a = b = 0$ ou $b = ac$ avec $c \in A^*$.*

*$a \mid b$ peut aussi s'exprimer par $\langle b \rangle \subset \langle a \rangle$. Si $a \sim b$, les deux idéaux sont égaux. Ainsi, $A/\sim$ s'identifie à l'ensemble des idéaux de $A$ monogènes muni de l'ordre $\supset$.*

**Définition 3.2** Soit $(a_i)_i$ une famille d'éléments de $A$.

- On dit que les $a_i$ ont un pgcd ssi l'ensemble de leurs diviseurs communs dans $A/\sim$ possède un plus grand élément. On le note $\bigwedge_i a_i \in A/\sim$.
- On dit que les $a_i$ ont un ppcm ssi l'ensemble de leurs diviseurs communs dans $A/\sim$ possède un plus petit élément. On le note $\bigvee_i a_i \in A/\sim$.

- On dit que les $a_i$ sont premiers entre eux dans leur ensemble ssi ils possèdent un pgcd égal à 1.

Par abus, on dit que $d \in A$ est un pgcd des $a_i$ si $\overline{d}$ est le pgcd des $(a_i)_i$.

**Définition 3.3** Soit $(a, b, p) \in A$.

- On dit que $p$ est irréductible ssi pour tout $a, b \in A$, $p = ab \Rightarrow a$ ou $b$ est inversible.
- $p$ est premier ssi $\langle p \rangle$ l'est.

*Remarque 3.2 Si $p$ est premier alors $p$ est irréductible, mais la réciproque n'est pas toujours vraie.*

**Exemple 3.1** Soit $(a, p) \in A$ avec $p$ irréductible. Alors $a \wedge p$ existe et vaut $p$ si $p \mid a$ et 1 sinon.

**Définition 3.4** Soit $A$ un anneau commutatif. On dit que $A$ est factoriel ssi

(I) $A$ est intègre

(E) Pour tout $A \setminus \{0\}$, il existe $u \in A^*$, $p_1, \ldots, p_r$ irréductibles distincts, $\alpha_1, \ldots, \alpha_r$ entiers supérieurs à 1 tel que $a = up_1^{\alpha_1} \ldots p_r^{\alpha_r}$.

(U) Toute écriture du point précédent est unique à permutation et association des facteurs près.

*Remarque 3.3 Si on choisit un ensemble $\Sigma$ de représentants des irréductibles (un dans chaque classe) alors dans un anneau factoriel, tout élément $a \in A$ s'écrit de manière unique $a = u \prod_{p \in \Sigma} p^{\alpha_p}$ avec $\alpha_p = 0$ pour presque tout $p$.*

**Lemme 3.0.1**

Dans un anneau factoriel, toute famille d'éléments non nuls possède un pgcd et un ppcm. En effet, si on écrit $a_i = u_i \prod_{p \in \Sigma} p^{\alpha_p(i)}$ alors

$$\bigwedge_{i=1} r a_i = \prod_{p \in \Sigma} p^{\min(\alpha_p(1), \ldots, \alpha_p(r))}$$

$$\bigvee_{i=1} r a_i = \prod_{p \in \Sigma} p^{\max(\alpha_p(1), \ldots, \alpha_p(r))}$$

*Démonstration.* Soit $b = v \prod_{p \in \Sigma} p^{\beta_p}$ un élément non nul de $A$.

On a $b \mid a$ ssi pour tout $p \in \Sigma$, $\beta_p \leqslant \alpha_p$. Ainsi, $b \mid a_i$ pour tout $i$ ssi $\beta_p \leqslant \min(\alpha_p(1), \ldots, \alpha_p(r))$.

Cecie montre que $\prod_{p \in \Sigma} p^{\min(\alpha_p(1), \ldots, \alpha_p(r))}$ est un diviseur commun de $a_i$ et c'est clairement le plus grand d'entre eux. ∎

 

En particulier, si $r = 2$, comme $\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$, on a $ab \sim (a \wedge b)(a \vee b)$.

*Remarque 3.4 Si $A$ est nœthérien, la propriété d'existence de la décomposition est toujours vérifiée.*

**Lemme 3.0.2**
Soit $A$ intègre et $a, b, x$ des éléments non nuls tels que $ax \wedge bx$ existe. Alors $a \wedge b$ existe et $ax \wedge bx = x(a \wedge b)$.

*Démonstration.* Soit $d_1 = ax \wedge bx$. Comme $x$ divise $ax$ et $bx$, il divise $d_1$ ie il existe $d \neq 0$ tel que $d_1 = dx$. Montrons que $d$ est un pgcd pour $a$ et $b$.

On a $dx = d_1 \mid ax$ donc $d \mid a$ (intégrité) donc $d$ est un diviseur commun à $a$ et $b$.

Soit $e \in A \setminus \{0\}$ un diviseur commun de $a$ et $b$. Alors $ex \mid ax$ et $ex \mid bx$ donc $ex \mid d_1 = dx$ donc $e \mid d$. ■

*Remarque 3.5 Il existe des exemples où $a$ et $b$ ont un pgcd sans que $ax$ et $bx$ en aient un.*

**Proposition 3.1** Soit $A$ un anneau vérifiant (I) et (E). Les conditions suivantes sont équivalentes :

1. $A$ est factoriel.
2. Si $p$ est irréductible, $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.
3. Si $p$ est irréductible, $p$ est premier.
4. Si $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$.
5. Deux éléments non nuls de $A$ ont un pgcd.

*Démonstration.* Comme $3 \Leftrightarrow 2$, on montre $1 \Rightarrow 5 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1$.

$1 \Rightarrow 5$ Voir lemme précédent.

$5 \Rightarrow 4$ Il existe $u \in A$ tel que $bc = au$. On a $c = c(a \wedge b) = ca \wedge cb = ac \wedge au = a(c \wedge u)$. Donc $a \mid c$.

$4 \Rightarrow 2$ On prend $a = p$, $b = a$ et $c = b$ dans (4). On trouve que $p \mid ab$ et $p \wedge a = 1$ implique $p \mid b$ qui est cqfd puisque $p \wedge a = 1$ ssi $p \nmid a$.

$2 \Rightarrow 1$ Soit $a \in A \setminus \{0\}$, $a = u \prod\limits_{p \in \Sigma} p^{\alpha_p} = v \prod\limits_{p \in \Sigma} p^{\beta_p}$.

On veut montrer que $\alpha = \beta$. Soit $q$ un irréductible tel que $\alpha_q \geqslant 1$. $q \mid a$ donc $q \mid \prod\limits_{p \in \Sigma} p^{\beta_p}$.

Par le lemme d'Euclide, on trouve que $q \mid p$ pour $p \in \Sigma$ tel que $\beta_p \geqslant 1$. Alors $q \sim p$ donc $q = p$.

On a donc $\frac{a}{q} = uq^{\alpha_q - 1} \prod\limits_{p \neq q} p^{\alpha_p} = vq^{\beta_q - 1} \prod\limits_{p \neq q} p^{\beta_p}$.

 

On conclut par récurrence sur la longueur des décompositions en irréductibles de $a$. On introduit $\nu(a)$ le minimum des $\sum_{p\in\Sigma}\alpha_p$ sur l'ensemble des décompositions de $a$ d'exposants $\alpha_p$.
Si $\nu(a) = 0$, $a$ est inversible et $a = a$ est la seule décomposition. Le raisonnement précédent assure le passage de $\nu$ à $\nu + 1$. ∎

**Définition 3.5** Soit $A$ un anneau factoriel et $P \in A[X]$ un polynôme. On appelle contenu de $P$, noté $c(P)$ le pgcd de ses coefficients.

On dit que $P$ est primitif ssi $c(P) = 1$.

*Remarque 3.6 Pour tout $P$, $P = c(P)P'$ avec $P'$ primitif.*

**Lemme 3.0.3**
$c(PQ) = c(P)c(Q)$ donc si $P$ et $Q$ sont primitifs, $PQ$ est primitif.

*Démonstration.* Soient $P = c(P)P'$ et $Q = c(Q)Q'$ avec $P', Q'$ primitifs. Comme $c(\lambda P) = \lambda c(P)$, on se ramène à montrer $c(P'Q') = 1$.

Or $c(P) = 1$ ssi pour tout $p$ irréductible, il existe un coefficient de $P$ non divisible par $p$ ssi la classe $\overline{P}$ de $P$ dans $(A/p)[X]$ est non nulle.

Ainsi, $P$ et $Q$ sont primitifs ssi pour tout $p$ irréductible, $\overline{P} \neq 0 \neq \overline{Q}$ ssi pour tout $p$, $\overline{P} \cdot \overline{Q} \neq 0$ (intégrité) ssi $PQ$ est primitif. ∎

Théorème 3.1 Gauss *Si $A$ est factoriel, alors $A[X]$ est factoriel.*

*Plus précisément, les irréductibles de $A[X]$ sont les irréductibles de $A$ (vus comme polynômes constants) et les $P \in A[X]$ primitifs et irréductibles dans* $\mathrm{Frac}(A)[X]$.

**Exemple 3.2** Si $A$ est un corps, $A[X]$ est factoriel.

## 3.3 Anneaux principaux et euclidiens

**Définition 3.6** Un idéal $I$ de $A$ commutatif est dit principal ssi il est engendré par un seul élément. Un anneau est dit principal ssi il est intègre et tous ses idéaux sont principaux.

**Exemple 3.3** Les corps et $\mathbb{Z}$ sont principaux, mais pas $\mathbb{Z}/n\mathbb{Z}$ si $n \neq 0$ et $n$ non premier.

**Proposition 3.2** Soit $A$ un anneau principal et $a, b \in A$ non nuls. Alors tout générateur de l'idéal engendré par $a$ et $b$ est un pgcd pour $a$ et $b$. Tout générateur de $(a) \cap (b)$ est un ppcm pour $a$ et $b$. Enfin, $A$ est factoriel.

*Démonstration.* Soit $d$ un générateur de $(a, b)$. Pour tout $e \in A$, on a

$$e \mid a \text{ et } e \mid b \quad \text{ssi} \quad (a) \subset (e) \supset (b) \quad \text{ssi} \quad (d) = (a, b) \subset (e) \quad \text{ssi} \quad e \mid d$$

 

Ceci montre que $d$ est un pgcd de $a$ et $b$.

Soit $m$ un générateur de $(a) \cap (b)$. Pour tout $n \in A$, on a

$$a \mid n \text{ et } b \mid n \quad \text{ssi} \quad (a) \supset (n) \subset (b) \quad \text{ssi} \quad (n) \subset (m) = (a) \cap (b) \quad \text{ssi} \quad m \mid n$$

Ceci montre que $m$ est un ppcm de $a$ et $b$.

(I) est claire par définition, (E) est vraie car tout idéal est engendré par un élément, donc de type fini donc $A$ est nœthérien, donc vérifie (E). De plus, (U) est vraie puisque tout $(a, b) \in A$ non nuls ont un pgcd. ■

Corollaire 3.1 Bézout *Soit $A$ principal et $(a, b) \in A^2$ non nuls. Alors $a$ et $b$ sont premiers entre eux ssi il existe $u, v \in A$ tel que $ua + vb = 1$.*

*Plus généralement, $a \wedge b = d$ ssi il existe $u, v$ premiers entre eux tel que $ua + vb = d$.*

*Remarque 3.7*
- *Si $d = ua + vb$ alors $(xu)a + (xv)b = xd$ n'implique pas que $a \wedge b = xd$ car $xu$ et $xv$ ne sont pas premiers entre eux.*
- *Un couple de Bézout n'est jamais unique.*

*Démonstration du cas $d = 1$.* Par la proposition, $a$ et $b$ sont premiers entre eux ssi $(a, b) = A$ ssi $1 \in (a, b)$ ssi il existe $u, v$ tel que $ua + vb = 1$. ■

**Définition 3.7** Soit $A$ un anneau commutatif. Un stathme euclidien pour $A$ est une application $\delta : A \to \mathbb{N}$ tel que
- Si $a \mid b$ et $b \neq 0$, $\delta(a) \leqslant \delta(b)$
- Pour tout $a, b \in A^2$, avec $b \neq 0$, il existe un unique couple $(q, r) \in A^2$ tel que $a = bq + r$ et $\delta(r) < \delta(b)$.

On dit que $A$ est euclidien ssi il est intègre et muni d'un stathme.

*Remarque 3.8*
- *Il existe des variantes sur la définition d'un stathme mais elles sont toutes à peu près équivalentes.*
- *Si $\delta$ est un stathme, pour tout $k \in \mathbb{Z}$, $\delta + k$ aussi.*

**Proposition 3.3** Tout anneau euclidien est principal.

*Démonstration.* $A$ est intègre par définition. Soit $I \subset A$ un idéal. Si $I = \{0\}$, $I$ est principal, sinon il existe $b \in I$ non nul de stathme minimal parmi les $\delta(b_i)$, $b_i \in I \setminus \{0\}$.

$(b) \subset I$ et réciproquement, si $a \in I$, on fait la DE de $a$ par $b$ : $a = bq + r$ avec $\delta(r) < \delta(b)$.

