UNIVERSITE PARIS 7 – DENIS DIDEROT

COURS D'ALGEBRE DE MAITRISE

A. Bruguières

1^{er} semestre 1995-1996

Révisé le 24/11/2001

ALGEBRE II

Chapitre I : Anneaux

1. Généralités sur les anneaux

1.1. Introduction de la notion d'anneau

1.1.1. Définition. On appelle *anneau* la donnée d'un ensemble A, muni de deux lois de composition interne $+$ (l'*addition*) et $\cdot$ (la *multiplication*) vérifiant les conditions suivantes :

1) $(A, +)$ est un groupe abélien;
2) $\cdot$ est associative et admet un élément neutre (appelé *unité*, et noté 1);
3) $\cdot$ est distributive à gauche et à droite par rapport à $+$, autrement dit :

$$\forall x, y, z \in A, \quad x \cdot (y + z) = (x \cdot y) + (x \cdot z) \text{ et } (y + z) \cdot x = (y \cdot x) + (z \cdot x)$$

(ce qui revient à dire que pour tout $x \in A$, les applications $y \mapsto x \cdot y$ et $y \mapsto y \cdot x$ sont des morphismes de groupe de $(A, +)$ dans lui-même).
On dit que l'anneau A est *commutatif* si la loi $\cdot$ est commutative.

1.1.2. Remarques.
1) On omet le plus souvent le symbole $\cdot$ dans la notation; on écrit donc xy pour $x \cdot y$.
2) Si $x \in A$ et $n \in \mathbb{N}$, on note $x^n = x \cdot x \cdots x$ (n fois), en convenant que $x^0 = 1$.
3) On a pour tout $x \in A$: $0 \cdot x = x \cdot 0 = 0$, et $(-1) \cdot x = -x = x \cdot (-1)$.
4) On a $0 = 1$ si et seulement si $A = \{0\}$.

1.1.3. Définition. Un élément x de l'anneau A est dit *inversible* s'il existe $y \in A$ tel que $xy = 1 = yx$. Si un tel y existe, il est unique; on l'appelle *inverse de* x, et on le note x^{-1}. On note A^* l'ensemble des éléments inversibles de A.

1.1.4. Remarque. Si x et y sont inversibles, xy est inversible, d'inverse $y^{-1}x^{-1}$; et 1 est inversible (il est son propre inverse), de sorte que A^*, muni de la multiplication, est un groupe (abélien si A est un anneau commutatif).

1.1.5. Définition. Soit A un anneau. On dit que A est un *corps* si $A^* = A - \{0\}$.

1.1.6. Remarque. Tout corps a au moins deux éléments; en effet si $A = \{0\}$, $0 = 1$ donc tout élément de A est inversible.

EXEMPLES. $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ sont des corps. $(\mathbb{Z},+,\times)$ est un anneau, mais pas un corps. On a en effet $\mathbb{Z}^* = \{1,-1\}$.

1.2. Sous-anneaux, morphismes d'anneaux, idéaux

1.2.1. Définition. Soit A un anneau. On dit qu'une partie B de A est un *sous-anneau de* A si les conditions suivantes sont satisfaites :

1) $\forall x, y \in B,\ x - y \in B$;
2) $\forall x, y \in B,\ x \cdot y \in B$;
3) $1 \in B$.

Si L est un corps, on appelle *sous-corps de* L tout sous-anneau K de L vérifiant en outre : $\forall x \in K - \{0\},\ 1/x \in K$.

1.2.2. REMARQUES.
1) Un sous-anneau de l'anneau A est donc en particulier un sous-groupe de $(A,+)$.
2) Soit A un anneau. L'intersection d'une famille quelconque de sous-anneaux de A est encore un sous-anneau de A. En particulier, si X est une partie de A, l'intersection des sous-anneaux de A contenant X est le plus petit sous-anneau de A contenant X. On l'appelle *sous-anneau de* A *engendré par* X.

1.2.3. Définition. Soient A et B deux anneaux, et f une application de A dans B. On dit que f est un *morphisme d'anneaux* si :

1) $\forall x, y \in A,\ f(x+y) = f(x) + f(y)$;
2) $\forall x, y \in A,\ f(xy) = f(x)f(y)$;
3) l'image par f de l'unité de A est l'unité de B.

