

Mohamed Aqalmoun

Algèbre de base et applications

Module M

ENS-MEKNÈS

Avant-propos

Ce cahier-cours (version $\frac{1}{2}$ -cours) est destiné aux étudiants de première année du master mathématiques appliquées et ingénierie de l'enseignement de l'école normale supérieure de Meknès. Il propose un cours non complet (sans démonstrations) de l'algèbre de base.

Table des matières

1 Modules sur anneau principal	1
1.1 Anneaux et morphismes	1
1.2 Idéaux	3
1.3 Idéaux premiers et idéaux maximaux	6
1.4 Modules	7
1.5 Module sur un anneau principal	13
1.6 Exercices	14
2 Polynômes à plusieurs indéterminées	19
2.1 L'anneau $K[X_1, \dots, X_n]$	19
2.2 Ordres monômiaux	20
2.3 Division euclidienne dans $K[X_1, \dots, X_n]$	22
2.4 Idéaux monomiaux	23
2.5 Bases de Gröbner	24
2.6 Exercices	25
3 Extensions Galoisiennes	27
3.1 Extensions de corps	27
3.2 Extension algébrique	29
3.3 Corps de décomposition	31
3.4 Extensions normales	32

Chapitre 1

Modules sur anneau principal

1.1 Anneaux et morphismes

Définition 1.1.

Un anneau est un triplet $(A, +, \times)$ vérifiant :

- $(A, +)$ est un groupe abélien (de neutre 0).
- La multiplication $\times$ est associative c'est à dire pour tous $a, b, c \in A$, $a(bc) = (ab)c$.
- La multiplication $\times$ est distributive par rapport à l'addition $+$ c'est à dire; pour tous $a, b, c \in A$, $(a + b) \times c = a \times c + b \times c$ et $a \times (b + c) = a \times b + a \times c$.

L'anneau A est dit unitaire si $\times$ admet un élément neutre appelé unité et se note 1_A ou 1 .

L'anneau A est dit commutatif si la multiplication $\times$ est commutative.

Notation : Si $a, b \in A$, l'élément $a \times b$ sera noter ab .

Dans ce qui suit on ne considère que les anneaux commutatifs unitaires, ainsi par **anneau** on désigne un **anneau commutatif unitaire**.

Soit $(A_i)_{i \in I}$ une famille d'anneaux. On muni le produit cartésien $\prod_{i \in I} A_i$ des deux lois :

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I}, \quad (x_i)_{i \in I} (y_i)_{i \in I} = (x_i y_i)_{i \in I}$$

Alors $(\prod_{i \in I} A_i, +, \times)$ est un anneau (commutatif unitaire) dit anneau produit direct des anneaux A_i , $i \in I$.

Un anneau trivial est un anneau réduit à un singleton, dans ce cas $1 = 0$.

Un cas particulier : Si $A_1, \dots, A_m$ sont des anneaux commutatifs unitaires alors $\prod_{i=1}^m A_i = A_1 \times \dots \times A_m$ est un anneau commutatif.

Soit A un anneau et $a \in A$. On dit que a est inversible s'il existe $b \in A$ tel que $ab = 1$. Si c'est le cas l'élément b est unique et se note a^{-1} . L'ensemble des éléments inversibles de A se note $A^\times$ ou $U(A)$ appelé groupe des unités. On vérifie facilement que $A^\times$ est un groupe (muni de la multiplication).

Définition 1.2.

Un anneau A est dit intègre si

1. A non trivial ($1 \neq 0$),
2. Pour tous $x, y \in A$, $xy = 0 \implies x = 0$ ou $y = 0$.

Exemples :

1. $\mathbb{Z}$
2. $\mathbb{R}[X]$

Définition 1.3.

Un corps est un anneau A tel que

1. A non trivial ($1 \neq 0$),
2. $A^\times = A \setminus \{0\}$.

Remarque : Un corps est un anneau non trivial dans lequel tout élément non nul est inversible.

Si A est un corps alors il est intègre.

Exemples :

1. $\mathbb{R}$, $\mathbb{Q}$ et $\mathbb{C}$ sont des corps.
2. $\mathbb{R}(X)$ est un corps.

Définition 1.4.

Soit A un anneau et B une partie de A . On dit que B est un sous anneau de A si $(B, +)$ est un sous groupe de $(A, +)$, B stable par la multiplication et $1 \in B$.

CHAPITRE 1 : Modules sur anneau principal

Exemple : $\mathbb{Z}$ est un sous anneau de $\mathbb{R}$.

$\mathbb{Z}[X] := \{ \sum_{k=0}^n a_k X^k \mid n \in \mathbb{N}, a_k \in \mathbb{Z} \}$ est un sous anneau de $\mathbb{R}[X]$.

Définition 1.5.

Soit A, B deux anneaux et $f : A \rightarrow B$ une application. On dit que f est un morphisme d'anneaux si : pour tout $x, y \in A$, $f(x + y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ et $f(1) = 1$.

Si $f : A \rightarrow B$ est un morphisme d'anneaux alors $f(0) = 0$, $f(x - y) = f(x) - f(y)$ et si de plus x est un élément inversible de A alors $f(x)$ est aussi inversible dans B . Un morphisme d'anneaux $f : A \rightarrow B$ est un isomorphisme si de plus il est bijectif. Deux anneaux sont isomorphes, lorsqu'il existe un isomorphisme entre eux.

1.2 Idéaux

Définition 2.1.

Soit A un anneau et I une partie de A . On dit que I est un idéal de A si ;

1. I est un sous groupe de $(A, +)$,
2. $\forall a \in A, \forall x \in I, ax \in I$.

Remarque :

1. $\{0\}$ et A sont des idéaux de A .
2. Si I est un idéal de A contenant un élément inversible alors $I = A$.
3. Un anneau A (non trivial) est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A .

Proposition 2.2.

Soit A un anneau.

- Si I et J sont des idéaux de A alors $I + J := \{x + y \mid (x, y) \in I \times J\}$ est un idéal de A appelé la somme de I et J .
- Si $(I_\alpha)_{\alpha \in \Gamma}$ est une famille d'idéaux de A alors $\bigcap_{\alpha \in \Gamma} I_\alpha$ est un idéal de A , autrement dit une intersection quelconque d'idéaux de A

est un idéal de A .