On a alors $r \in I$ et $\delta(r) < \delta(b)$ donc par minimalité de $b$, $r = 0$. Donc $a = bq \in (b)$. ■

 

**Exemple 3.4**

- $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q}, p \nmid b\}$ est euclidien pour $\delta$ la valuation $p$-adique (l'exposant de $p$ dans la décomposition en facteurs premiers de $a$.
- $k[\![X]\!]$ est euclidien pour $\delta\left(\sum_{i=1}^{d} a_i X^i\right) = \min\{n \geqslant 0, a_n \neq 0\}$.
- $\mathbb{Z}[i]$ est euclidien pour $|\cdot|^2$.
- $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal non euclidien

<u>Théorème 3.2</u> des restes chinois *Soient $A$ un anneau commutatif et $I, J$ deux idéaux tels que $I + J = A$ (on dit que $I$ et $J$ sont étrangers).*

*Le morphisme d'anneaux canonique $A/IJ \to A/I \times A/J$ est un isomorphisme.*

*Démonstration.* L'hypothèse signifie que $1 \in I + J$ ie il existe $i \in I$, $j \in J$ tel que $1 = i + j$. Montrons l'injectivité.

Soit $a + IJ \in A/IJ$ tel que $f(a + IJ) = 0$ ie $a + I = I$ et $a + J = J$. Alors $a \in a + I = I$ et $a \in a + J = J$ donc $a \in I \cap J$.

On en déduit que $a = ai + aj \in IJ$ donc $a + IJ = IJ$.

La surjectivité : soit $(x + I, y + J) \in A/I \times A/J$. On pose $a = xj + yi$ et on vérifie que $a + IJ$ est un antécédent pour $(x + I, y + J)$. On a $a = x(1 - i) + yi = x + i(y - x)$ donc $a + I = x + I$ et de même, $a = y + (x - y)j$ donc $a + J = y + J$. ∎

*Remarque 3.9 On pourrait le démontrer en montrant directement que l'application $(\overline{x}, \widetilde{y}) \mapsto \widehat{xj + yi}$ est bien définie et réciproque de l'énoncé.*

**Exemple 3.5** $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$ via $(a, b) \mapsto 4a - 3b$.

**Proposition 3.4** Soit $A$ un anneau principal et $p \in A$ non nul. Alors les conditions suivantes sont équivalentes :

(i) $p$ est irréductible

(ii) $(p)$ est premier

(iii) $(p)$ est maximal

*Démonstration.*

(i) $\Leftrightarrow$ (ii) car $A$ est factoriel.

(iii) $\Rightarrow$ (ii) car maximal implique premier.

(iii) $\Leftarrow$ (ii) à lire dans le poly. ∎

 

# Chapitre 4

# Modules sur les anneaux principaux

Les modules sur un corps, c'est facile (espace-vectoriel), sur un anneau principal, on a un théorème de structure assez précis, mais sinon, c'est compliqué !

## 4.1 Opérations élémentaires sur les matrices et forme de Smith

Soit $A$ un anneau principal, $\mathfrak{M}_{n,p}(A)$ le $A$ module des matrices de format $n \times p$. C'est un $A$-module libre de rang $np$.

On pose $E_{i,j}$ la matrice élémentaire $(\delta_{u,i}\delta_{v,j})_{u,v}$. On a $E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l}$.

On se limite dans la suite aux matrices carrés de taille $n = p$. On pose $E_{i,j}(a) = \mathrm{Id} + aE_{i,j}$ si $i \neq j$. On a $\det(E_{i,j}(a)) = 1$ donc $E_{i,j}(a) \in SL_n(A)$.

**Lemme 4.0.1**
Soit $M \in \mathfrak{M}_n(A)$, $L_i$ sa $i^{\text{e}}$ ligne et $C_j$ sa $j^{\text{e}}$ colonne.

Multiplier $M$ à droite par $E_{i,j}(a)$ revient à ajouter $aC_i$ à $C_j$ : $C_j \leftarrow aC_i + C_j$.

Multiplier $M$ à gauche par $E_{i,j}(a)$ revient à faire $L_i \leftarrow L_i + aL_j$.

**Définition 4.1** Soient $M, N \in \mathfrak{M}_{n,p}(A)$.

On dit que $M$ et $N$ sont ($G$-)équivalentes ssi il existe $P \in GL_n(A)$ et $Q \in GL_n(A)$ tel que $M = PNQ$.

On dit que $M$ et $N$ sont $S$-équivalentes ssi il existe $P \in SL_n(A)$, $Q \in SL_p(A)$ tel que $M = PNQ$.

Théorème 4.1 *Soit $A$ principal. Toute matrice $M \in \mathfrak{M}_{n,p}(A)$ est $S$-équivalente à une matrice dite sous forme normale de Smith ie de la forme*

$\mathrm{diag}(d_1, \dots, d_r, 0, \dots, 0)$ *avec* $d_i \neq 0$ *et* $d_1 \mid d_2 \mid \dots \mid d_r$.

*De plus cette forme normale des Smith est unique au sens suivant : si* $M$ *est* $S$*-équivalente (en fait* $G$*-équivalente suffit) à* $\mathrm{diag}(d_1, \dots, d_r, 0, \dots, 0)$ *et à* $\mathrm{diag}(d'_1, \dots, d'_s, 0, \dots, 0)$*, on a* $r = s$ *et* $(d_i) = (d'_i)$ *pour tout* $i$*. Les* $d_i$ *sont appelés facteurs invariants de* $M$*.*

*La suite d'idéaux* $(d_1) \supset \dots \supset (d_n)$ *est unique est appelée suite des facteurs invariants de* $M$*.*

*Démonstration dans le cas euclidien.* Soit $\delta$ un stathme sur $A$. On pose

$$\tau(M) = \max(n, p) \text{ et } \delta(M) = \min_{m_{i,j} \neq 0} \delta(m_{i,j})$$

On va utiliser deux procédures de base :

- celle qui échange deux colonnes en opposant l'une : $(a\,b) \to (b\ -a)$ qui correspond à $C_1 \leftarrow C_1 + C_2$, $C_2 \leftarrow C_2 - C_1$ et $C_1 \leftarrow C_1 + C_2$.
- si $a \neq 0$, on fait la DE de $b$ par $a$ : $b = aq + r$, $\delta(r) < \delta(a)$. On a $(a\,b) \sim (a\,r)$ via $C_2 \leftarrow C_1 - qC_2$

On procède par récurrence sur $\tau(M) + \delta(M) \geqslant 1$. On peut supposer $M \neq 0$.

Si $\tau(M) = 1$, c'est fini. Si $\tau(M) + \delta(M) \geqslant 2$. Par itération de la première procédure sur les colonnes et sur les lignes, on peut mettre en position $(1, 1)$ un coefficient $m_{i,j}$ de $M$ tel que $\delta(M) = \delta(m_{i,j})$. On suppose donc désormais que $\delta(M) = \delta(m_{1,1})$.

S'il existe $j \geqslant 2$ tel que $m_{1,1} \nmid m_{1,j}$, on applique la deuxième procédure, on a $M \sim M'$ avec $\delta(M') < \delta(M)$. Par hypothèse de récurrence, $M' \sim \mathrm{diag}(d_1, \dots, d_r, 0, \dots, 0)$ et on a fini.

S'il existe $i \geqslant 2$ tel que $m_{1,1} \mid m_{i,1}$, on fait pareil sur les lignes et ça marche.

Sinon, par la deuxième procédure, on a $M \sim \begin{pmatrix} m_{1,1} & 0 \\ 0 & M_1 \end{pmatrix}$ et $\tau(M_1) < \tau(M)$. Par hypothèse de récurrence, il existe $P_1 \in SL_{n-1}(A)$, $Q_1 \in SL_{p-1}(A)$ tel que $M_1 = P_1 D_1 Q_1$ avec $D_1 = \mathrm{diag}(d_2, \dots, d_r, 0, \dots, 0)$ et $d_2 \mid d_3 \mid \dots \mid d_r$.

Posons $P = \begin{pmatrix} 1 & 0 \\ 0 & P_1 \end{pmatrix}$ et $Q = \begin{pmatrix} 1 & 0 \\ 0 & Q_1 \end{pmatrix}$. Ona alors $M = PDQ$ avec $D = \mathrm{diag}(m_{1,1}, d_2, \dots, d_r, 0, \dots, 0)$. Si $m_{1,1} \mid d_2$, on l'appelle $d_1$ et c'est fini. Sinon, $\begin{pmatrix} m_{1,1} & 0 \\ 0 & d_2 \end{pmatrix} \sim \begin{pmatrix} m_{1,1} & d_2 \\ 0 & d_2 \end{pmatrix} \sim \begin{pmatrix} m_{1,1} & r \\ 0 & d_2 \end{pmatrix}$ avec $\delta(r) < \delta(m_{1,1})$. L'hypothèse de récurrence appliquée à la matrice $\begin{pmatrix} m_{1,1} & 0 \\ 0 & D_1 \end{pmatrix} + rE_{1,2}$ conclut.

L'unicité est admise. ■

 

**Exemple 4.1** $M = \begin{pmatrix} 7 & 11 & 3 \\ 3 & 4 & 2 \end{pmatrix}$ sur $A = \mathbb{Z}$. On a

$$\begin{aligned} M &\sim \begin{pmatrix} 3 & 11 & -7 \\ 2 & 4 & -3 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & -3 \\ -3 & -11 & 7 \end{pmatrix} \\ &\sim \begin{pmatrix} 2 & 0 & 1 \\ -3 & -5 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -2 \\ 1 & -5 & 3 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 0 & 0 \\ 1 & -5 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -5 & 5 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix} \end{aligned}$$

*Remarque 4.1 Il vaudrait mieux commencer par $C_1 \leftarrow C_1 - 2C_3$ pour faire apparaître un 1 dès que possible en haut à gauche. Ce 1 est le pgcd des coefficients de $M$. Plus généralement, $d_1$ est le pgcd des $m_{i,j}$ non nuls et $\prod_{i=1}^{r} d_i$ est le pgcd des mineurs de taille $r$ de $M$. Sur l'exemple, les mineurs sont 10, 5 et $-5$ donc $d_1 d_2 = 5$. Une fois que ceci est démonté, l'unicité en découle.*

## 4.2 Structure des modules de type fini sur un anneau principal

**Lemme 4.1.1**
Si $A$ est principal et $n \geqslant 1$ entier. Alors tout sous-module $M$ de $A^n$ est engendré par moins de $n$ éléments.

*Démonstration.* Par récurrence sur $n$. Si $n = 1$, c'est la définition d'un anneau principal. Sinon, notons $A^{n-1} \subset A^n$ le sous-module engendré par $(e_1, \dots, e_{n-1})$ les $n-1$ premiers vecteurs de la base canonique de $A^n$. Soit $N = M \cap A^{n-1}$, c'est encore un sous-module de $A^{n-1}$. Par l'hypothèse de récurrence, $N$ est engendré par moins de $n-1$ éléments $x_1, \dots,_r$ avec $r \leqslant n-1$. On regarde le morphisme :

$$\begin{tikzcd} M \arrow[r] \arrow[d, "\rho"] & A^n \arrow[r, "\pi"] & A^n/A^{n-1} \arrow[d, "\sim"] \\ M/N \arrow[rr, hook] & & A \end{tikzcd}$$

Donc $M/N$ est isomorphe à un sous-module de $A$ et par le cas $n = 1$, il peut être engendré par un élément $\overline{x_{r+1}} \in M/N$.

 

Soit $x_{r+1} \in M$ un antécédent de $\overline{x_{r+1}}$. On montre que $x_1, \dots, x_{r+1}$ engendre $M$. Si $m \in M$, alors son image dans $M/N$ est de la forme $a\overline{x_{r+1}}$ donc $m - ax_{r+1} \in \operatorname{Ker} \rho$.

Comme $\operatorname{Ker} \rho = N$ engendré par $x_1, \dots, x_r$, il existe $a_1, \dots, a_r$ tel que $m = \sum_{i=1}^{r} a_i x_i + ax_{r+1}$.

$M$ est donc engendré par $r + 1 \leqslant n$ éléments. ■

<u>Théorème 4.2</u> de la base adaptée *Soit $A$ un anneau principal, $L$ un $A$-module libre de type fini, de rang $l$, $K$ un sous-module de $L$. Alors il existe $k \leqslant l$, $d_1 \mid d_2 \mid \dots \mid d_k$ non nuls dans $A$. et une base $f_1, \dots, f_l$ de $L$ tels que $d_1 f_1, \dots, d_k f_k$ soit une base de $K$.*

*En particulier, $K$ est libre de rang $k \leqslant l$ et les idéaux $(d_k) \supset \dots \supset (d_1)$ ne dépendent que de $L$ et $K$ (et non des bases), ce sont les facteurs invariants de $K$ dans $L$.*

*Démonstration.* Par le lemme, $K$ est engendré par un nombre $k \leqslant l$ d'éléments. Supposons $k$ choisi minimal, ie $K$ ne peut pas être engendré par $k-1$ éléments. On a une surjection $A^k \to K$ qui envoie $e'_i$ sur $x_i$ avvec $(x_1, \dots, x_k)$ est un système générateur minimal fixé.

La composée $u : A^k \to K \hookrightarrow L \simeq A^l$ est un morphisme de $A$-modules entre deux modules libres de rang fini. Si on choisit une base $f'_1, \dots, f'_l$ de $L$, la matrice de cette composée dans $(e'_i)$ et $(f'_j)$ est une matrice $M \in \mathfrak{M}_{l,k}(A)$.

D'après la section précédente, il existe $P \in SL_l(A)$ et $Q \in SL_k(A)$ tel que $M = P \operatorname{diag}(d_1, \dots, d_r, 0, \dots, 0) Q$.

Il existe donc des bases $(e_1, \dots, e_k)$ de $K$ et $f_1, \dots, f_l$ de $L$ qui sont images de précédents par $P$ et $Q$ et telles que $u(e_j) = d_j f_j$ si $j \leqslant r$ et $u(e_j) = 0$ sinon.

Comme $k$ est choisi minimal, on a en fait $r = k$. Comme les $d_i$ sont non nuls, donc non diviseurs de 0 (anneau intègre) donc $u$ est injectif. Ceci montre que $K$ est libre et que $(d_i f_i)$ est une base de $K$.