Si K et L sont deux corps, un morphisme d'anneaux de K vers L est aussi appelé *morphisme de corps.*

1.2.4. REMARQUES.
1) Un morphisme d'anneaux $f : A \longrightarrow B$ est en particulier un morphisme de groupes de $(A,+)$ dans $(B,+)$.
2) Si $f : A \longrightarrow B$ et $g : B \longrightarrow C$ sont des morphismes d'anneaux, $g \circ f : A \longrightarrow C$ est un morphisme d'anneaux.
L'identité de A est un morphisme d'anneaux de A dans A.
3) Si $f : A \longrightarrow B$ est un morphisme d'anneaux bijectif, la bijection réciproque f^{-1} est un morphisme d'anneaux de B vers A. On dit alors que f est un *isomorphisme d'anneaux.*
4) Soit $f : A \longrightarrow B$ un morphisme d'anneaux; alors $f(A^*) \subset B^*$, et f induit par restriction un morphisme de groupes de A^* vers B^*.
En particulier, un morphisme de corps est toujours injectif.
5) Soit A un anneau, $B \subset A$ un sous-anneau de A, et notons i l'application d'inclusion de B dans A. Alors il existe une unique structure d'anneau sur B telle que i soit un morphisme d'anneaux de B dans A (c'est la structure obtenue en munissant B de l'addition et de la multiplication induites par celles de A).
Un sous-corps d'un corps est un corps.

1.2.5. Définition. Soit A un anneau. Une partie I de A est un *idéal à gauche* (resp. *à droite*) de A si elle vérifie :

1) I est un sous-groupe de $(A, +)$;
2) $\forall x \in A, \forall y \in I$, $x \cdot y \in I$ (resp. $y \cdot x \in I$).

On dit que I est un *idéal bilatère* si c'est un idéal à gauche et à droite.

1.2.6. Définitions. Soit $f : A \longrightarrow B$ un morphisme d'anneaux. On appelle *image de* f l'ensemble

$$\mathsf{Im}\, f = \{b \in B \mid \exists a \in A, f(a) = b\} \subset B$$

(c'est l'image ensembliste de f) et *noyau de* f l'ensemble

$$\mathsf{Ker}\, f = \{a \in A \mid f(a) = 0\} \subset A$$

(c'est le noyau de f vu comme un morphisme de groupes de $(A, +)$ vers $(B, +)$).

1.2.7. Remarque. L'image de f est un sous-anneau de B, et le noyau de f est un idéal bilatère de A.

1.3. Anneaux quotients

1.3.1. Proposition-définition. *Soit A un anneau, I un sous-groupe additif de A. Les deux conditions suivantes sont équivalentes :*

(i) I est un idéal bilatère de A;

(ii) il existe sur le groupe quotient A/I une structure d'anneau telle que la surjection canonique $\pi : A \longrightarrow A/I$ soit un morphisme d'anneaux.

En outre, si une telle structure d'anneau existe sur A/I, elle est unique. Muni de cette structure, A/I est appelé anneau quotient de A par I.

Demonstration. Le groupe $(A, +)$ étant commutatif, le sous-groupe $I \subset A$ est distingué. Il définit sur A une relation d'équivalence, la *congruence modulo* I :

$$x \equiv y \ \ (I) \Longleftrightarrow y - x \in I\,.$$

L'ensemble quotient A/I est l'ensemble des classes d'équivalence pour cette relation; et la surjection canonique $\pi : A \longrightarrow A/I$ associe à $x \in A$ sa classe d'équivalence $\overline{x}$, qui n'est autre que $x + I$. Il existe sur A/I une unique loi de composition interne $+$ telle que $(A/I, +)$ soit un groupe commutatif, et π un morphisme de groupes de noyau I.
Supposons qu'il existe sur A/I une multiplication $\cdot$ telle que $(A/I, +, \cdot)$ soit un anneau, et π un morphisme d'anneaux. Alors pour tous $x, y \in A$, $\pi(x) \cdot \pi(y) = \pi(xy)$; comme π est surjectif, on voit qu'il y a unicité d'une telle multiplication. En outre, $I = \mathsf{Ker}(\pi)$ est un idéal bilatère.
Réciproquement supposons que I soit un idéal bilatère. Pour $a, b \in A/I$, choisissons $x, y \in A$ tels que $\pi(x) = a$ et $\pi(y) = b$; l'élément $\pi(xy)$ ne dépend pas du choix de x et de y. En effet, si $x' \equiv x \ \ (I)$ et $y' \equiv y \ \ (I)$, alors $x'y' - xy = x'(y' - y) + (x' - x)y \in I$, donc $x'y' \equiv xy \ \ (I)$. On peut donc poser $a \cdot b = \pi(xy)$, définissant ainsi une loi de composition interne $\cdot$ sur A/I. On vérifie facilement que $(A/I, +, \cdot)$ est un anneau, et que π est un morphisme d'anneaux. $\square$

1.3.2 Proposition. (Factorisation d'un morphisme d'anneaux)
Soit $f : A \to B$ un morphisme d'anneaux, et $p : A \to A'$ un morphisme d'anneaux surjectif. Les deux conditions suivantes sont équivalentes :

(i) $\operatorname{Ker} p \subset \operatorname{Ker} f$ *;*

(ii) il existe un morphisme d'anneaux $g : A' \to B$ tel que $g \circ p = f$.