Démonstration :

Soit S une partie de A . L'intersection de tous les idéaux de A contenant S est appelé l'idéal engendré par S et se note (S) . Ainsi

$$(S) = \bigcap_{I \text{ idéal} \supseteq S} I$$

Proposition 2.3.

Soit A un anneau et S une partie non vide de A .

- $(S) = \left\{ \sum_{i=1}^m a_i s_i \mid m \geq 1, a_i \in A, s_i \in S \right\}$
- $(\emptyset) = \{0\}$.

Démonstration :

Remarque : Si $S = \{s_1, \dots, s_n\}$, alors $(S) = \left\{ \sum_{i=1}^n a_i s_i \mid a_i \in A \right\}$ il se note aussi $(s_1, \dots, s_n)$.

Définition 2.4.

Soit A un anneau.

1. Soit I, J deux idéaux de A . Le produit de I et J noté IJ est l'idéal engendré par les éléments de la forme ab où $a \in I$ et $b \in J$.
2. Soit $(I_\alpha)_{\alpha \in \Gamma}$ une famille d'idéaux. La somme des idéaux I_α , $\alpha \in \Gamma$, est l'idéal engendré par $\bigcup_{\alpha \in \Gamma} I_\alpha$ on le note $\sum_{\alpha \in \Gamma} I_\alpha$

Les éléments de IJ sont de la forme $\sum_{k=1}^m a_k b_k$ où les $a_k \in I$ et les $b_k \in J$.

Les éléments de $\sum_{\alpha \in \Gamma} I_\alpha$ sont de la forme $\sum_{\alpha \in \Gamma} a_\alpha$ où $a_\alpha \in I_\alpha$ sont tous nuls sauf peut être un nombre fini d'entre eux.

On définit d'une manière analogue le produit d'un nombre fini d'idéaux $I_1, \dots, I_m$, comme étant l'idéal engendré par les éléments de la forme $a_1 \cdots a_m$ où $a_k \in I_k$.

Définition 2.5.

Soit A un anneau et I un idéal de A .

1. On dit que I est un idéal principal s'il est engendré par un élément, c'est à dire $I = (a)$, où $a \in A$.
2. On dit que I est un idéal de type fini s'il est engendré par un ensemble fini c'est à dire $I = (a_1, \dots, a_n)$ où $a_1, \dots, a_n \in A$.

Exemples :

1. Dans l'anneau $\mathbb{Z}[X]$, l'idéal $I = \{P \in \mathbb{Z}[X] / P(0) = 0\}$ est principal. En effet $I = (X)$.
2. Si I et J sont des idéaux de type fini alors IJ et $I + J$ sont de type fini.

Définition 2.6.

Un anneau est dit principal¹ s'il est intègre et tous ses idéaux sont principaux.

Soit I un idéal de A . Le groupe quotient A/I hérite d'une multiplication définie de manière unique de A qui en fait un anneau commutatif unitaire ($\bar{x} \bar{y} = \overline{xy}$). De plus l'application $\pi : A \rightarrow A/I$ définie par $\pi(x) = \bar{x}$ est un morphisme d'anneaux (surjectif).

Proposition 2.7.

Soit A un anneau et I un idéal de A . Le morphisme $\pi : A \rightarrow A/I$ induit une bijection entre les idéaux de A/I et les idéaux de A contenant I .

Démonstration :

Proposition 2.8.

Soit $f : A \rightarrow B$ un morphisme d'anneaux.

1. Si J est un idéal de B alors $f^{-1}(J)$ est un idéal de A . En particulier $\ker f$ est un idéal de A .
2. $\text{Im } f$ est un sous anneau de B .

1. Il est dit quasi-principal si tous ses idéaux sont principaux (sans condition intègre).

Démonstration :

Théorème 2.9. (théorème d'isomorphisme)

Soit $f : A \rightarrow B$ un morphisme d'anneaux. L'application

$$\bar{f} : A/\ker f \rightarrow \operatorname{Im} f, \quad \bar{f}(\bar{x}) = f(x)$$

est (bien définie et c'est) un isomorphisme

Démonstration :

1.3 Idéaux premiers et idéaux maximaux

Définition 3.1.

Soit A un anneau.

1. Un idéal P de A est dit premier si $P \neq A$ et $\forall x, y \in A, xy \in P \Rightarrow x \in P$ ou $y \in P$.
2. Un idéal M de A est dit maximal s'il n'existe pas d'idéal I de A tel que $M \subset I \subset A$ (inclusions strictes).

L'ensemble des idéaux premiers de A s'appelle le spectre premier de A et se note $\operatorname{Spec}(A)$ et celui des idéaux maximaux de A s'appelle le spectre maximal de A et se note $\operatorname{MaxSpec}(A)$ ou $\operatorname{Max}(A)$.

Définition 3.2.

Soit A un anneau.

1. Un idéal P est premier si et seulement si A/P est intègre.
2. Un idéal M est maximal si et seulement si A/M est un corps.

Démonstration :

Proposition 3.3.

1. Tout idéal maximal est premier.
2. Soit $f : A \rightarrow B$ un morphisme d'anneaux. Si P est un idéal pre-

mier de B alors $f^{-1}(P)$ est un idéal premier de A .

Démonstration :

Théorème 3.4. (de Krull)

Soit A un anneau non trivial c'est à dire $A \neq 0$, alors $\text{Max}(A) \neq \emptyset$. Autrement dit A contient au moins un idéal maximal.

Démonstration :

Corollaire 3.5.

Soit A un anneau.

1. Tout idéal propre (i.e $\neq A$) de A est contenu dans un idéal maximal.
2. Si $a \in A$ est non inversible alors a appartient à un idéal maximal.

Démonstration :

Remarque : Une conséquence immédiate du Corollaire précédent est que

$$A^\times = A \setminus \left(\bigcup_{M \in \text{Max}(A)} M \right)$$

1.4 Modules

Définition 4.1.