L'unicité découle de celle de la forme normale de Smith. ■

**Exemple 4.2** Le sous-module de $\mathbb{Z}^2$ engendré par les vecteurs $x_1 = (1,0)$ et $x_2 = (1,2)$ a pour base adaptée $\{e_1 = x_1, 2e_2 = x_2 - x_1\}$.

<u>Théorème 4.3</u> de structure des modules de type fini sur un anneau principal *Soient $A$ un anneua principal, $M$ un $A$-module de type fini. Alors il existe un entier $n \geqslant 0$ et des éléments $d_1, \dots, d_n \in A$ non inversibles tels que $M \simeq A/(d_1) \times \dots \times A/(d_n)$ et $d_1 \mid \dots \mid d_n$.*

*La suite d'idéaux $(d_1) \supset \dots \supset (d_n)$ est unique et on l'appelle suite des facteurs invariants de $M$.*

 

*Remarque 4.2* *Si on note $q$ le nombre de $d_i$ nuls, ce sont les $q$ derniers. Posons $r = n - q$, on a alors $M \simeq A/(d_1) \times \ldots \times A/(d_r) \times A^q$ où $d_1 \mid \ldots \mid d_r$ inversibles et non nuls.*

*La partie $A/(d_1) \times \ldots \times A/(d_r)$ est appelée partie de torsion de $M$.*

*Démonstration.* Soit $(x_1, \ldots, x_n)$ une famille de générateurs avec $n$ minimal. Soit $\varphi : A^n \to M$ le morphisme surjectif associé à $(x_1, \ldots, x_n)$ et $K = \operatorname{Ker} \varphi$.

Par le théorème de la base adaptée, $K$ est libre de rang $r$ et il existe une base $(f_1, \ldots, f_n)$ de $A^n$ et $d_1 \mid \ldots \mid d_r$ non nuls de $A$ telle que $\{d_1 f_1, \ldots, d_r f_r\}$ soit une base de $K$. Posons $d_{r+1} = \ldots = d_n = 0$.

On a $K \subset A^n = Ae_1 \oplus \ldots \oplus Ae_n = Af_1 \oplus \ldots \oplus Af_r \oplus Af_{r+1} \oplus \ldots \oplus Af_n = Ad_1 f_1 \oplus \ldots \oplus Ad_r f_r \oplus 0$.

Le morphisme $\varphi$ identifie donc $M$ à $A^n/K \simeq A/d_1 A \oplus \ldots \oplus A/d_r A \oplus A^{n-r}$. ■

Corollaire 4.1 Cas des groupes abéliens de type fini *Pour tout groupe abélien de type fini $M$ il existe un unique entier $r \geqslant 0$ et des uniques entiers $d_1 \mid \ldots \mid d_r \geqslant 2$ tel que*

$$M \simeq \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z} \times \mathbb{Z}^q$$

**Exemple 4.3** $M = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z}$. Par le théorème des restes chinois, on a

$$\begin{aligned} M &\simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \\ &\simeq (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \\ &\simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z} \end{aligned}$$

## 4.3 Application à la réduction des endomorphismes

Soit $k$ un corps. Décrivons un lien entre $k[X]$-modules et $k$ espaces vectoriels muni d'un endomorphisme.

Si $M$ est un $k[X]$-module, l'application $k \times M \to k[X] \times M \to M$ munit $M$ d'une structure de $k$-ev. Par ailleurs, l'application $u : M \to M$ telle que $u(m) = Xm$ est un endomorphismes $k$-linéaire de l'ev $M$. Notons $E$ le $k$-ev $M$.

Réciproquement, si $E$ est un $k$-ev muni d'un endomorphisme $k$-linéaire $u : E \to E$ alors on peut former un $k[X]$-module de $k$-ev sous-jacent $M = E$ avec la loi externe

$$\begin{cases} k[X] \times E & \to \quad E \\ (P, v) & \mapsto \quad P(u)(v) \end{cases}$$

 

On vérifie qu'on a une bijection entre les $k[X]$-modules de $M$ et les couples $(E, u)$ formés d'un $k$-ev et d'un endomorphisme $k$-linéaire. On a un dictionnaire :

| $(E, u)$ | $M$ |
|---|---|
| $v : E \to E$ qui commute avec $u$ | endomorphisme de $k[X]$-module |
| sous-espace stable sous $u$ | sous $k[X]$-module |
| $x \in E$ | morphisme $P \mapsto P(X)x$ |
| polynôme minimal (en dim finie) | générateur unitaire de $\text{Ann}(M)$ |

Dans la suite on note $E_u$ le $k[X]$-module associé à $E_u$. Dans le tableau, $\text{Ann}(E_u) = \{P \in k[X], \forall x \in E_u, Px = 0\}$. C'est un idéal de $k[X]$ donc il est principal, engendré par un unique polynôme unitaire.

**<u>Définition 4.2</u>** Soit $M$ un $k[X]$-module. On dit que $M$ est cyclique ssi il existe $P \in k[X]$ non nul tel que $M \simeq k[X]/(P)$.

**Lemme 4.3.1**
Soit $M$ un $k[X]$-module et $(E, u)$ l'ev avec endomorphisme qui lui correspond. Alors $M$ est $k[X]$-cyclique ssi $\dim_k(E) < \infty$ et il existe $x \in E$ tel que $\{x, u(x), \dots, u^{n-1}(x)\}$ engendre $E$pour $n \geqslant 0$.

*Démonstration.*

$\Rightarrow$ On a $M \simeq k[X]/(P)$ pour un certain polynôme $P \neq 0$ de degré $n$. Par division euclidienne, on voit que les classes $1, \underline{x}, \dots, \underline{x}^{n-1}$ de $1, X, \dots, X^{n-1}$ dans $M$ forment une base de $E$ (liberté car $(P) \setminus \{0\}$ ne contient que des polynômes de degré au moins $n$, et génératricité par DE). Posons $x = \overline{1}$, on a $u^i(x) = X^i\overline{1} = \overline{X}^u = x^i$. On a donc le résultat.

$\Leftarrow$ Choisissons $x$ tel que $n$ soit minimal. Considérons le morphisme

$$\varphi : \begin{cases} k[X] & \to & E \\ F & \mapsto & F(u)(x) \end{cases}$$

Ce morphisme est surjectif car $\{x, \dots, u^{n-1}(x)\}$ engendre $E$. Comme $\dim_k(E) < \infty$, $\varphi$ n'est pas injectif. Donc $\text{Ker}(\varphi) \neq 0$ est engendré par un unique polynôme non nul unitaire $P$.

En passant au quotient, on définit un isomorphisme de $k[X]/(P)$ sur $M$. ■

*Remarque 4.3 Si $M = E_u$ est un $k[X]$-module cyclique, notons $P$ tel que $M \simeq k[X]/(P)$. Dans la base $\{x, \dots, u^{n-1}(x)\}$, la matrice de $u$ est la matrice compagnon associée à $P$.*

 

<u>Théorème 4.4</u> Réduction de Frobénius *Soit $E$ un $k$-ev de dimension finie et $u$ un endomorphisme de $E$. Il existe des polynômes non constants unitaires $P_1, \dots, P_r \in k[X]$ tels que $P_1 \mid \dots \mid P_r$ et une base de $E$ telle que la matrice de $u$ dans cette base soit diagonales par blocs avec des blocs égaux aux matrices compagnon $c_{P_1}, \dots, c_{P_r}$ de $P_1, \dots, P_r$.*

*Les $P_i$ sont appelés facteurs invariants de $v$ et ne dépendent pas de la base choisie.*

*Démonstration.* Soit $M$ le $k[X]$-module associé à $(E, u)$. Comme $E$ est de dimension finie, il possède une base $\{e_1, \dots, e_n\}$ qui est un système de générateurs comme $k$-ev, donc a fortiori comme $k[X]$-module. Donc $M$ est de type fini comme $k[X]$-module.

Par la théorème de structure des modules de type fini sur $A = k[X]$, il existe une unique suite de $P_1 \mid \dots \mid P_r$ unitaires non inversibles telle que $E_u \simeq k[X]/(P_1) \times \dots \times k[X]/(P_r)$.

Comme $\dim_k(E) < \infty$, on a $P_i \neq 0$ pour tout $i$. Chaque $k[X]/(P_i)$ correspond à un sous-$k$-ev stable sous $u = E_i$. Par le lemùe et la remarque qui suit $E_i$ est cyclique et possède un une base dans laquelle la matrice de $u|_{E_i}$ et $c_{P_i}$. ■

*Remarque 4.4 On verra que $P_r$ est le polynôme minimal de $u$, $P_1 \dots P_r$ est le polynôme caractéristique de $u$ et que la suite des $I_i$ s'obtient en mettant une matrice de $X\,\mathrm{Id} - u$ sous forme normale de Smith.*

**Exemple 4.4** Trouver les facteurs invariants de l'endomorphisme défini par la matrice $\begin{pmatrix} 0 & 4 & 2 \\ -1 & -4 & -1 \\ 0 & 0 & -2 \end{pmatrix}$. On a

$$\begin{aligned} X\,\mathrm{Id} - M &= \begin{pmatrix} X & -4 & -2 \\ 1 & X+4 & 1 \\ 0 & 0 & X+2 \end{pmatrix} \sim \begin{pmatrix} 1 & X+4 & 1 \\ -X & 4 & 2 \\ 0 & 0 & X+2 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 0 & 0 \\ -X & 4+X(X+4) & X+2 \\ 0 & 0 & X+2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & (X+2)^2 & X+2 \\ 0 & 0 & X+2 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & (X+2)^2 & 0 \\ 0 & 0 & X+2 \end{pmatrix} \end{aligned}$$

Les facteurs invariants sont $X + 2$ et $(X + 2)^2$. Le polynôme minimal est donc $(X + 2)^2$ et le polynôme caractéristique est $(X + 2)^3$.

 

La réduite de Frobénius de $M$ est alors $\begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & 1 & -4 \end{pmatrix}$.

 

# Deuxième partie

# Théorie de Galois

# Introduction

On considère l'équation polynômiale $f = a_n X^n + \ldots + a_0 = 0$ avec $a_i \in k$ le corps de base.

On sait bien résoudre $aX^2 + bX + c \in \mathbb{Q}[X]$ qui a deux racines $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$, de même que $X^3 - aX - b$ qui s'écrivent (Tartaglia, 1535)

$$\sqrt[3]{\frac{b}{2} + \sqrt{\frac{b^2}{4} - \frac{a^2}{9}}} + \sqrt[3]{\frac{b}{2} - \sqrt{\frac{b^2}{4} - \frac{a^2}{9}}}$$

on peut aussi faire ça pour le degré 4, mais plus à partir de 5.

Cependant, manipuler des racines n'est pas sympathique, car on a des formules comme (Ramanujan)

$$\begin{aligned}
\sqrt{\sqrt[3]{5} - \sqrt[3]{4}} &= \frac{\sqrt[3]{2} + \sqrt[3]{20} - \sqrt[3]{25}}{3} \\
\sqrt[6]{7\sqrt[3]{20} - 19} &= \sqrt[3]{\frac{5}{3}} - \sqrt[3]{\frac{2}{3}}
\end{aligned}$$

 

# Chapitre 5

# Extensions de corps

On se place dans des anneaux commutatifs unitaires.

**Définition 5.1** Soit $k$ un corps.

- $K$ est une extension du corps $k$ ssi il existe un morphisme (unitaire) $\varphi : k \to K$ (forcément injectif). On note $k \hookrightarrow K$
- Un sous corps de $k$ est un corps $K \subset k$ compatible avec les lois de $k$.

**Définition 5.2** Si $k \hookrightarrow K$ alors le degré $[K : k]$ de l'extension est la dimension de $K$ en tant que $k$-ev.

**Exemple 5.1** $\mathbb{F}_p \hookrightarrow \mathbb{F}_p[X] \hookrightarrow \mathbb{F}_p(X)$ et on a $[\mathbb{F}_p(X) : \mathbb{F}_p] = \infty$.

**Lemme 5.0.1**
Soit $K$ un corps et $(K_i)_{i \in I}$ des sous-corps de $K$. L'intersection $\bigcap_{i \in I} K_i$ est un sous-corps.

*Démonstration.* L'intersection d'anneaux reste un anneau. Soit $a \in \bigcap_{i \in I} K_i$ non nul. $a \in K_i$ donc $a^{-1} \in K_i$ donc $a^{-1} \in \bigcap_{i \in I} K_i$, qui en devient un corps. ∎

**Définition 5.3** Soit $k$ un corps.

- Le corps premier de $k$ est l'intersection de tous les sous-corps de $k$.
- Pour $(\alpha_1, \ldots, \alpha_n)$ dans une extension $K$ de $k$, on définit $k(a_1, \ldots, a_n) = \bigcap_{\substack{a_1, \ldots a_n \in K_i \\ k \subset K_i}} K_i$ le plus petit sous-corps de $K$ (la plus petite extension de $k$) qui contient $k$ et $(a_1, \ldots, a_n)$.

**Définition 5.4** Soit $A$ un anneau. Le morphisme

$$\varphi : \begin{cases} \mathbb{Z} & \to & A \\ n & \mapsto & n1_A \end{cases}$$

$\mathrm{Ker}(\varphi)$ est un idéal donc de la forme $n\mathbb{Z}$. On dit que $A$ est de caractéristique $n$.