Soit A un anneau commutatif. Un A -module ou module sur A est un triplet $(M, +, \cdot)$ tel que;

1. $(M, +)$ est un groupe abélien.
2. $\cdot : A \times M \rightarrow M, (a, m) \mapsto a.m$ est une loi externe sur M de base A vérifiant les propriétés suivantes; pour tous $a, b \in A, m, m' \in M$,
 - $a.(m + m') = a.m + a.m'$
 - $(a + b).m = a.m + b.m$

- $(ab).m = a.(b.m)$
- $1.m = m$

Remarque : Les modules peuvent être vus comme une généralisation des espaces vectoriels. En effet un $\mathbb{K}$ -module sur un corps commutatif $\mathbb{K}$ est tout simplement un $\mathbb{K}$ -espace vectoriel.

Exemples :

1. Soit G un groupe abélien. Alors G est naturellement un $\mathbb{Z}$ -module où la multiplication externe “.” est définie par $\mathbb{Z} \times G \rightarrow G, (n, g) \mapsto ng$.
2. Si I est un idéal de A alors I est naturellement un A -module.
3. Si I est un idéal de A alors A/I est un A -module.

Définition 4.2.

Soient M et N deux A -modules et $f : M \rightarrow N$ une application. On dit que f est un morphisme de A -modules si, pour tous $a \in A, m, m' \in M$;

1. $f(m + m') = f(m) + f(m')$.
2. $f(am) = af(m)$.

Exemples :

1. Soit I un idéal de A . L'application $s : A \rightarrow A/I, x \mapsto s(x) = \bar{x}$ est un morphisme de A -modules.
2. Un morphisme de groupes abéliens est un morphisme de $\mathbb{Z}$ -modules.

Le composé de deux morphismes de A -modules est un morphisme de A -modules. L'ensemble de tous les morphismes de A -modules de M dans N est un A -module, où pour f, g deux morphismes de A -modules et $a \in A, (f + g)(x) = f(x) + g(x)$ et $(af)(x) = af(x)$. On note $\text{Hom}_A(M, N)$ ou simplement $\text{Hom}(M, N)$ le A -module des morphismes de A -modules de M dans N .

Définition 4.3. (A -algèbre)

Soit A un anneau. Une A -algèbre est un quadruplet $(B, +, \times, .)$ tels que ;

1. $(B, +, \times)$ est un anneau,

2. $(B, +, \cdot)$ est un A -module,
3. $a(xy) = (ax)y = x(ay), \forall a \in A, x, y \in B$.

Exemples : Soit A un anneau.

1. A est naturellement une $\mathbb{Z}$ -algèbre.
2. $A[X]$ est une A -algèbre.
3. Soit $f : A \rightarrow B$ un morphisme d'anneaux. Alors B est un A -module ($a.b := f(a)b$), plus précisément c'est une A -algèbre.

Définition 4.4.

Soit M un A -module et N une partie de M . On dit que N est un sous module de M si;

1. N est un sous groupe de M ,
2. $\forall a \in A, \forall n \in N, an \in N$.

Remarque : Si N est un sous module de M , alors N lui même est un A -module.

Exemples :

1. Si I est un idéal de A , alors I est un sous module de A .
2. Soit $f : M \rightarrow N$ un morphisme de A -modules. Alors $\ker f$ est un sous module de M et $\operatorname{Im} f$ est un sous module de N .
3. Si $x \in M$, alors $\{ax \mid a \in A\}$ est un sous module de M et il se note Ax .

Proposition 4.5.

Soit M un A -module.

1. Si $(N_i)_{i \in I}$ est une famille de sous modules de M , alors $\bigcap_{i \in I} N_i$ est un sous module de M .
2. Si N et N' sont des sous modules de M , alors $N + N'$ est un sous module de M , où $N + N' = \{x + y \mid x \in N, y \in N'\}$.

Démonstration :

Soit M un A -module et N un sous module de M . Alors M/N est un groupe abélien où l'addition est définie par ;

$$\overline{x} + \overline{y} = \overline{x+y}, \quad x, y \in M$$

C'est aussi un A -module muni de la multiplication externe suivante ;

$$a\overline{x} = \overline{ax}, \quad a \in A, x \in M.$$

de plus l'application $s : M \rightarrow M/N$ définie par $s(x) = \overline{x}$ est un morphisme de A -modules surjectif.

Théorème 4.6. (Théorème d'isomorphisme)

Soit $f : M \rightarrow M'$ un morphisme de A -modules. Alors f induit un isomorphisme $\overline{f} : M/N \rightarrow \text{Im } f$ où $\overline{f}(\overline{x}) = f(x)$.

Démonstration :

Sous module engendré par une famille :

Définition 4.7.

Soit M un A -module et $(x_i)_{i \in I}$ une famille d'éléments de M . Le sous module engendré par la famille $(x_i)_{i \in I}$ est l'intersection de tous les sous modules de M contenant les éléments de la famille $(x_i)_{i \in I}$, il se note $\langle x_i, i \in I \rangle$. C'est le plus petit (au sens de l'inclusion) sous module de M contenant les éléments de la famille $(x_i)_{i \in I}$.

Proposition 4.8.

Soit M un A -module et $(x_i)_{i \in I}$ une famille d'éléments de M . Alors

$$\langle x_i, i \in I \rangle = \left\{ \sum_{j \in J} a_j x_j \mid J \text{ partie finie de } I, a_j \in A \right\}$$

Démonstration : ... On pose $N' = \left\{ \sum_{j \in J} a_j x_j \mid J \text{ partie finie de } I, a_j \in A \right\}$. Il suffit de démontrer que N' est le plus petit (au sens de l'inclusion) sous module de M contenant les $x_i, i \in I$. Il est clair que $0 \in N'$. Soient $x, y \in N'$ et $a \in A$. Par définition $x = \sum_{j \in J} a_j x_j$ et $y = \sum_{j \in J'} b_j x_j$ où $a_j, b_j \in A, J$ et J' sont des parties finies de I .

CHAPITRE 1 : Modules sur anneau principal

On a $x + ay = \sum_{j \in J} a_j x_j + \sum_{j \in J} aa_j x_j = \sum_{j \in J \cup J'} a'_j x_j$ où

$$a'_j = \begin{cases} a_j & \text{si } j \in J - J' \\ a_j + ba'_j & \text{si } j \in J \cap J' \\ aa'_j & \text{si } j \in J' - J \end{cases}$$

Ainsi $x + ay \in N'$. Il est clair que N' contient les x_i ; en effet $x_i = \sum_{j \in \{i\}} 1 \cdot x_j \in N'$.