**Proposition 5.1** Soit $K$ un corps.
- Si la caractéristique de $K$ est 0, son corps premier est $\mathbb{Q}$.
- Si sa caractéristique est $n > 0$ alors $n$ est premier et le corps premier est $\mathbb{F}_n$.
- Si $K_1 \hookrightarrow K_2$ alors $K_1$ et $K_2$ ont même caractéristique et même corps premier.

*Démonstration.*
- $\varphi$ est injectif donc $\mathbb{Z}$ est inclus dans le corps premier de $K$ donc $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z}) \hookrightarrow K$ et $\mathbb{Q}$ est bien le plus petit sous-corps inclus dans $K$
- $\mathrm{Ker}\,\varphi = n\mathbb{Z}$. $\mathrm{Im}(\varphi) \subset K$ est donc intègre donc $\mathbb{Z}/n\mathbb{Z}$ intègre donc $n$ premier.
  De plus $\mathbb{Z}/n\mathbb{Z}$ est un sous-corps de $K$ et c'est bien le plus petit car le plus petit contient 1 donc $n \times 1$ donc $\mathbb{F}_n$.
- exo ■

**Proposition 5.2** Le cardinal d'un corps fini est une puissance d'un nombre premier.

*Démonstration.* Si $K$ est corps fini, son corps premier est $\mathbb{F}_p$ ($\mathbb{Q}$ infini). On a alors l'extension $F_p \hookrightarrow K$.

$K$ est donc un $\mathbb{F}_p$-ev de dimension $n$ (car $\{x, x \in K\}$ est une famille génératrice finie de $K$) donc $\mathrm{Card}(K) = p^n$. ■

*Remarque 5.1 On a $k \hookrightarrow k[X] \twoheadrightarrow k[X]/(f)$ donc $k[X]/(f)$ est une extension de $k$, c'est donc un $k$-ev dont une base est $(1, \overline{X}, \ldots, \overline{X}^{\deg f - 1})$.*

**Exemple 5.2** $f = X^5 + 5X + 5 \in \mathbb{Q}[X]$ est irréductible donc tout $g \neq 0$ de degré inférieur à 5 est premier à $f$ donc inversible dans le quotient. Son inverse est donné par son coefficient de Bezout et s'obtient facilement par Euclide.

**Proposition 5.3** Soit $k$ un corps, $f \in k[X]$ irréductible. Alors $K = k[X]/(f)$ est un corps et une extension de $k$.

**Exemple 5.3** $f = 2X+5 \in \mathbb{Q}[X]$, $\overline{X} \to -\frac{5}{2}$. Donc $k[X]/(f) = \mathbb{Q}(-\frac{5}{2}) = \mathbb{Q}$.

$f = X^3 - 2$, on peut prendre $K = \mathbb{Q}(a\sqrt[3]{2})$ avec $a \in \{1, j, j^2\}$.

**Proposition 5.4** Soit $\varphi : k \hookrightarrow K$ et $b \in K$. On pose $\varphi_{X \to b}(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \varphi(a_i) b^i$.

 

- $\mathrm{Ker}(\varphi_{X\to b})$ est de la forme $(f)$. Il existe un unique $f$ unitaire qui vérifie cette relation. On l'appelle polynôme minimal de $b$ sur $k$.
- tout $g \in k[X]$ qui s'annule en $b$ est divisible par $f$
- $f$ est irréductible ou nul
- Si $\mathrm{Ker}\,\varphi \neq (0)$, alors $(1, b, \dots, b^{\deg(f)-1})$ est une $k$-base de $\mathrm{Im}(\varphi_{X\to b})$ noté $k[b]$. En fait $k[b] = k(b)$.

*Démonstration.* Les deux premiers points sont faciles (principalité).

On a $k[X]/(f) \sim \mathrm{Im}(\varphi_{X\to b}) \subset K$ donc le quotient est intègre donc $(f)$ est premier donc $f$ irréductible. ∎

**<u>Définition 5.5</u>** Soit $\varphi : k \to K$ et $b \in K$.

Si $\mathrm{Ker}(\varphi_{X\to b}) = (0)$ alors $b$ est dit transcendant sur $k$. Dans le cas contraire il est dit algébrique.

**Proposition 5.5** Soit $k \hookrightarrow K$, $\alpha \in K$ est algébrique sur $k$ ssi il existe $k \hookrightarrow L \hookrightarrow K$ avec $[L : k] < \infty$ et $\alpha \in L$.

*Démonstration.*

$\Rightarrow$ Soit $\alpha$ algébrique sur $k$. On a $k(\alpha) \simeq k[X]/(\mu_{k,\alpha})$ qui admet la base $(1, \overline{X}, \dots, \overline{X}^{\deg \mu_{\alpha,k}})$.
On a $k \subset k(\alpha) \subset K$ (car $\alpha \in K$). Donc c'est fini

$\Leftarrow$ $(1, \alpha, \dots, \alpha^n)$ avec $n = [L : k]$ est liée sur $k$ donc on a $\sum_{i=0}^{n} a_i\alpha^i = 0$.
$\alpha$ est donc racine de $\sum_{i=0}^{n} a_i X^i$. ∎

**Lemme 5.0.2**
Soit $k \hookrightarrow L \hookrightarrow K$. On a

$$[K : k] < \infty \quad \text{ssi} \quad [L : k] < \infty \text{ et } [K : L] < \infty$$

Dans ce cas, on a $[K : k] = [K : L][L : k]$.

*Démonstration.*

$\Rightarrow$ $(v_1, \dots, v_n)$ partie $k$-génératrice finie de $K$ est aussi une partie $L$-génératrice de $K$ donc $[K : L] < \infty$.
Si on a une famille $k$-libre de $L$, elle est $k$-libre dans $K$ donc $[L : k] < [K : k] < \infty$.

$\Leftarrow$ Soit $(v_1, \dots, v_n)$ une $L$-base de $K$ et $(w_1, \dots, w_m)$ une $k$-base de $L$.
Tout élément $x \in K$ s'écrit $\sum_{i=1}^{n} \alpha_i v_i$ avec $\alpha_i = \sum_{j=1}^{m} \beta j, iw_i$ donc $(v_i w_j)_{i,j}$ est une $k$-base à $nm$ éléments de $K$. D'où l'égalité des dimensions. ∎

 

**Proposition 5.6** Soit $k \hookrightarrow K$. L'ensemble des éléments de $K$ algébriques sur $k$ forment un corps.

*Démonstration.* Soient $\alpha, \beta \in K$ algébriques sur $k$.

On montre que $\alpha - \beta$ et $\alpha\beta^{-1}$ ($\beta \neq 0$) sont algébriques. Pour le premier, c'est clair.

On considère l'extension $k \hookrightarrow k(\alpha) \hookrightarrow k(\alpha)(\beta)$. $\mu_{\beta,k} \in k[X] \subset k(\alpha)[X]$ donc $\mu_{\beta,k(\alpha)} \mid \mu_{\beta,k}$. En notant $n = \deg \mu_{\alpha,k}$ et $m = \deg \mu_{\beta,k}$, on trouve donc que $[k(\alpha)(\beta) : k] \leqslant mn < \infty$. ∎

**Exemple 5.4**

- $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. On a $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
  Comme $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2}))] \in \{1, 2\}$, on sait que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \in \{2, 4\}$.
  Ça ne peut pas être 2 car sinon $(1, \sqrt{2})$ serait une base et on aurait $\sqrt{3} = a + b\sqrt{2}$. Contradiction.
- Idem avec $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. Ça n'est pas de dimension 1 car $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$. Si $a_0 + a_1(\sqrt{2} + \sqrt{3}) + a_2(\sqrt{2} + \sqrt{3})^2 = 0$ donc $a_1 = a_2 = a_3 = 0$ ($(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ est une base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$). Ce n'est donc pas de dimension 2.
  On trouve que $(X^2 + 1)^2 - 12X^2$ annule $\sqrt{2} + \sqrt{3}$ et comme il est de degré 4, c'est le polynôme minimal.

**Proposition 5.7** Soit $k \hookrightarrow K$, $\alpha \in K$ transcendant sur $k$. On a alors

$$k(\alpha) \simeq k(X) = \mathrm{Frac}(k[X])$$

*Remarque 5.2 Dans le cas algébrique,* $k(\alpha) = k[\alpha]$ *(puisque* $\alpha$ *a un polynôme minimal et donc la suite* $(1, \alpha, \alpha^2, \ldots)$ *est liée)*

*Démonstration.* Notons $\varphi$ l'injection associée à $k \hookrightarrow K$. Par hypothèse, $\mathrm{Ker}(\varphi_{X\to\alpha}) = (0)$ et $\mathrm{Im}(\varphi_{X\to\alpha}) = k[\alpha]$.

Donc $k[X] \simeq k[\alpha] \subset k(\alpha)$ via $X \to \alpha$. On a de même $k[X] \to k(X) \to k(\alpha)$ via $X \to \alpha$. Ainsi, $k(X) \simeq k(\alpha)$. (On peut étendre tout morphisme de $k[X]$ dans un corps à un morphisme de $k(X)$ dans ce corps, et l'injectivité est conservée.). ∎

**Définition 5.6** Soit $k$ un corps et $f \in k[X]$, $\deg(f) \geqslant 1$. un corps de rupture de $f$ est une extension $K$ telle que

- $f$ admet un zéro $\alpha$ dans $K$
- $K = k(\alpha)$.

 

**Proposition 5.8** Soit $k$ un corps, $f \in k[X]$ irréductible, $\alpha$ un zéro dans une extension $K$. Il existe un unique isomorphisme $k[X]/(f) \to k(\alpha)$ qui vaut l'identité sur $k$ et qui envoie $\overline{X}$ sur $\alpha$.

Par conséquent, tout corps de rupture de $f$ sur $k$ est isomorphe au quotient $k[X]/(f)$.

*Démonstration.* $\varphi_{X\to\alpha} : k[X] \to k(\alpha)$ a pour noyau $(f_{\alpha,k})$. Par irréductibilité, $(f) = (f_{\alpha,k})$.

Ainsi, $k(\alpha) \simeq k[X]/(f)$ (surjectivité car $k(\alpha) = k[\alpha]$ car $\alpha$ racine de $f$ donc algébrique sur $k$) et envoie $\overline{X}$ sur $\alpha$ et vaut l'identité sur $k$.

L'unicité est claire car on donne l'image de $\overline{X}$ et de $k$. ■

**Exemple 5.5** $X^3 - 2 \in \mathbb{Q}[X]$. On a donc $\mathbb{Q}(\varepsilon\sqrt[3]{2})$ isomorphes entre eux ($\varepsilon \in \{1, j, j^2\}$).

<u>**Définition 5.7**</u> Soit $k \hookrightarrow K$. Alors deux éléments $\alpha$ et $\beta$ sont dits conjugués ssi ils ont même polynôme minimal.

<u>**Définition 5.8**</u> Soit $k$ un corps, $f \in k[X]$. $K$ est un corps de décomposition ssi

- $f$ est scindé sur $K$
- $K = k(\alpha_1, \ldots, \alpha_n)$.

<u>Théorème 5.1</u> *Soit $k$ un corps, $f \in k[X]$ non constant. Il existe un corps de décomposition $K$ avec $[K : k] \leqslant \deg(f)!$.*

*Démonstration.* Par récurrence sur $\deg(f)$. Si c'est 1, c'est fini.

Supposons que $\deg(f) > 1$ et que l'hypothèse de récurrence est vérifiée pour tout corps et tout polynôme de degré inférieur strictement à $n$. On écrit $f = h_1 \ldots h_m$ et on se place dans le cas non trivial où un des $h_i$ vérifie $\deg(h_i) > 1$ et on peut prendre $i = 1$.

Il existe donc un corps de rupture $k(\alpha_1)$ de $h_1$ sur $k$. Dans $k(\alpha_1)$, $h_1 = (X - \alpha_1)\widetilde{h}$ avec $\deg(\widetilde{h}) < \deg h_1 - 1$.

On a $\deg(\widetilde{h}h_2 \ldots h_m) < \deg f$ donc il existe un corps de décomposition $k(\alpha_1)(\alpha_2, \ldots, \alpha_{\deg f - 1})$.

On a enfin $[k : k(\alpha)] = \deg h_1 \leqslant \deg f$ et $[k(\alpha_1)(\alpha_2, \ldots, \alpha_{\deg f-1}) : k(\alpha_1)] = (\deg f - 1)!$ (permutaton des $\alpha_i, i > 1$). Donc

$$[k(\alpha_1)(\alpha_2, \ldots, \alpha_{\deg f-1}) : k] \leqslant (\deg f)!$$ ■

<u>Théorème 5.2</u> *Soit $\varphi : k_1 \to k_2$ un isomorphisme, $f \in k_1[X]$ irréductible, $k_1 \hookrightarrow K_1$, $k_2 \hookrightarrow K_2$, $\alpha$ un zéro de $f$ dans $K_1$ et $\alpha_2$ un zéro de $\varphi_{X\to X}(f)$ dans $K_2$.*

*Alors il existe $\overline{\varphi} : k_1(\alpha_1) \to k_2(\alpha)$ isomorphisme qui prolonge.*

 

*Démonstration.* $\varphi$ est un isomorphisme donc $\varphi_{X\to X}$ induit une correspondance des idéaux de $k_1[X]$ avec ceux de $k_2[X]$. On a alors

$$\begin{tikzcd}
k_1 \arrow[r, hook] \arrow[d, "\varphi"] & k_1[X] \arrow[r, two heads, "\pi_1"] \arrow[d, "\varphi_{X\to X}"] & k_1[X]/(f)\ \text{(corps !)} \arrow[r, hook, two heads] \arrow[d, hook] & k_1(\alpha_1) \\
k_2 \arrow[r, hook] & k_2[X] \arrow[r, two heads, "\pi_2"] & k_2[X]/(\varphi_{X\to X}(f))\ \text{(corps !)} \arrow[r, hook, two heads] & k_2(\alpha_2)
\end{tikzcd}$$

D'où un isomorphisme entre $k_1(\alpha_1)$ et $k_2(\alpha_2)$. ∎

<u>Théorème 5.3</u> Extension des isomorphismes *Soit $\varphi : k_1 \to k_2$ isomorphisme. Soit $f \in k_1[X]$.*

*Soit $K_1$ un corps de décomposition de $f$, $K_2$ un corps de décomposition de $\varphi_{X\to X}(f)$.*

*Alors il existe $\overline{\varphi} : K_1 \to K_2$ qui étend $\varphi$, ie pour tout $a \in k_1$, $\overline{\varphi}(a) = \varphi(a)$.*

*Démonstration.* Notons $n = \deg f$ et $m$ le nombre de racines de $f$ n'appartenant pas à $k_1$. On a donc $\alpha_1, \ldots, \alpha_m$ des racines de $f$ n'appartenant pas à $k_1$ et $\alpha_{m+1}, \ldots, \alpha_n$ racines de $f$ dans $k_1$.