Soit maintenant N un sous module de M contenant les x_i . Si $x \in N'$, alors $x = \sum_{j \in J} a_j x_j$ où J est une partie finie de I , puisque x est une combinaison d'éléments de N , c'est bien que $x \in N$. Ainsi $N' \subseteq N$. On en déduit que $(x_i; i \in I) = N'$.

Exemples : Soit M un A -module.

1. Soit $x \in M$. Le sous module engendré par x est le sous module Ax .
2. Si $x_1, \dots, x_n \in M$, alors $(x_1, \dots, x_n) = \{a_1 x_1 + \dots + a_n x_n \mid a_i \in A, \text{ pour } 1 \leq i \leq n\}$.
3. Soit I un idéal de A et N un sous module de M . Si on note IN le sous module de M engendré par tous les éléments de la forme ax où $a \in I$ et $x \in N$, alors

$$IN = \left\{ \sum_{i=1}^n a_i x_i \mid n \in \mathbb{N}^*, a_i \in I, x_i \in N \right\}$$

Remarque : Notons que si $(N_i)_{i \in I}$ est une famille de sous modules d'un A -module M , alors $\cup_{i \in I} N_i$ n'est pas (en général) un sous module de M .

Définition 4.9.

Soit M un A -module et $(N_i)_{i \in I}$ une famille de sous modules de M . La somme des sous modules $N_i, i \in I$ est le sous module engendré par tous les éléments de $\cup_{i \in I} N_i$, il se note $\sum_{i \in I} N_i$. Ainsi

$$\sum_{i \in I} N_i = (\cup_{i \in I} N_i)$$

Proposition 4.10.

Soit M un A -module et $(N_i)_{i \in I}$ une famille de sous modules de M .
Alors

$$\sum_{i \in I} N_i = \left\{ \sum_{j \in J} x_j \mid J \text{ partie finie de } I, x_j \in N_j \right\}$$

Démonstration : On posons $N' = \{ \sum_{j \in J} x_j \mid J \text{ partie finie de } I, x_j \in N_j \}$, puis par un raisonnement analogue à celui de la démonstration de la proposition 1.4, on montre que N' est le plus petit sous module de M contenant $\cup_{i \in I} N_i$.

Remarques : Soit M un A -module.

1. Si $N_1, \dots, N_n$ sont des sous modules de M , alors

$$\sum_{i=1}^n N_i = \left\{ \sum_{i=1}^n x_i \mid \text{pour } 1 \leq i \leq n, x_i \in N_i \right\}$$

2. Si $(x_i)_{i \in I}$ est une famille d'éléments de M , alors $\sum_{i \in I} Ax_i$ est le sous module engendré par la famille $(x_i)_{i \in I}$, autrement dit

$$\sum_{i \in I} Ax_i = (x_i, i \in I)$$

Définition 4.11.

Soit M un A -module. On dit que M est de type fini s'il existe $m_1, \dots, m_r \in M$ tels que $M = (m_1, \dots, m_r)$, autrement dit M est engendré par un nombre fini d'éléments.

Exemples :

1. Le $\mathbb{Z}$ -module $\mathbb{Z}^2$ est de type fini.
2. Le A -module A^n est de type fini.

Définition 4.12.

Soit M un A -module et $(m_1, \dots, m_r)$ une famille d'éléments de M . On

dit que $(m_1, \dots, m_r)$ est libre si pour tout $(\alpha_1, \dots, \alpha_r) \in A^r$, $\sum_{k=1}^r \alpha_k m_k = 0 \implies \alpha_1 = \dots = \alpha_r = 0$.

Une base de M est une famille qui est à la fois libre et génératrice M .

Un module M est dit libre s'il admet une base.

Le rang d'un module libre est le nombre d'éléments d'une base.

Exemple : Si A est un anneau, le A -module A^n est libre.

Théorème 4.13.

Soit A un anneau et M un A -module libre de rang r . Alors M est isomorphe à A^r .

Proposition 4.14.

Soit M un A -module. Alors M est de type fini si et seulement si il existe $n \in \mathbb{N}^*$ tel que M est isomorphe à un quotient de A^n .

Démonstration :

1.5 Module sur un anneau principal

Théorème 5.1.

Soit A un anneau principal et M un A -module libre de rang n fini. Alors tout sous module de M est libre de rang inférieur ou égale n .

Démonstration :

Théorème 5.2. (de la base adaptée)

Soit A un anneau principal et M un A -module libre de rang fini n . Soit N un sous module de M . Alors il existe $r \leq n$ et des éléments $d_1, \dots, d_r$ non nuls de A tels que $d_1 | d_2 | \dots | d_r$ et une base $(e_1, \dots, e_n)$ de M telle

que $(d_1 e_1, \dots, d_r e_r)$ soit une base de N .

Théorème 5.3. (structure des modules de type fini)

Soit A un anneau principal et M un A de type fini. Alors il existe des éléments $d_1, \dots, d_r \in A$ tels que :

1. $d_1 / d_2 / \dots / d_r$,
2. M est isomorphe à $A/(d_1) \times \dots \times A/(d_r)$.

Démonstration :

Groupe de type fini :

Un groupe abélien $(G, +)$ est de type s'il existent $(g_1, \dots, g_r \in G)$ tels que $G = \langle g_1, \dots, g_r \rangle$, autrement G est un $\mathbb{Z}$ -module de type fini. Il est dit libre de rang fini s'il possède une base fini (entant que $\mathbb{Z}$ -module).

1. Un groupe libre de rang n est isomorphe à
2. Un sous groupe d'un groupe libre de rang fini est
3. Soit G un groupe de type fini, alors ils existent des entiers

1.6 Exercices

Exercice 1.1

Soit A un anneau. Pour I idéal de A le radical de I est défini par;

$$\sqrt{I} := \{a \in A / \exists n \in \mathbb{N} \text{ tel que } a^n = 0\}$$

1. Montrer que $\sqrt{I}$ est un idéal de A .
2. Montrer que si $I \subseteq J$, alors $\sqrt{I} \subseteq \sqrt{J}$.
3. Dans l'anneau $\mathbb{Z}$, montrer que $\sqrt{(72)} = (6)$.

Exercice 1.2

Soient A un anneau et I, J deux idéaux de A tel que $I + J = A$.

1. Montre que $I \cap J = IJ$.

2. Soit $f : A \rightarrow A/I \times A/J$ l'application définie par $f(x) = (\bar{x}, \bar{x})$.
- (a) Montrer que f est un morphisme d'anneaux.
 - (b) Montrer que f est surjectif.
 - (c) En déduire que A/IJ est isomorphe à $A/I \times A/J$.

Exercice 1.3

Soit A un anneau, I, J deux idéaux de A et P un idéal premier de A .

- 1. Montrer que si $IJ \subseteq P$, alors $I \subseteq P$ ou $J \subseteq P$.
- 2. Montrer que si $I \cap J \subseteq P$, alors $I \subseteq P$ ou $J \subseteq P$.

Exercice 1.4

Soit A un anneau principal.

- 1. Soit $P = (a)$ un idéal premier non nul. Montrer que a est premier.
- 2. Montrer que tout idéal premier non nul de A est maximal.

Exercice 1.5

- 1. Montrer que (X) et $(X^2 + 1)$ sont des idéaux maximaux de $\mathbb{R}[X]$.
- 2. Quels sont les idéaux premiers de $\mathbb{R}[X]/(X^3(X^2 + 1))$.

Exercice 1.6

Soit A un anneau.

- 1. On suppose A intègre et que A possède un nombre fini d'idéaux. Montrer que A est un corps.
- 2. On suppose que A possède un nombre fini d'idéaux. Montrer que tout idéal premier de A est maximal.

Exercice 1.7

Soient M un A -module et $x \in M$; on dit que x est un élément de torsion dans M s'il existe $a \in A \setminus \{0\}$ tel que $ax = 0$. On note M_{tors} l'ensemble des éléments de torsion du module M . Un module M est dit sans torsion si $M_{\text{tors}} = \{0\}$; il est dit de torsion si $M_{\text{tors}} = M$.

1. Quels sont les éléments de torsion du A -module A ?
On suppose pour le reste de l'exercice que A est un anneau intègre.
2. Montrer que M_{tors} est un sous-module de M . Est-ce encore vrai si A n'est plus supposé intègre ?.
3. Montrer que M/M_{tors} est un A -module sans torsion.
4. Soient N et P deux sous-modules de M tels que $M = N \oplus P$. Montrer que $M_{\text{tors}} = N_{\text{tors}} \oplus P_{\text{tors}}$.

Exercice 1.8

Soit A un anneau principal, et $(a_1, a_2, a_3) \in A^3$ tels que $\text{pgcd}(a_1, a_2, a_3) = 1$. On cherche à décrire

$$E = \{(x_1, x_2, x_3) \in A^3 / \sum_{i=1}^3 a_i x_i = 0\}$$

Pour i, j, k distincts, on note $d_k = \text{pgcd}(a_i, a_j)$.

1. Montrer que E libre.
2. Montrer que si i, j, k sont distincts $d_i d_j | a_k$.
Soit $b_k \in A$ tel que $a_k = d_i d_j b_k$.
3. Montrer que les b_i sont premiers deux à deux.
4. Soit $F = \{(y_1, y_2, y_3) \in A^3 / \sum_{i=1}^3 b_i y_i = 0\}$. Montrer que l'application $\varphi : F \rightarrow E$ définie par $\varphi(y_1, y_2, y_3) = (d_1 y_1, d_2 y_2, d_3 y_3)$ est un isomorphisme de A -modules.

Exercice 1.9

Soit A un anneau principal et $f : A^n \rightarrow A^m$ un morphisme de modules. Montrer que $\ker f$ admet un supplémentaire dans A^n .

Exercice 1.10

Soit $N = \{(x, y, z) \in \mathbb{Z}^3 \mid 2 \text{ divise } x + y + z\}$

1. Montrer que N est un sous module libre de $\mathbb{Z}^3$.
2. Justifier que $(2, 0, 0), (0, 2, 0), (0, 0, 2) \in N$.
3. En déduire que N est libre de rang 3.
4. Montrer que $((1, -1, 0), (1, 0, -1), (2, 0, 0))$ est une base de N .

Exercice 1.11

Soit A un anneau principal et L un A -module libre de rang fini. Soit M un sous A -module de L . Montrer que M possède un supplémentaire dans L si et seulement si L/M est sans torsion.

Chapitre 2

Polynômes à plusieurs indéterminées

2.1 L'anneau $K[X_1, \dots, X_n]$

Soit A un anneau commutatif unitaire. On note $A[X]$ l'anneau des polynômes à une indéterminée et coefficient dans A , ainsi

$$A[X] = \left\{ \sum_{k=0}^n a_k X^k \mid n \in \mathbb{N}, a_k \in A \right\}$$

C'est un anneau commutatif unitaire.

Remarque : Si l'anneau A est intègre alors $A[X]$ est intègre.

Définissons l'anneau $A[X_1, \dots, X_n]$ des polynômes à coefficients dans A en n indéterminées, par récurrence sur $n \geq 1$:

- Pour $n = 1$ c'est l'anneau $A[X_1]$;
- Pour $n \geq 2$, $A[X_1, \dots, X_n]$ est l'anneau $A[X_1, \dots, X_{n-1}][X_n]$.

Remarque : Si A est intègre alors $A[X_1, \dots, X_n]$ est intègre, en particulier si K est un corps alors l'anneau $K[X_1, \dots, X_n]$ est intègre.

Exemple : $K[X, Y] = K[X][Y]$, chaque élément de $K[X, Y]$ s'écrit sous la forme

Plus généralement un élément de $K[X_1, \dots, X_n]$ s'écrit sous la forme

$$P = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}$$

où tous les éléments $a_{i_1, \dots, i_n} \in K$ sont nuls sauf un nombre fini d'entre eux.

Définition 1.1.

On appelle monôme de $K[X_1, \dots, X_n]$ tout polynôme de la forme $aX_1^{i_1} \dots X_n^{i_n}$ où $a \in K$ et $i_1, \dots, i_n \in \mathbb{N}$.

Pour $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, on note X^α le monôme $X_1^{\alpha_1} \dots X_n^{\alpha_n}$. Avec cette notation, chaque élément de $K[X_1, \dots, X_n]$ s'écrit sous la forme (d'une somme finie);

$$P = \sum_{\alpha \in A} a_\alpha X^\alpha$$

où A est une partie finie de $\mathbb{N}^n$.