On procède par récurrence sur $m$. Si $m = 0$ c'est fini car toutes les racines de $f$ sont dans $k_1$.

Si $m \geqslant 1$, $\alpha_1$ est racine d'un facteur irréductible $h$ de $f$. On a $f = h_1 h_2 \ldots h_l$ et, sur $k_1(\alpha_1)$, $h = (X - \alpha_1)\widetilde{h_1} h_2 \ldots h_l$. Par le théorème précédent, on étend $\varphi$ en $\overline{\varphi}$ à $k_1(\alpha_1) \to k_2(\beta_1)$ avec $\beta_1$ zéro de $\varphi_{X\to X}(h)$.

Dans $k_1(\alpha_1)$, $\widetilde{h_1} h_2 \ldots h_l$ a au plus $m - 1$ racines donc par hypothèse de récurrence, on étend $\overline{\varphi}$ à $\psi : K_1 \to K_2$ et ça marche ! ∎

Corollaire 5.1 *Soit $k$ un corps, $f \in k[X]$. Deux corps de décomposition de $f$ sur $k$ sont toujours isomorphes.*

**<u>Définition 5.9</u>** $f \in k[X]$ est radical ssi $f = X^n - a$.

Une extension est dire radicale simple ssi $K = k(\alpha)$ avec $\alpha$ un zéros d'un polynôme radical.

Une extension radicate de $k$ est une extension $K_n$ tel que $k = K_0 \subset K_1 \subset \ldots \subset K'_n$ avec $K_{i+1} = K_i(\alpha_i)$ radicale simple.

 

# Chapitre 6

# Clôture algébrique

**Définition 6.1** $K$ est algébriquement clos ssi pour tout $f \in K[X]$ tel que $\deg f \geqslant 1$ possède une racine dans $K$.

**Proposition 6.1** Soit $K$ un corps. Les assertions suivantes sont équivalentes.

(i) $K$ est algébriquement clos

(ii) tout $f \in K[X]$ est produit de facteurs de degré 1

(iii) les irréductibles de $K[X]$ sont de degré 1

(iv) toute extension algébrique de $K$ est de degré 1.

Théorème 6.1 *Pour tout corps $k$, il existe une extension de corps $K/k$ avec $K$ algébriquement clos.*

*Démonstration.* On peut définir $A[X_I]$ avec $I$ un ensemble quelconque comme une union croissante d'anneaux.

À $f \in k[X]$, on associe $X_f \in A := k[X_f, f \in k[X]]$. Posons $I$ l'idéal $(f(X_f), f \in k[X])$. Montrons que c'est un idéal propre.

Si $I = A$, alors $1 \in I$ donc il existe $g_1, \ldots, g_n$ tel que

$$g_1(f_1(X_{f_1})) + \cdots + g_n f_n(X_{f_n}) = 1$$

On construit une extension $\widetilde{k}$ de $k$ qui contient $(\alpha_1, \ldots, \alpha_n)$ zéros de $f_1, \ldots, f_n$. En évaluant en $X_1 \to \alpha_1 \ldots, X_n \to \alpha_n$, on obtient $0 = 1$. Contradiction.

$I$ est donc propre et il est donc inclus dans un idéal maximal $J$. $K_1 := A/J$ est un corps dans lequel tout polynôme de $k[X]$ possède une racine. On peut ainsi construire une suite croissante de corps $K_n \subset K_{n+1}$ tel que tout polynôme de $K_n[X]$ ait une racine dans $K_{n+1}$.

L'union croissante $K$ des $K_i$ est un corps. Montrons qu'il est algébriquement clos.

Si $f \in K[X]$, il existe $s$ tel que $f \in K_s[X]$. $K_{s+1}$ contient un zéro de $f$ donc $K$ aussi. ■

**Définition 6.2** Une extension algébrique de $k$ qui est algébriquement close est une clôture algébrique. On note une cloture $\overline{k}$.

THÉORÈME 6.2 *$\overline{k}$ existe et est unique à isomorphisme près.*

*Démonstration.* On prend $F$ l'ensemble des nombres algébriques du $K$ du théorème précédént. C'est bien un corps. Il faut montrer que tout $f \in F[x]$ possède une racine dans $F$. Il existe une racine $\alpha \in K$.

Notons $F = \sum_{i=0}^{n} a_i X^i$. On a $k \hookrightarrow k(a_i) \hookrightarrow k(a_i)(\alpha)$. Ce sont des extensions algébriques donc $\alpha$ est algébrique sur $k$ donc $\alpha \in F$. ■

 

# Chapitre 7

# Corps finis

## 7.1 Dérivation

**Définition 7.1** On définit l'opérateur de dérivation par

$$D : \begin{cases} k[X] & \to \quad k[X] \\ \sum_{i=0}^{n} a_i X^i & \mapsto \quad \sum_{i=0} i a_i X^{i-1} \end{cases}$$

**Lemme 7.0.1**
Soit $f \in k[X]$ tel que $f' = 0$.

1. Si $\mathrm{car}(k) = 0$ alors $f \in k$
2. Si $\mathrm{car}(k) = p$ alors $f = g(X^p)$ avec $g \in k[X]$.

**Lemme 7.0.2**
Soit $f \in k[X]$ non nul et $a \in k$.
$a$ est zéro multiple de $f$ ssi $f(a) = f'(a) = 0$ ssi $(X - a) \mid f \wedge f'$.

**Lemme 7.0.3**
Si $(X - a)^n \mid f$ alors $f(a) = f'(a) = \ldots = f^{(n-1)} = 0$ et la réciproque est vraie si et seulement si $\mathrm{car}(k) = 0$

## 7.2 Groupes cycliques

**Définition 7.2** L'exposant d'un groupe fini est le ppcm des ordres de ses éléments.

Théorème 7.1 *Si $A$ est un groupe abélien fini, il s'écrit $\mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$ avec $m_i \mid m_{i+1}$.*

Corollaire 7.1 *Soit $A$ un groupe abélien fini alors $A$ contient un élément d'ordre* $\exp A$.

*Démonstration.* On décompose $A$ en un produit de $\mathbb{Z}/m_i\mathbb{Z}$.

$(0,\dots,0,1)$ est d'ordre $m_k$ donc $m_k \mid \exp A$. De plus, $m_k(a_1,\dots,a_k)=0$ pour tout $(a_1,\dots,a_k)\in A$. Donc $\exp(A)\mid m_k$. ∎

Corollaire 7.2 *Soit $A$ abélien fini. S'il existe au plus un sous-groupe d'ordre $d$ dans $A$ pour tout $d \mid n$ alors $A$ est cyclique.*

*Démonstration.* Soit $m=\exp A$, $a$ un élément d'ordre $m$ et $b\in A$. $d := |\langle b\rangle| \mid m$. $a^{\frac{m}{d}}$ est d'ordre $d$ donc $\langle b\rangle = \langle a^{\frac{m}{d}}\rangle \subset \langle a\rangle$ donc $b\in\langle a\rangle$.

Donc $A\subset\langle a\rangle$. ∎

## 7.3 Racines de l'unité

**<u>Définition 7.3</u>** Soit $K$ un corps, $n\geqslant 1$, on pose $\mu_n(K)=\{\alpha\in K, \alpha^n=1\}$ l'ensemble des racines de l'unité.

Les éléments de $\mu_n$, s'ils existent, sont les racines primitives $n^{\text{e}}$ de l'unité

**Lemme 7.1.1**
$\mu_n$ est un sous-groupe de $K^*$ d'ordre au plus $n$.

*Démonstration.* C'est clairement un sous-groupe. Les $\alpha\in\mu_n$ sont zéros de $X^n-1$ qui a au plus $n$ racines donc $|\mu_n|\leqslant n$. ∎

<u>Théorème 7.2</u> *Soit $G$ un sous-groupe fini d'ordre $n$ de $K^*$. Alors $G=\mu_n(K)$ et $G$ est cyclique.*

*Démonstration.* Par Lagrange, pour tout $\alpha\in G$, $\alpha^n=1$ donc $\alpha$ est zéro de $X^n-1$ donc $\alpha\in\mu_n$.

Soit $H$ un sous-groupe de $G$ d'ordre $d\mid n$. On a $H\subset\mu_d$ qui est d'ordre au plus $d$. Donc $H$ est unique et $G$ est cyclique. Ainsi, $G$ est d'ordre $n$ donc $G=\mu_n$. ∎

<u>Théorème 7.3</u> *Soit $k$ un corps et $n\in\mathbb{N}$. Il existe une racine primitive $n^{\text{e}}$ de l'unité dans une extension $K/k$ ssi* $\mathrm{car}(k)=0$ *ou* $\mathrm{car}(k)\nmid n$.

*Démonstration.*

- $\Leftarrow$ $f:=X^n-1$ ne possède pas de zéros multiples car $f'=nX^{n-1}\neq 0$.
  Donc $f$ a $n$ zéros distincts (non nuls) $\alpha_1,\dots,\alpha_n$.
  $\{\alpha_i, i\in[\![1,n]\!]\}$ est un sous-groupe cyclique d'ordre $n$ donc il existe une racine primitive $n^{\text{e}}$.

 

$\Rightarrow$ Si $\xi$ est une racine primitive $n^e$, alors les $n$ éléments distincts de $\langle\xi\rangle$ sont racines de $X^n - 1$ donc ses racines sont simples donc $\operatorname{car} k = 0$ ou $n \nmid \operatorname{car} k$. ■

## 7.4 Corps finis

**Proposition 7.1** Soit $A$ un anneau commutatif de caractéristique $p \neq 0$.

$x \mapsto x^p$ est un morphisme (dit de Frobénius).

*Remarque 7.1 Si $A$ est un corps alors ce morphisme est bijectif.*

<u>Théorème 7.4</u> *Soient $p$ premier et $n \geqslant 1$. Il existe un corps $K$ à $p^n$ éléments isomorphe au corps de décomposition de $X^{p^n} - X \in \mathbb{Z}/p\mathbb{Z}[X]$.*

*Démonstration.* Soit $F$ un corps de décomposition de $f := X^{p^n} - X$.

$f' = p^n X^{p^n - 1} - 1 = -1$ donc $f$ a $p^n$ zéros simples distincts $(\alpha_1, \ldots, \alpha_{p^n})$ dans le corps de décomposition. Ce sont des points fixes du Frobénius donc $\{\alpha_1, \ldots, \alpha_{p^n}\}$ est un sous-corps, c'est donc le corps de décomposition ! ■

**Exemple 7.1** $f := X^4 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$ est irréductible. Donc le corps de rupture $\mathbb{Z}/2\mathbb{Z}[X]/f$ est de cardinal $2^4$ donc c'est le corps de décomposition de $X^{2^4} - X$ donc $X^4 + X + 1 \mid X^{16} - X$.

<u>**Définition 7.4**</u> On appelle $\mathbb{F}_{p^n}$ l'unique corps à $p^n$ éléments dans une clôture algébrique de $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$.

**Lemme 7.4.1**
Si $p$ est premier, $m, n \in \mathbb{N}$ tel que $m \mid n$. Alors $X^{p^m} - X \mid X^{p^n} - X$ dans $\mathbb{Z}[X]$.

*Démonstration.* On a $y^d - 1 = (y-1)(1 + \ldots + y^{d-1}$. Avec $y = p^m$ et $d = \frac{n}{m}$, on obtient que $p^m - 1 \mid p^n - 1$. Avec $y = X^{p^m - 1}$ et $d = \frac{p^n - 1}{p^m - 1}$, on trouve

$$X^{p^m - 1} - 1 \mid X^{p^n - 1} - 1$$

D'où le résultat. ■

**Lemme 7.4.2**
Tout sous-corps de $\mathbb{F}_{p^n}$ est de cardinal $p^d$ avec $d \mid n$ et pour tout $d \mid n$, il existe un sous-corps à $p^d$ éléments.

**Exemple 7.2** Quels sont les sous-corps de $\mathbb{F}_{2^{12}}$ ? Son sous-corps premier est $\mathbb{F}_2$ donc il sera contenu dans tous les sous-corps. Via le lemme précédent, on trouve le treillis suivant

 

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{F}_{2^{12}} \arrow[dl] \arrow[dr] & \\
\mathbb{F}_{2^6} \arrow[d] \arrow[dr] & & \mathbb{F}_{2^4} \arrow[dl] \\
\mathbb{F}_{2^3} \arrow[dr] & \mathbb{F}_{2^2} \arrow[d] & \\
 & \mathbb{F}_2 &
\end{tikzcd}$$

*Démonstration.*

$\Leftarrow$ Si $d \mid n$, $X^{p^d} - X \mid X^{p^n} - X$ donc $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ donc on a un sous-corps d'ordre $d$.

$\Rightarrow$ Soit $k$ un sous-corps de $K := \mathbb{F}_{p^n}$. à $q$ éléments. On a $\mathbb{F}_p \subset k \subset K$. Notons $m = [K : k]$.
On a $(p^d)^m = q^m = p^n$ donc $n = dm$ et $q = p^d$. ∎

Corollaire 7.3 *Soit $k$ un corps fini à $q = p^n$ éléments et $m \geqslant 1$ un entier. Il existe un polynôme $f \in k[X]$ de degré $m$ irréductible.*

*Démonstration.* $\mathbb{F}q^m$ est cyclique. Notons $\xi$ un générateur. On a $\mathbb{F}_{q^m} = \mathbb{F}_p(\xi)$.

On a $[\mathbb{F}_{q^m} : \mathbb{F}_p] = mn$ et $\mathbb{F}_{q^m} = \mathbb{F}_p[X]/(\mu_{\xi,\mathbb{F}_p})$. Donc $\deg(f_{\xi,\mathbb{F}_p}) = mn$.

Si on considère $\mu_{\xi,\mathbb{F}_q}$, son degré est $[\mathbb{F}_q(\xi) : \mathbb{F}_q] = [\mathbb{F}_{q^m} : \mathbb{F}_q] = m$.

On a donc trouvé un polynôme irréductible de degré $m$. ∎

Corollaire 7.4 *$X^{p^n} - X$ est le produit des irréductibles unitaires de $F_p[X]$ dont le degré divise $n$.*

*Démonstration.* Fixons $\overline{\mathbb{F}_p}$.

1. Les polynômes irréductibles de degré $m \mid n$ divisent $X^{p^n} - X$. Soit $f \in \mathbb{F}_p[X]$ irréductible de degré $m$.
   $\mathbb{F}_p[X]/(f)$ est de cardinal $p^m$ donc il est isomorphe à l'ensemble des zéros de $X^{p^m} - X$, inclus dans $\mathbb{F}_{p^n}$.
   $f$ et $X^{p^n} - X$ possèdent un zéro commun dans $\overline{\mathbb{F}_p}$ donc, comme $m \mid n$, $f \mid X^{p^n} - X$.
2. Si $f$ est un facteur irréductible de $X^{p^n} - X$, posons $k = \mathbb{F}_p[X]/(f)$ qui a $p^{\deg f}$ éléments. On sait que $k \subset \mathbb{F}_{p^n}$ donc $\deg f \mid n$.
3. Il n'y a pas de facteurs multiples car $(X^{p^n} - X)' = -1$. ∎

Corollaire 7.5 *Soit $k$ un corps fini et $f \in k[X]$ irréductible/ Le corps de rupture $k[X]/(f)$ est aussi (déjà) le corps de décomposition de $f$.*

*Démonstration.* On note $k = \mathbb{F}_q$ $(q = p^n)$ et $K = k/(f)$. C'est un corps à $q^{\deg f}$ éléments, donc c'est l'ensemble des zéros de $X^{p^{n \deg f}} - X$.

$f$ divise $X^{p^{n \deg f}} - X$ dans $\mathbb{F}_q[X]$. $K$ contient les zéros de ce dernier donc de $f$. C'est donc le corps de décomposition. ∎

 

*Remarque 7.2* *Soit* $X^3 - 2 \in \mathbb{Q}[X]$*. On a* $j\sqrt[3]{2} \notin \mathbb{Q}[\sqrt[3]{2}]$ *donc un corps de rupture n'est pas toujours un corps de décomposition quand le corps est infini.*

 

# Chapitre 8

# Extensions normales et séparables

**Définition 8.1** $f \in k[X]$ est séparable ssi tous les zéros de $f$ dans un corps de décomposition de $f$ sont de multiplicité 1.

Un élément $\alpha \in K/k$ est séprable ssi $\mu_{\alpha,k}$ est séparable. $K/k$ est séparable ssi tous les $\alpha \in K$ le sont sur $k$.

**Proposition 8.1** Soit $f \in k[X]$ irréductible. Si $f' \neq 0$ alors $f$ est séparable.

En particulier, si $\mathrm{car}(k) = 0$ alors $f$ est séparable et sinon, soit $f$ est séparable, soit $f \in \mathrm{Ker}(D)$.

*Démonstration.* Soit $\alpha$ un zéro de $f$ dans $K/k$. $f$ est irréductible ie $f = \lambda\mu_{\alpha,k}$.

Si $f' \neq 0$ alors $\deg f' < \deg f$. Si $\alpha$ est racine multiple, $(X - \alpha) \mid f \wedge f'$. Il existe donc un pgcd non trivial de $f$ et $f'$.

Donc $f$ n'est pas irréductible. Contradiction. Donc $f' = 0$. ∎

Corollaire 8.1 *Si $k$ est de caractéristique $0$ alors $K/k$ est séprable.*

**Définition 8.2** Un corps $k$ est parfait ssi toute extension algébrique de $k$ est séparable.

Théorème 8.1 *$k$ est parfait ssi $\mathrm{car}(k) = 0$ ou ($\mathrm{car}(k) = p$ et $k^p := \{a^p, a \in k\} = k$).*

Corollaire 8.2 *Un corps fini est parfait.*

*Démonstration.* Le Frobénius est un automorphisme donc on a bien $k^p = k$. ∎

*Démonstration du théorème.* Le cas de la caractéristique 0 est déjà traité.

Si $\mathrm{car}(k) = p$ et $\alpha \in k$ algébrique inséparable, on a $\mu'_{\alpha,k} = 0$ donc $\mu_{\alpha,k} = \displaystyle\sum_{i=1}^{n} a_i X^{pi} = \sum_{i=1}^{n} (b_i X^i)^p$ (surjectivité du Frobénius par hypothèse).

Donc $\mu_{\alpha,k} = \left(\displaystyle\sum_{i=1}^{n} b_i X^i\right)^p$ n'est pas irréductible. Contradiction et $\alpha$ est séparable. Donc $k$ est parfait. ∎

**Définition 8.3** $k \hookrightarrow K$ est normale ssi tout $f \in k[X]$ irréductible qui possède un zéro dans $K$ est scindé sur $K$.

**Exemple 8.1**
- $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt[3]{2})$ n'est pas normale car $X^3 - 2$ a une racine mais n'est pas scindé dedans.
- Si $[K : k] = 2$ alors $K/k$ est normale car si on a une racine $\alpha$ on est déjà scindé (factorisable par $X - \alpha$).

<u>Théorème 8.2</u> *$K/k$ de degré fini est normale ssi $K$ est un corps de décomposition d'un polynôme $f \in k[X]$.*

*Démonstration.*

$\Rightarrow$ On écrit $K = k(\alpha_1, \dots, \alpha_n)$. Les $f_{\alpha_i,k}$ sont tous scindés. $K$ est alors le corps de décomposition de $g := \displaystyle\prod_{i=1}^{n} f_{\alpha_i,k}$.

$\Leftarrow$ Posons $K$ un corps de décomposition de $g$ sur $k$ et $f \in k[X]$ ayant une racine $\alpha \in K$. Soit $\beta$ une autre racine de $f$.
Posons $L$ le corps de décomposition de $f$ sur $K$. On a le diagramme

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K(\alpha) \arrow[r, dash] \arrow[d, dash] & K \arrow[r, dash] \arrow[d, dash] & K(\beta) \arrow[d, dash] \\
k(\alpha) \arrow[r, dash] & k \arrow[r, dash] & k(\beta)
\end{tikzcd}$$

On a $K(\alpha) = K$ et les relations

$$[K : k] = [K(\alpha) : k] = [K(\alpha) : k(\alpha)][k(\alpha) : k]$$

$$[K(\beta) : K][K : k] = [K(\beta) : k(\beta)][k(\beta) : k]$$

$L$ est aussi le corps de décomposition de $f$ sur $K(\alpha)$ ou $K(\beta)$.
$k(\alpha)$ et $k(\beta)$ sont deux corps de rupture donc isomorphes. On peut étendre cet isomorphisme à $\varphi : K(\alpha) \to K(\beta)$ puisque ce sont des corps de décomposition de $g$ sur $k(\alpha)$ et $k(\beta)$ (isomorphes).

 

Donc

$$[k(\alpha):k] = [k(\beta):k] \text{ et } [K(\alpha):k(\alpha)] = [K(\beta):k(\beta)]$$

Ainsi, $[K(\beta):K][K:k] = [K:k]$ donc $K(\beta) = K$ et $\beta \in K$. ■

Corollaire 8.3 *Soit $K/k$ une extension normale de degré fini, $L$ tel que $k \subset L \subset K$.*

*Tout $k$-morphisme $\varphi : L \to K$ ($\varphi|_k = \mathrm{Id}_k$) s'étend en un morphisme de $K \to K$.*

**Définition 8.4** On note $S_{g,k}$ le corps de décomposition de $g$ sur $k$.

*Démonstration.* $\varphi$ fixe $k$ donc pour un $g$ tel que $K = S_{g,k}$, on a $\varphi(g) = g$ donc $K = S_{\varphi(g),k}$.

On a aussi $S_{g,L} = S_{g,k} = K = S_{\varphi(g),L}$. Donc on étend $\varphi$ aux corps de décompositions et on obtient l'extension voulue. ■

Corollaire 8.4 *SOit $K/k$ normale de degré fini et $f \in k[X]$ irréductible, $\alpha_1, \alpha_2$ deux zéros de $f$ dans $K$. Il existe un $k$-automorphisme $\varphi : K \to K$ tel que $\varphi(\alpha_1) = \alpha_2$.*

*Démonstration.* Appliquer le théorème avec $L = k(\alpha_1)$. ■

**Définition 8.5** On appelle groupe de Galois de $K/k$ et on note $G(K/k)$ l'ensemble des $k$-automorphismes de $K$.

Soit $G$ inclus dans l'ensemble des automorphismes de $K$. Le corps fixe, noté $K^G$ est l'ensemble des éléments de $K$ fixés par tous les éléments de $G$.

**Exemple 8.2** $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{Id}\}$.

**Proposition 8.2** $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ est cyclique d'ordre $n$ et engendré par le Frobénius.

*Démonstration.* $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ avec $\alpha$ racine $p^n - 1^{\text{e}}$ de l'unité.

$\deg(\mu_{\alpha,\mathbb{F}_p}) = n$ donc si $\sigma$ est un automorphisme, on a $n$ choix pour $\sigma(\alpha)$ donc $\mathrm{Card}(G(\mathbb{F}_{p^n}/\mathbb{F}_p)) \leqslant n$.

Or le Frobénius $f$ appartient à $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ donc ses puissances aussi.

Si $i \neq j$ et $f^i = f^j$ donc $f^{j-i} = \mathrm{Id}$ donc $p^{j-i} = p^n$. Or $j - i < n$. Contradiction. Ainsi, on a trouvé $n$ éléments distincts de $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ d'où le résultat. ■

**Proposition 8.3** Soit $\alpha$ une racine primitive $n^{\text{e}}$ de l'unité (existence si $p \nmid n$). Posons $K = k(\alpha)$. $G(K/k)$ est abélien fini est c'est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$.

 

**Proposition 8.4** Soit $K = k(\alpha)$ avec $\alpha$ une racine primitive $n^{\text{e}}$ de 1.
$G(K/k)$ est isomorphe à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$, donc abélien.

*Démonstration.* $k(\alpha)$ contient toutes les racines de $X^n - 1$ c'est un corps de décomposition. Soit $\sigma \in G(K/k)$.

$\sigma$ est déterminé par $\sigma(\alpha)$ qui est d'ordre $n$ puisque $\alpha$ l'est. Donc $\sigma(\alpha) = \alpha^i$ avec $i \wedge n = 1$.

On appelle $\sigma_i$ l'élément de $G(K/k)$ qui envoie $\alpha$ sur $\alpha^i$. On obtient donc une application

$$\psi : \begin{cases} G(K/k) & \to & (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma_i & \mapsto & i \end{cases}$$

qui est (assez clairement) un morphisme de groupes injectif. ∎

**Définition 8.6** Une extension algébrique est galoisienne ssi $k = K^{G(K/k)}$.

$\text{Aut}(K)$ agit sur $K$. On considère l'orbite de $\alpha \in K$ sous l'action de $G(K/k)$. Notons $\mu_{\alpha,k} = \sum_{i=0}^{n} a_i X^i$. Si $\sigma \in G(K/k)$, on a $\sigma(f(\alpha)) = f(\sigma(\alpha))$.

**Définition 8.7** Soit $\alpha \in K$ algébrique sur $k$. Alors les conjugués de $\alpha$ sont les éléments de l'orbite de $\alpha$ sous $G(K/k)$. Il y en a un nombre fini par ce qui précède.

**Lemme 8.2.1**
Soit $K/k$ galoisienne finie et $\alpha \in K$ algébrique sur $k$. Les conjugués de $\alpha$ sous $G(K/k)$ est un ensemble fini $\{\alpha_1 = \alpha, \dots, \alpha_m\}$ et

$$\mu_{\alpha,K} = \prod_{i=1}^{n} (X - \alpha_i) = \prod_{\sigma} (X - \sigma(\alpha))$$

où le dernier produit est indicé par les représentants des classes à gauche de $\text{Stab}(\alpha)$.

*Démonstration.* Tous les $\alpha_i$ sont racines de $\mu_{\alpha,k}$. On pose $g = \prod_{i=1}^{m} \alpha_i$. Ses coefficients sont des fonctions symétriques des racines $\alpha_i$ qui sont donc invariants par permutation des racines donc aussi sous l'action de de $G(K/k)$, donc dans $k$.