2.2 Ordres monômiaux

Définition 2.1.

Un ordre monomial sur $K[X_1, \dots, X_n]$ est une relation $>$ d'ordre sur $\mathbb{N}^n$ satisfaisant les conditions suivantes;

1. $>$ est un ordre total sur $\mathbb{N}^n$,
2. $>$ est un bon ordre sur $\mathbb{N}$, c'est-à-dire toute partie non vide de $\mathbb{N}^n$ admet un plus petit élément.
3. Si $\alpha > \beta$ et $\gamma \in \mathbb{N}$, alors $\alpha + \gamma > \beta + \gamma$. (compatibilité avec l'addition).

Nous allons définir trois exemples fondamentaux d'ordres monomiaux sur $K[x_1, \dots, x_n]$;

Définition 2.2. (ordre lexicographique)

On définit la relation d'ordre lexicographique $>_{\text{lex}}$ sur $\mathbb{N}^n$ elle que pour $\alpha, \beta \in \mathbb{N}^n$, $\alpha >_{\text{lex}} \beta$ si $\alpha \neq \beta$ et la composante non nulle la plus à gauche de $\alpha - \beta$ est (strictement) positive.

CHAPITRE 2 : Polynômes à plusieurs indéterminées

Soient $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$, alors

Exemples :

Notation : Pour $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, on pose $|\alpha| = \alpha_1 + \dots + \alpha_n$.

Définition 2.3. (ordre lexicographique gradué)

Soient $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$. L'ordre lexicographique gradué est la relation $>_{\text{glex}}$ définie par $|\alpha| > |\beta|$ ou si $|\alpha| = |\beta|$ et $\alpha >_{\text{lex}} \beta$

Définition 2.4. (ordre lexicographique gradué renversé)

Soient $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$. L'ordre lexicographique gradué renversé est la relation $>_{\text{grevlex}}$ définie par $|\alpha| > |\beta|$ ou si $|\alpha| = |\beta|$ et $(\alpha_n, \dots, \alpha_1) >_{\text{lex}} (\beta_n, \dots, \beta_1)$

Remarque : Les ordres précédents sont monomiaux c'est-à-dire

Exemple : Soit $P = 3X^2Y + 4XYZ - 2X^2 + 7YZ^2 - 3Z^2 + X^4 \in K[X, Y, Z]$,
Ordonnons ses monômes selon les trois ordres monomiaux vus précédemment :

1.
2.
3.

Définition 2.5. (multidegré)

On fixe un ordre monomial $>$. Soit $P = \sum_{\alpha} a_{\alpha} X^{\alpha} \in K[X_1, \dots, X_n]$ un polynôme non nul. Le multidegré de P noté $\text{multideg}(P)$ est le n -uplet défini par;

$$\text{multideg}(P) = \max\{\alpha / a_{\alpha} \neq 0\}$$

On appelle alors coefficient dominant de P le scalaire $CD(P) = a_{\text{multideg}(P)}$, le monôme dominant de P le monôme unitaire $MD(P) = X^{\text{multideg}(P)}$, et enfin le terme dominant est le monôme $TD(P) = CD(P)MD(P)$.

Exemple : Reprenons le polynôme P de l'exemple précédent. Le multidegré de P dépend de l'ordre monomial choisi, par exemple :

1.
2.
3.

Ce multidegré a de bonnes propriétés de calcul analogues à celles du degré.

Proposition 2.6.

Soient P et Q des polynômes non nuls de $K[x_1, \dots, x_n]$. Alors

1. $\text{multideg}(PQ) = \text{multideg}(P) + \text{multideg}(Q)$.
2. Si $P + Q \neq 0$, alors $\text{multideg}(P + Q) \leq \max(\text{multideg}(P), \text{multideg}(Q))$.
3. Si $\text{multideg}(P) \neq \text{multideg}(Q)$, alors $\text{multideg}(P + Q) = \max(\text{multideg}(P), \text{multideg}(Q))$.
4. Si $TD(P) + TD(Q) = 0$, alors $\text{multideg}(P + Q) < \max(\text{multideg}(P) + \text{multideg}(Q))$.

2.3 Division euclidienne dans $K[X_1, \dots, X_n]$

Théorème 3.1. (Division dans $K[X_1, \dots, X_n]$)

On fixe un ordre monomial $>$. Soit $F = (P_1, \dots, P_m)$ un m -uplet de polynômes de $K[X_1, \dots, X_n]$ et $A \in K[X_1, \dots, X_n]$. Alors il existe $Q_1, \dots, Q_m, R \in K[X_1, \dots, X_n]$ tels que

$$A = Q_1 P_1 + \dots + Q_m P_m + R$$

et $R = 0$ ou R est une combinaison K -linéaire des monômes divisibles par aucun des $TD(P_i)$, $1 \leq i \leq m$.

On appelle alors R un reste de la division de A par F dans $K[X_1, \dots, X_n]$. De plus, si $1 \leq i \leq s$ et $Q_i P_i \neq 0$, alors on a $\text{multideg}(A) \geq \text{multideg}(Q_i P_i)$.

Exemple : Dans $\mathbb{R}[X, Y]$, $A = X^2 Y + 2XY - Y^2 + X + 1$, $P_1 = XY + Y$ et $P_2 = Y + 1$

2.4 Idéaux monomiaux

Définition 4.1.

On dit qu'un idéal I de $K[X_1, \dots, X_n]$ est monomial s'il existe $A \subseteq \mathbb{N}^n$ tel que $I = (X^\alpha, \alpha \in A)$.

Exemple : L'idéal (XY^2, XYZ^3, Y^3) est un idéal monomial de $K[X, Y, Z]$.

Proposition 4.2.

Soit $A \subseteq \mathbb{N}^n$ et $I = (X^\alpha, \alpha \in A)$ un idéal monomial. Soit $\beta \in \mathbb{N}^n$, alors

$$X^\beta \in I \Leftrightarrow \exists \alpha \in A, X^\alpha \text{ divise } X^\beta$$

Démonstration :
Le résultat précédent permet de montrer une condition nécessaire et suffisante d'appartenance d'un polynôme à un idéal monomial :

Proposition 4.3.

Soit I un idéal monomial de $K[X_1, \dots, X_n]$ et $P \in K[X_1, \dots, X_n]$. On a équivalence entre;

1. $P \in I$,
2. Chaque terme de P appartient à I ,
3. P est combinaison K -linéaire de monômes de I .

Démonstration :

Théorème 4.4. (le lemme de Dickson)

Soit $A \subseteq \mathbb{N}^n$ et $I = (X^\alpha, \alpha \in A)$ un idéal monomial de $K[X_1, \dots, X_n]$. Alors il existe $r \in \mathbb{N}^*$ et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^n$ tels que

$$I = (X^{\alpha_1}, \dots, X^{\alpha_r})$$

En particulier tout idéal monomial de $K[X_1, \dots, X_n]$ est de type fini.

Démonstration :

2.5 Bases de Gröbner

Définition 5.1.

Soit I un idéal non nul de $K[X_1, \dots, X_n]$. On note

$$TD(I) = \{TD(P) / P \in I \setminus \{0\}\}$$

Proposition 5.2.

Soit I un idéal non nul de $K[X_1, \dots, X_n]$.

1. $(TD(I))$ est un idéal monomial de $K[X_1, \dots, X_n]$.
2. Il existe $m \in \mathbb{N}^*$ et $P_1, \dots, P_m \in I$ tels que $(TD(I)) = (TD(P_1), \dots, TD(P_m))$.

Démonstration :

Théorème 5.3. (théorème de base d'Hilbert)

Tout idéal de $K[X_1, \dots, X_n]$ est de type fini.

Démonstration :

Définition 5.4. (Bases de Gröbner)

Soit I un idéal de $K[X_1, \dots, X_n]$ et $G = \{P_1, \dots, P_m\}$ une partie de I . On dit que G est une base de Gröbner de I si

$$(TD(I)) = (TD(P_1), \dots, TD(P_m))$$

Proposition 5.5.

Tout idéal non nul de $K[X_1, \dots, X_n]$ admet une base de Gröbner, et toute base de Gröbner d'un idéal non nul de $K[X_1, \dots, X_n]$ en est une partie génératrice.

Démonstration :

Proposition 5.6.

Soit I un idéal non nul de $K[X_1, \dots, X_n]$ et $G = \{P_1, \dots, P_m\}$ une base de Gröbner de I . Si $P \in K[X_1, \dots, X_n]$, alors il existe un unique couple (Q, R) d'éléments de $K[X_1, \dots, X_n]$ tels que

1. $P = Q + R$.
2. $Q \in I$,
3. R est une combinaison K -linéaire de monômes divisibles par aucun des $TD(P_i)$ pour $1 \leq i \leq m$.

R est appelé reste de la division euclidienne de P par G . Étant unique, il ne dépend pas de l'ordre dans lequel on considère les éléments de G . On notera $P \equiv R \text{ modulo } G$, et $\overline{P}^G = R$

Démonstration :

2.6 Exercices

Exercice 2.1

Soit $I = (X_1, \dots, X_n)$. Montrer que I est un idéal maximal de $K[X_1, \dots, X_n]$.

Exercice 2.2

Soit $>$ un ordre monomial sur $\mathbb{N}^{n+1}$.

1. Montrer que $>$ induit un ordre monomial sur $\mathbb{N}^n$.
2. Soient $(\alpha, k), (\beta, l) \in \mathbb{N}^{n+1}$. Montrer que si $(\alpha, k) < (\beta, l)$ alors $\alpha < \beta$ ou $k < l$.

Exercice 2.3

Soit $P = X^7 Y^2 + X^3 Y^2 - Y + 1$, $P_1 = XY^2 - X$ et $P_2 = X - Y^3$.

1. Calculer le reste de la division de P par P_1, P_2 en utilisant l'ordre lexicographique et l'ordre lexicographique gradué.
2. Même question avec les diviseurs dans l'ordre P_2, P_1 .

Exercice 2.4

Soit $P_1 = X^2 + Y$, $P_2 = XY + X$ et $I = (P_1, P_2)$ l'idéal engendré par P_1 et P_2 dans $K[X, Y]$.

1. Effectuer la division euclidienne de $F = X^3 - XY^2 + X^2 - Y^2$ par (P_1, P_2) .
2. Le polynôme F est-il dans I ?

Exercice 2.5

On considère l'idéal $I = (X_3 - X_1^5, X_2 - X_1^3)$ de $K[X_1, X_2, X_3]$.

1. Déterminer une base de Grobner de I pour l'ordre lexicographique.
2. Déterminer une base de Grobner de I pour l'ordre lexicographique gradué inversé.

Exercice 2.6

Soit $(I_m)_m$ une suite croissante d'idéaux de $K[X_1, \dots, X_n]$.

1. Montrer que $I := \cup_{m \in \mathbb{N}} I_m$ est un idéal de $K[X_1, \dots, X_n]$.
2. En déduire qu'il existe $N \in \mathbb{N}$, tel que pour tout $n \geq N$, $I_n = I_N$.

Chapitre 3

Extensions Galoisiennes

3.1 Extensions de corps

Rappelons qu'un corps K est par définition un anneau commutatif non nul dans lequel tout élément non nul est inversible.

Soit K un corps, l'application $f : \mathbb{Z} \rightarrow K, n \mapsto f(n) = n1_K$ est un morphisme d'anneaux, son noyau est un idéal de $\mathbb{Z}$, il existe alors $n \in \mathbb{N}$ tel que $\ker f = n\mathbb{Z}$. L'entier n s'appelle la caractéristique de K .

Remarque : Soit K un corps de caractéristique n , alors ;

1. $n = 0$ ou n est un nombre premier,
2. Pour tout $x \in K, nx = 0$.

Exemples :

1. $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des corps de caractéristique nulle.
2. Si p est un nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p .

On rappelle qu'un morphisme de corps est un morphisme d'anneaux (unitaires).

Proposition 1.1.

Soit K, K' deux corps et $f : K \rightarrow K'$ un morphisme de corps. Alors le morphisme f est injectif.

Démonstration :

Soit L un corps et K une partie de L . On rappelle que K est un sous corps de L si K est un sous anneau de L et pour tout $x \in K^*, x^{-1} \in K$.

Définition 1.2.