Ainsi, $g \in k[X]$. Or $\deg(g) = m \leqslant n = \deg(\mu_{\alpha,k})$ donc nécessairement, $m = n$ et $g = \mu_{\alpha,k}$. ∎

Corollaire 8.5 *Soit $k \subset K$ galoisienne, $\alpha \in K$ algébrique sur $k$. $[k(\alpha) : k] = \deg(\mu_{\alpha,k})$ est le nombre de racines de $\mu_{\alpha,k}$ sur $K$.*

 

Théorème 8.3 *Soit $K/k$ de degré fini. Les assertions suivantes sont équivalentes :*

(i) *$K/k$ est galoisienne*

(ii) *$K/k$ est normale séparable*

(iii) *$K/k$ est le corps de décomposition d'un polynôme séparable*

*Démonstration.*

(i) ⇒ (ii) $K/k$ est galoisienne et $\alpha \in K$. Alors $\alpha$ est algébrique. $\mu_{\alpha,k} = \prod_{i=1}^{n}(X-\alpha_i)$. Donc l'extension est normale. Elle est de plus séparable car les $\alpha_i$ sont distincts.

(ii) ⇒ (iii) On écrit $K = k(\alpha_1, \dots, \alpha_m)$. $g = \mu_{\alpha_1,k} \dots \mu_{\alpha_m,k}$ est scindé sur $K$ et toutes les racines de $g$ sont simples (produit de polynômes SARS premiers entre eux). Notons $L = k(\alpha_{1,1}, \dots, \alpha_{1,n_1}, \dots, \alpha_{m,1}, \dots, \alpha_{m,n_m})$ le corps de décomposition de $g$. On remarque que $K \subset L$ et $L \subset K$ puisque, comme l'extension est normale, tous les $\alpha_{i,j}$ appartiennent à $K$. Donc $K$ est le corps de décomposition.

(iii) ⇒ (i) $K/k$ est le corps de décompositon d'un polynôme séparable $f$. Il faut montrer que $K^{G(K/k)} = k$. On procède par récurrence sur $[K : k]$ pour tout corps.
Si $[K : k] = 1$, $K = k$ donc $G(K/k) = \{1\}$ et $K^{\{1\}} = K = k$. On suppose vérifié le resultat pour tout extension de corps $[\widetilde{K} : \widetilde{k}] = \widetilde{m} < n$. Comme $[K : k] > 1$, $f$ possède un facteur irréductible $g$ de degré $> 1$ (sinon $f$ scindé sur $k$).
Les zéros de $g$ sont zéros de $f$ donc tous distincts. Notons $\{\alpha = \alpha_1, \dots, \alpha_m\}$ les zéros de $g$. Les $k(\alpha_i)$ sont isomorphes à $k(\alpha)$ via $\varphi_i : k(\alpha) \to k(\alpha_i)$. On peut étendre $\varphi_i$ en un morphisme $\overline{\varphi_i} : K = S_{f,k(\alpha)} \to S_{f,k(\alpha_i)}$.
Par hypothèse de récurrence, $k(\alpha) = K^{G(K/k(\alpha))}$ et on a l'inclusion $G(K/k(\alpha)) \subset G(K/k)$. Donc $F := K^{G(K/k)}$ vérifie $k \subset F \subset k(\alpha)$. Ainsi, $F(\alpha) = k(\alpha)$. Pour montrer que $F = k$, on compare $\mu_{\alpha,F}$ et $\mu_{\alpha,k}$. On sait que $\mu_{\alpha,F} \mid \mu_{\alpha,k}$. On sait que $F$ est fixe par $\overline{\varphi_i}$ ($K/k(\alpha)$ galoisienne). On écrit $\mu_{\alpha,f} = \sum_{i=0}^{l} b_i X^i$. On a $\overline{\varphi_j}\left(\sum_{i=0}^{l} b_i \alpha^i\right) = 0$ donc $\mu_{\alpha,F}$ a les mêmes zéros que $\mu_{\alpha,k}$ donc $[F(\alpha) : F] = [F(\alpha) : k]$ donc $[F : k] = 1$. Le principe de récurrence conclut. ■

**Proposition 8.5** Soit $f \in k[X]$ séparable et $K = S_{f,k}$ avec $\deg(f) = n$ zéros. Alors $G(K/k)$ permute les zéros. On a donc un morphisme $\varphi : G(K/k) \to \mathfrak{S}_n$ injectif.

 

Si $f$ est irréductible alors $G(K/k)$ est isomorphe à un sous-groupe transitif de $\mathfrak{S}_n$ (ie qui a une seule orbite : on peut envoyer tout le monde sur tout le monde).

*Démonstration.* $\mathrm{Ker}(\varphi) = \bigcap_i \mathrm{Stab}(\alpha_i) = \{1\}$ donc injectif.

Supposons que l'action n'est pas transitive. On a $\alpha$ racine de $f$ tel que $\{\alpha = \alpha_1, \ldots, \alpha_m\}$ avec $m < \deg f$. $\mu_{\alpha,f} = \prod_i (X - \alpha_i)$ est de degré $< \deg(f)$ donc $f$ n'est pas irréductible. ■

 

# Chapitre 9

# Correspondance de Galois

**Définition 9.1** Soit $G$ un groupe et $K$ un corps. Un caractère (linéaire) est un morphisme de groupe $\chi : G \to K^*$.

**Exemple 9.1** À $\sigma \in \mathrm{Aut}(K)$, on peut associer un caractère $\chi_\sigma : K^* \to K^*$.

**Définition 9.2** $(\chi_1, \ldots, \chi_n)$ est linéairement indépendant sur $K$ ssi l'égalité $\sum_{i=1}^{n} a_i \chi_i = 0$ implique $a_i = 0$.

**Lemme 9.0.1 Dedekind**
Tout ensemble fini de caractères distincts est linéairement indépendant.

*Démonstration.* Par récurrence sur le nombre de caractères. Si $n = 1$, $a_1 \chi = 0$ donc $a_1 \chi(1) = 0$ donc $a_1 = 0$.

Si l'hypothèse est vraie pour $n - 1$. Si $\sum_{i=1}^{n} a_i \chi_i = 0$ avec $a_i$ non tous nuls, on peut permuter pour avoir $a_1 \neq 0$.

Comme $\chi_1 \neq \chi_n$, il existe $g \in G$ tel que $\chi_1(g) \neq \chi_n(g)$. On a pour tout $h \in G$,

$$\sum_{i=1}^{n} a_i \chi_i(h) = 0$$

Pour $h \leftarrow gh$, on a

$$\sum_{i=1}^{n} a_i \chi_i(g) \chi_i(h) = 0$$

La première formule donne :

$$\sum_{i=1}^{n} a_i \chi_i(h) \chi_n(g) = 0$$

et en faisant la différence, on a

$$\sum_{i=1}^{n-1} a_i(\chi_n(g) - \chi_i(g))\chi_i(h) = 0$$

donc (HR) pour tout $i$, $a_i(\chi_n(g), \chi_i(g)) = 0$. Contradiction pour $i = 1$. ∎

**Lemme 9.0.2**
Soit $K$ un corps, $\sigma_1, \ldots, \sigma_n$ des automorphismes distincts qui forment un sous-groupe $G$ de $\mathrm{Aut}(K)$.

Alors $[K : K^G] = n$.

*Démonstration.* Supposons que $[K : K_G] = r < n$, $\alpha_1, \ldots, \alpha_r$ une $K^G$-base. On pose $M = (\sigma_j(\alpha_i))_{i,j}$. L'équation $MX = 0$ a $n$ inconnues et $r$ équations donc il existe une solution non nulle.

Soit $\beta \in K$ un élément. il s'écrit $\sum_{j=1}^{r} b_j\alpha_j$. On a

$$\sum_{i=1}^{n} a_i\sigma_i(\beta) = \sum_{i=1}^{n}\sum_{j=1}^{r} a_i b_j \sigma_i(\alpha_j) = \sum_{j=1}^{r} b_j \sum_{i=1}^{n} a_i\sigma_i(\alpha_j) = \sum_{j=1}^{r} b_j \times 0 = 0$$

Contradiction.

Supposons que $r > n$, on prend $\alpha_1, \ldots, \alpha_{n+1}$ linéairement indépendants. Avec $M = (\sigma_i(\alpha_j))_{i,j}$, l'équation $MX = 0$ a plus l'inconnues que d'équations donc admet une solution non nulle $(\beta_1, \ldots, \beta_{n+1})$.

Quitte à réordonner, on prend $\sigma_1 = \mathrm{Id}$. Posons $(\beta_1, \ldots, \beta_s = 1, 0, \ldots, 0)$ avec un nombre minimal de composantes non nulles. $s > 1$ car sinon $\beta_1\alpha_1 = \sigma_1(\beta_1\alpha_1) = 0$ donc $\beta_1 = 0$. On a donc

$$\beta_1\sigma_i(\alpha_1) + \ldots + \beta_{s-1}\sigma_i(\alpha_{s-1}) + \sigma_i(\alpha_s) = 0$$

Les $\beta_i$ ne sont pas tous dans $K^G$. En effet, si $\beta_i \in K^G$ pour tout $o$ ;

$$\sum_{i=1}^{n+1} \beta_i\alpha_i = \sigma_1\left(\sum_{i=0}^{n+1} \beta_i\alpha_i\right) = \sum_{i=0}^{n+1} \beta_i\sigma_1(\alpha_i) = 0$$

donc pour tout $i$, $\beta_i = 0$, contradiction. On suppose donc $\beta_1 \in K \setminus K^G$ après renumérotation. Il existe $m$ tel que $\sigma_m(\beta_1) \neq \beta_1$. Pour tout $\sigma_i \in G$, il existe $\sigma_j \in G$ tel que $\sigma_i = \sigma_m\sigma_j$.

En appliquant $\sigma_m$, on obtient

$$\sigma_m(\beta_1)\sigma_m\sigma_j(\alpha_1) + \ldots + \sigma_m(\beta_{s-1})\sigma_m\sigma_j(\alpha_{s-1}) + \sigma_m\sigma_j(\alpha_s) = 0$$

 

Donc
$$\sigma_m(\beta_1)\sigma_i(\alpha_1)+\ldots+\sigma_m(\beta_{s-1})\sigma_i(\alpha_{s-1})+\sigma_i(\alpha_s)=0$$
On a aussi
$$\beta_1\sigma_i(\alpha_1)+\ldots+\beta_{s-1}\sigma_i(\alpha_{s-1})+\sigma_i(\alpha_s)=0$$
En faisant la différence,
$$(\beta_1-\sigma_m(\beta_1))\sigma_1(\alpha_1)+\ldots+(\beta_{s-1}-\sigma_m(\beta_{s-1}))\sigma_i(\alpha_{s-1})=0$$
Or $s$ était supposé minimal donc pour tout $i$, $\beta_i=\sigma_m(\beta_i)$. On obtient une contradiction pour $i=1$.

Finalement $r=n$. ∎

Corollaire 9.1 *Soit $K/k$ de degré fini. L'extension $K/k$ est galoisienne ssi $|G(K/k)|=[K:k]$*

Corollaire 9.2 *Soit $\alpha$ algébrique sur $k$. $k(\alpha)/k$ est galoisienne ssi $\mu_{\alpha,k}$ possède $[k(\alpha):k]=\deg(\mu_{\alpha,k})$ zéros dans $k$.*

On a une application entre les sous-corps de $K$ et les sous-groupes de $G(K/k)$ donnée par $L\mapsto G(K/L)$. Cette application est décroissante et on va montrer qu'elle est bijective d'inverse $H\mapsto K^H$.

Corollaire 9.3

(i) *Soit $H$ un sous-groupe fini de* $\mathrm{Aut}(K)$ *et $L=K^H$. Alors tout $G(K/L)\subset H$.*

(ii) *Soient $H_1$ et $H_2$ deux sous-groupes distincts de* $\mathrm{Aut}(K)$, *alors $K^{H_1}\neq K^{H_2}$*

*Démonstration.*

(i) Notons $n=|H|=[K:K^H]$. S'il existe $\sigma\in\mathrm{Aut}(K)\setminus H$ qui fixe $K^H$ alors $\sigma\in G(K/K^H)$ qui serait d'ordre $>|H|$. Or $|G(K/K^H)|=[K:K^H]$.

(ii) Par contraposée, si $K^{H_1}=K^{H_2}$, alors on a deux inclusions qui impliquent chacune $H_1\subset H_2$ et $H_2\subset H_1$ par (i). Donc $H_1=H_2$. ∎

Corollaire 9.4 *Soiut $G\subset$* $\mathrm{Aut}(K)$ *qui fixe $k\subset K$ et $H\subset G$. Si $L=K^H$ alors pour tout $\sigma\in G$, $\sigma(L)=K^{\sigma H\sigma^{-1}}$.*

*Démonstration.*

$\subset$ Pour $a\in L$ et $\tau\in H$, on a $\sigma\tau\sigma^{-1}(\sigma(a))=\sigma(\tau(a))=\sigma(A)\in\sigma(L)$.