Soit K un corps. Une extension de K est un corps L tel que K soit un sous-corps de L (et on note L/K). Une extension intermédiaire entre L et K est un corps F tel que $K \subseteq F \subseteq L$.

Exemples :

Définition 1.3.

Si $f : K \rightarrow L$ est un morphisme de corps, il est injectif et on peut considérer L comme une extension de K en identifiant K à $f(K) \simeq K$.
Si L et M sont deux extensions d'un corps K , un K -morphisme de L dans M est un morphisme de corps qui fixe les éléments de K , c'est-à-dire un morphisme de corps $g : L \rightarrow M$ tel que pour tout $x \in K$, $g(x) = x$.

Remarque : Si L est une extension de K , alors L est un K -espace vectoriel (c'est aussi une K -algèbre).

Définition 1.4. (degré d'une extension)

Soit L/K une extension de corps. Si L est de dimension finie sur K , on appelle degré de L sur K et on note $[L : K]$ la dimension de L sur K , autrement dit $[L : K] = \dim_K L$. On dit dans ce cas que L est finie sur K .

Exemples : $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$ est une

Théorème 1.5.

Soit L/F et F/K deux extensions finies. Si $(e_i)_{1 \leq i \leq n}$ est une base de L sur F et $(\varepsilon_j)_{1 \leq j \leq m}$ est une base de F sur K , alors $(e_i \varepsilon_j)_{1 \leq i \leq n, 1 \leq j \leq m}$ est une base de L sur K .

Démonstration :

Corollaire 1.6.

Si L est finie sur F et F finie sur K , alors L est finie sur K et on a

$$[L : K] = [L : F][F : K]$$

Démonstration :

3.2 Extension algébrique

Définition 2.1.

Soient L/K une extension de corps et $x \in L$. On dit que x est algébrique sur K si il existe un polynôme non nul $P \in K[X]$ tel que $P(x) = 0$.

Exemple :

Remarque : Soit L/K une extension de corps et $x \in L$ un élément algébrique sur K . L'application $\varphi : K[X] \rightarrow L$, $P \mapsto \varphi(P) = P(x)$ est un morphisme d'anneaux, son noyau est un idéal de $K[X]$ il est donc principal.

Définition 2.2.

Avec les notations précédentes, l'unique polynôme unitaire $\pi \in K[X]$ tel que $\ker \varphi = (\pi)$ est appelé polynôme minimal de x .

Remarque : Le polynôme π est irréductible.

Exemples :

Soit L/K une extension de corps et $x \in L$. On note $K[x]$ l'ensemble des polynômes en x (à coefficients dans K), c'est-à-dire $K[x] = \{P(x) / P \in K[X]\}$, c'est un sous anneau de L .

Proposition 2.3.

Soit L/K une extension de corps et $x \in L$. Les propriétés suivantes sont équivalentes ;

1. x est algébrique sur K ,
2. $K[x]$ est un K -espace vectoriel de dimension finie.
3. $K[x]$ est un corps.

Démonstration :

Proposition 2.4.

Soit L/K une extension de corps, $x \in K$ un élément algébrique sur K et π son polynôme minimal. Alors $[K[x] : K] = \deg \pi$.

Démonstration :

Définition 2.5.

Une extension L/K est dite algébrique si tout élément de L est algébrique sur K .

Exemple :

Proposition 2.6.

Toute extension finie est algébrique.

Démonstration :

Théorème 2.7.

Soit L/K une extension de corps. On note F l'ensemble des éléments de L qui sont algébriques sur K . Alors :

1. F est un sous corps de L ,
2. Tout élément de L qui est algébrique sur F est dans F ; on dit que F est la fermeture algébrique de K dans L .

Démonstration :

3.3 Corps de décomposition

Définition 3.1.

Soit P un polynôme irréductible de $K[X]$. On dit qu'une extension L de K est un corps de rupture pour P sur K s'il existe une racine x de P dans L telle que $L = K[x]$

Ainsi un corps de rupture est une extension dans laquelle P a une racine, et qui est minimale pour cette propriété.

Exemples :

Proposition 3.2.

Pour tout polynôme irréductible $P \in K[X]$, il existe un corps de rupture L . De plus L est unique à K -isomorphisme près.

Démonstration :

Définition 3.3.

Soient K un corps et P un polynôme (qu'on ne suppose pas irréductible) de $K[X]$. On dit qu'une extension L/K est un corps de décomposition pour P sur K si L vérifie les deux propriétés suivantes :

1. P est scindé sur L .
2. On a $L = K[x_1, \dots, x_n]$, où $x_1, \dots, x_n$ sont les racines de P dans L .

Ainsi un corps de décomposition est une extension minimale de K sur laquelle P est scindé.

Théorème 3.4.

Pour tout P de $K[X]$, il existe un corps de décomposition L , qui est unique à K -isomorphisme près.

Démonstration : admis

Les résultats ci-dessus vont nous permettre de construire les corps finis.

Rappelons qu'un corps fini K est de caractéristique $p > 0$. Il peut être vu comme

extension de $F_p = \mathbb{Z}/p\mathbb{Z}$ via l'application $F_p \rightarrow K, \bar{n} \mapsto n1_K$. En particulier c'est un F_p -espace vectoriel de dimension finie (disons d) donc le cardinal de K est une puissance de p puisque K est isomorphe à F_p^d en tant que F_p -espace vectoriel.

Théorème 3.5.

Soit p un nombre premier et $q = p^n$ avec $n \in \mathbb{N}^*$. Alors il existe un corps de cardinal q , unique à isomorphisme près. C'est le corps de décomposition sur F_p du polynôme $X^q - X$. On le note F_q .

3.4 Extensions normales

Définition 4.1.

Une extension de corps L/K est dite normale si tout polynôme irréductible de $K[X]$ qui possède une racine dans L est scindé sur L .

Exemples :

1. L'extension $\mathbb{Q}[i]/\mathbb{Q}$ est normale.
2. L'extension $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ n'est pas normale, le polynôme $X^3 - 2$
3. L'extension $\mathbb{C}/\mathbb{R}$ est normale.

Proposition 4.2.

Toute extension de degré 2 est normale.

Démonstration :

Théorème 4.3.

Soit K un corps. Soit L une extension finie de K . Alors L est normale si et seulement s'il existe un polynôme $P \in K[X]$ dont elle est le corps de décomposition.