$\supset$ Si pour $b\in K$, on a $\sigma\tau\sigma^{-1}(b)=b$ donc $\tau\sigma^{-1}(b)=\sigma^{-1}(b)$ donc $\sigma^{-1}(b)\in L$ et $b\in\sigma(L)$. ∎

 

<u>Théorème 9.1</u> Galois *Soit $K/k$ galoisienne de degré fini.*

(i) *Les applications $f : L \to G(K/L)$ et $g : H \to K^H$ sont bijectives et inverses l'une de l'autre.*

(ii) $[K : L] = |G(K/L)|$ *et* $[L : k] = (G(K/k) : G(K/L))$

(iii) *$L/k$ est normale ssi $G(K/L) \lhd G(K/k)$. Dans ce cas, on a l'égalité $G(L/k) = G(K/k)/G(K/L)$.*

*Démonstration.*

(i) Comme $K/k$ est galoisienne, $K/L$ le reste donc $K^{G(K/L)} = L$ donc $g \circ f = \mathrm{Id}$ donc $g$ surjective. On sait que $g$ est injective par un des corollaires précédents donc $g$ est bijective.

(ii) On a

$$|G(K/k)| = [K : k] = [K : L][L : k] = [K : L][L : k] = |G(K/L)|[L : k]$$

Donc $[L : k] = \frac{|G(K/k)|}{|G(K/L)|}$.

(iii) Supposons $H = G(K/L) \lhd G(K/k)$. Pour tout $\sigma \in G(K/k)$, $\sigma(L) = K^{\sigma H \sigma^{-1}} = K^H = L$. Posons

$$\varphi : \begin{cases} G(K/k) & \to & G(L/k) \\ \sigma & \mapsto & \sigma|_L \end{cases}$$

C'est un morphisme surjectif de noyau $G(K/L)$ donc on a l'isomorphisme $G(L/k) = G(K/L)G(L/k)$. ■

**<u>Définition 9.3</u>** Soit $K/k$ algébrique. On dit que $K/k$ est simple s'il existe $\alpha \in K$ tel que $K = k(\alpha)$.

<u>Théorème 9.2</u> *Soit $K/k$ algébrique de degré fini. Il existe un nombre fini de corps intermédiaires $k \subset L \subset K$ ssi l'extension est simple.*

*Démonstration.*

$\Rightarrow$ Si $k$ est fini alors $K$ aussi et si on note $\alpha$ un générateur de $K^*$, $K = k(\alpha)$ donc l'extension est simple.

Si $k$ est infini alors on écrit par hypothèse $K = k(\alpha_1, \ldots, \alpha_n)$ (puisque $k \subsetneq k(\alpha_1) \subsetneq (\alpha_1, \alpha_2) \ldots$ fournit une suite de sous-corps qui est fini).

On démontre le résultat par récurrence sur $n$, le cas $n = 1$ étant trivial. Pour le cas $n$, on écrit

$$k(\alpha_1, \ldots, \alpha_n) = k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = k(\beta)(\alpha_n)$$

par HR.

 

Si pour tout $a \in k$, les $k(a\beta+\alpha_n)$ sont distincts, on a une contradiction ($k$ infini et il y a une nombre fini de sous-corps). Donc il existe $a' \neq a$ tel que $k(a\beta + \alpha_n) = k(a'\beta + \alpha_n)$.
Donc $a'\beta + \alpha_n \in k(a\beta + \alpha_n)$. On a ainsi

$$\frac{(a'\beta + \alpha_n) - (a\beta + \alpha_n)}{a' - a} = \beta \in k(a\beta + \alpha_n)$$

Donc $k(\beta, \alpha_n) \subset k(a\beta + \alpha_n)$ et l'inclusion réciproque est triviale. Le principe de récurrence conclut.

$\Leftarrow$ Si $K = k(\alpha)$ et $k \subset L \subset K$, on a $K = L(\alpha)$. On a $[K : L] = \deg(\mu_{\alpha,L})$ avec $\mu_{\alpha,L} \mid \mu_{\alpha,k}$.
On écrit $f_{\alpha,L} = \sum_{i=0}^{m} b_i X^i$. On va montrer que $F := k(b_0, \ldots, b_m) = L$.
On sait déjà $F \subset L$. On montre que $[L : F] = 1$. Or on a BUG ■

Corollaire 9.5 *Toute extension séparable de degré fini est simple.*

*Démonstration.* On écrit $K = k(\alpha_1, \ldots, \alpha_n)$ et $g$ le produit des $\mu_{\alpha_i,k}$. On pose $L = S_{g,k}$.

On a un nombre fini de sous-groupes $H$ tel que $G(L/k) = \{\mathrm{Id}\} \subset H \subset G(K/k)$ donc un nombre fini de corps intermédiaires, donc l'extension est simple. ■

**Définition 9.4** Soient $E$, $F$ deux sous-corps d'un corps $K$. Le compositum de $E$ et $F$ est le plus petit sous-corps de $K$ qui contient $E$ et $F$.

Théorème 9.3 *Soit $K$ et $E$ sous-corps de $F$ contenant $k$. Si $K/k$ est galoisienne alors $KE/E$ est galoisienne et $G(KE/E) \simeq G(K/K \cap E)$.*

*Démonstration.* On définit

$$\varphi : \begin{cases} G(KE/E) & \to & G(K/k) \\ \sigma & \mapsto & \sigma|_K \end{cases}$$

$\operatorname{Ker} \varphi = \{\mathrm{Id}\}$ car si $\sigma|_K = \mathrm{Id}$, on fixe $E$ et $K$ donc $KE$.

Montrons que $K^{\mathrm{Im}(\varphi)} = K \cap E$. On sait que $K \cap E \subset K^{\mathrm{Im}(\varphi)}$ (les $\sigma \in K^{\mathrm{Im}(\varphi)}$ fxent $E$).

$K^{\mathrm{Im}(\varphi)}E$ est dans le corps fixe $G(KE/E)$ donc $K^{\mathrm{Im}(\varphi)} \subset E$.

Donc $K^{\mathrm{Im}(\varphi)} = K \cap E$. ■

 

# Chapitre 10

# Applications

## 10.1 Généralités

**Lemme 10.0.1**
Soit $k$ un corps contenant $\xi$ une racine primitive $n^{\mathrm{e}}$ de l'unité et $K/k$ une extension galoisienne de degré fini tel que $G(K/k)$ cyclique $\langle\sigma\rangle$. Il existe $\alpha \in K$ tel que $\sigma(\alpha) = \alpha\xi$.

*Démonstration.* $\sigma : K \to K$ est $k$-linéaire. On en cherche un vecteur propre. Comme $\sigma^n - \mathrm{Id} = 0$, $X^n - 1$ s'annule sur $\sigma$. Si $f$ tel que $\deg(f) < n$ annule $\sigma$, on aurait une combinaison linéaire nulle de puissances $< n$ de $\sigma$. Par Dedekind, $f = 0$ ($n = [K : k]$ car extension galoisienne).

Donc $\xi$ est valeur propre et on a le résultat. ■

<u>THÉORÈME 10.1</u> *Si $k$ contient $\xi$, $K/k$ une extension galoisienne tel que $G(K/k)$ soit cyclique d'ordre $n$. Il existe $\alpha \in K$ tel que $\alpha^n = b \in k$.*

*Alors $K = k(\alpha)$ donc $K$ est un corps de décomposition de $X^n - b$ qui est irréductible.*

*Démonstration.* Par le lemme $G(K/k) = \langle\sigma\rangle$ avec $\sigma(\alpha) = \xi\alpha$. $\sigma^i \neq \mathrm{Id}$ donc $\sigma^i(\alpha) \neq \alpha$. $k(\alpha)$ est donc le corps fixe de $\{\mathrm{Id}\}$, ie $K$. Donc $K = k(\alpha)$.

$\alpha$ est zéro de $X^n - \alpha^n$ et appartient à $K$. Comme $\xi \in K$, $K$ est le corps de décomposition de $X^n - \alpha^n$. ■

**<u>Définition 10.1</u>** Un groupe fini $G$ est dit résoluble ss'il existe $G = G_0 \rhd \ldots \rhd G_n = \{e\}$ tel que $G_i/G_{i+1}$ soient abéliens.

<u>THÉORÈME 10.2</u> *Si le groupe est fini, la définition est équivalente à celle avec $G_i/G_{i+1}$ cyclique d'ordre premier.*

**Exemple 10.1** Dans $\mathfrak{S}_3$, on a $\mathfrak{A}_3$ qui est commutatif et distingué donc tout le monde est résoluble.

Dans $\mathfrak{S}_4$ c'est plus compliqué

$$\begin{tikzcd}
 & \mathfrak{S}_4 \arrow[dl, no head] \arrow[dr, no head] & \\
\mathfrak{A}_4 \arrow[d, no head] & & D_4 \arrow[d, no head] \\
V_4 \arrow[r, no head] \arrow[dr, no head] & \{1,(12)(34)\} \arrow[d, no head] & \langle(1234)\rangle \arrow[dl, no head] \\
 & \{1\} &
\end{tikzcd}$$

**Proposition 10.1** Soit $G$ un groupe, $H < G$ et $N \lhd G$.

- Si $G$ est résoluble alors $H$ l'est.
- $G$ est résoluble ssi $N$ et $G/N$ le sont.

**Proposition 10.2** Soit $k$ un corps de caractéristique 0. $f = X^n - a \in k[X]$ non nul. Soit $K$ le corps de décomposition de $f$ sur $k$.

Alors $G(K/k)$ est résoluble.

*Démonstration.* $K = k(\xi, \alpha)$. On a donc la chaîne :

$$G(K/k) \rhd G(K/k(\xi)) \rhd \{\mathrm{Id}\}$$

Or $G(K/k)/G(K/k(\xi))$ est abélien (proposition d'un des chapitres d'avant sur $k(\xi)/k$.

Il reste à montrer que $G(K/k(\xi))$ est abélien. $\mu_{\alpha,k(\xi)} \mid X^n - a = \prod_{i=0}^{n-1}(X - \xi^i\alpha)$. Les racines de $\mu_{\alpha,k(\xi)}$ sont donc de la forme $\xi^j\alpha$ donc $G(K/k(\xi))$ est constitué des $\alpha \to \xi^j\alpha$ donc c'est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ donc abélien. ∎

**<u>Définition 10.2</u>** On dit qu'un polynôme $f$ est résoluble par radicaux ssi un corps de décomposition $K$ est contenu dans un corps $L$ vérifiant

$$k \subset K_1 = k(\alpha_1) \subset \ldots \subset K_n = K_{n-1}(\alpha_n) = L$$

**Proposition 10.3** Dans la situation précédente, il existe $k \subset K'_0 \subset \ldots \subset K'_s$ avec $K_n \subset K'_s$, $K'_i/k$ galoisienne et $K'_i$ est corps de décomposition d'un $X^{m_i} - b_i \in K'_{i-1}[X]$.

 

*Démonstration.* Soit $\xi$ une racine primitive de l'unité dans $\overline{k}$. On pose $K_1 = k(\xi)$. Posons $f_1 = \prod_{\sigma\in G(K_1/k)} (X^{m_1} - \sigma(b_i))$ et $g_1 = (X^m - 1)f_1$.

Posons $K_2'$ le comps de décomposition de $g_1$. En réitérant la construction ça marche. ∎

<u>Théorème 10.3</u> *En caractéristique 0, $f \in k[X]$ est résoluble par radicaux ssi $G(K/k)$ l'est pour $K$ corps de décomposition de $f$.*

*Démonstration.* On montre uniquement ⇒.

On écrit la définition de $f$ résoluble par radicaux avec des $K_i'$. On considère les groupes de Galois associés $G_i = G(K_s'/K_i')/$

On a $G_s = \{\mathrm{Id}\}$ et $G_{i-1}/G_i = G(K_i/K_{i-1})$ donc résoluble donc les $G_i$ sont résolubles.

On a $k \subset K \subset K_s'$ donc $G(K/k) \simeq G(K_s'/k)/G(K_s'/K)$ est donc résoluble. ∎

Problème : si $G \subset \mathfrak{S}_n$, est-ce qu'il existe $g \in \mathbb{Q}[X]$ dont c'est le groupe de Galois ?

**Exemple 10.2** On considère $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$ irréductible par Eisenstein. En étudiant la fonction, on trouve 3 racines réelles et 2 racines complexes conjuguées.

Soit $K$ le corps de décomposition de $f$ sur $\mathbb{Q}$. La conjuguaison correspond à une permutation de $G(K/\mathbb{Q})$ et $5 \mid G(K/\mathbb{Q})$ (regarder les Sylow) donc $G(K/\mathbb{Q}) = \mathfrak{S}_5$ qui n'est pas résoluble. Donc pas de fomule pour les polynômes de degré 5.

## 10.2 Constructions à la règle et au compas

On part de $B_0 = \{0, 1\}$ et on pose $B_{i+1} = B_i \cup \{$ points constructibles à partir de $B_i\}$.

**Proposition 10.4** L'ensemble des points constructibles est un corps.

*Démonstration.* Thalès assure que si $a$ et $b$ sont constructibles, $a + b$, $ab$ et $\frac{a}{b}$ aussi. ∎

Considérer les intersections de droites et de cercles revient à considérer des extensions de degré 2. Un point est donc constructible ss'il appartient à une tour d'extensions de degré 2 de $\mathbb{Q}$.

 

### 10.2.1 Problèmes classiques

- Duplication du cube : Construire un cube de volume double à celui d'un cube construit, ie construire $\sqrt[3]{2}$.
- Trisection de l'angle : Couper un angle en trois parties égales, ce qui revient à construire des cos et sin.
- Quadrature du cercle : Construire un carré dont l'aire est celle d'un disque donné ie construire $\sqrt{\pi}$.

*Remarque 10.1* *Attention : si la règle est graduée, on peut trisecter l'angle !*

<u>THÉORÈME 10.4</u> *Le polygône régulier à $n$ côtés $P_n$ est constructible à la règle et au compas ssi $n = 2^k p_1 \dots p_s$ où $p_i = 2^{2^{k_i}} + 1$.*

 