En outre si un tel g existe, il est unique; on a alors $\operatorname{Im} g = \operatorname{Im} f$, et $\operatorname{Ker} g = p(\operatorname{Ker} f)$.

DEMONSTRATION. Notons $I = \operatorname{Ker} p$. Supposons qu'il existe une application $g : A' \to B$ telle que $g \circ p = f$. Alors g est un morphisme d'anneaux d'image $\operatorname{Im} f$, le noyau de f contient I, et le noyau de g est l'image par p de celui de f. En effet, soient $a, b \in A'$, et soient $x, y \in A$ tels que $p(x) = a$ et $p(y) = b$ (leur existence résulte de la surjectivité de p). Alors $g(a+b) = g(p(x)+p(y)) = g(p(x+y)) = f(x+y) = f(x)+f(y) = g(p(x))+g(p(y)) = g(a) + g(b)$, et de façon analogue $g(ab) = g(a)g(b)$; de plus $g(1) = g(p(1)) = f(1) = 1$. Ainsi, g est un morphisme d'anneaux. Il est clair que l'image de g est celle de f; si $x \in I$, on a $f(x) = g(p(x)) = g(0) = 0$, donc $I \subset \operatorname{Ker} f$; enfin pour $a = p(x)$, on a $g(a) = 0 \Longleftrightarrow f(x) = 0$ donc $\operatorname{Ker} g$ est l'image par p de $\operatorname{Ker} f$.
Pour achever la démonstration, il ne reste donc plus qu'a montrer que si $\operatorname{Ker} p \subset \operatorname{Ker} f$, il existe une application unique $g : A' \longrightarrow B$ telle que $g = f \circ p$. L'unicité de g résulte de la surjectivité de p : si $a = p(x)$, on doit avoir $g(a) = f(x)$. D'autre part, la valeur de $f(x)$ ne dépend pas du choix de l'antécedent x de a; en effet, si x' était un autre antécédent, on aurait $x' - x \in \operatorname{Ker} p \subset \operatorname{Ker} f$, donc $f(x') = f(x)$. D'où l'existence de g. $\square$

1.3.3. Proposition. (Propriété universelle du quotient)
Soit A un anneau, I un idéal bilatère de A, et $\pi : A \longrightarrow A/I$ la surjection canonique. Soit B un autre anneau.
Se donner un morphisme d'anneaux $g : A/I \to B$ équivaut à se donner un morphisme d'anneaux $f : A \to B$ tel que $I \subset \operatorname{Ker} f$.
Plus précisément, étant donné un morphisme d'anneaux $f : A \to B$ tel que $I \subset \operatorname{Ker} f$, il existe un unique morphisme d'anneaux $\widetilde{f} : A/I \to B$ tel que $\widetilde{f} \circ \pi = f$. On dit que $\widetilde{f}$ s'obtient à partir de f par passage au quotient.
On a alors $\operatorname{Im} \widetilde{f} = \operatorname{Im} f$, et $\operatorname{Ker} \widetilde{f} = \pi(\operatorname{Ker} f)$.

DEMONSTRATION. Résulte immédiatement de la proposition précédente, appliquée à $A' = A/I$ et $p = \pi$. $\square$

1.3.4. Proposition. (Factorisation canonique d'un morphisme d'anneaux)
Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Il existe un unique isomorphisme d'anneaux $\widetilde{f} : A/\operatorname{Ker} f \longrightarrow \operatorname{Im} f$ rendant commutatif le diagramme suivant :

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\
A/\operatorname{Ker} f \arrow[r, "\widetilde{f}"'] & \operatorname{Im} f \arrow[u, "\text{incl.}"']
\end{tikzcd}$$

(autrement dit, tel qu'on ait $\forall x \in A$, $\widetilde{f}(\pi(x)) = f(x)$).

DEMONSTRATION.
Appliquons **1.3.3** au morphisme f et à l'idéal $I = \mathsf{Ker}\, f$. Il existe un morphisme d'anneaux unique $g : A/I \longrightarrow B$ vérifiant : $\forall x \in A,\ g(\pi(x)) = f(x)$. En outre g a pour image $\mathsf{Im}\, f$, et pour noyau $\pi(\mathsf{Ker}\, f) = 0$. Soit $\widetilde{f} : A/\mathsf{Ker}\, f \longrightarrow \mathsf{Im}\, f$ l'application $a \mapsto g(a)$; c'est l'unique morphisme rendant commutatif le diagramme de l'énoncé, et c'est un isomorphisme d'après ce qui précède. □

1.4. Algèbres

1.4.1. Définitions. Soit A un anneau commutatif. On appelle A*-algèbre* la donnée d'un anneau B et d'un morphisme d'anneaux $\eta : A \longrightarrow B$ vérifiant :

$$\forall x \in A, \forall y \in B,\ \eta(x)\, y = y\, \eta(x)\,.$$

On dit souvent (abusivement) que B est une A-algèbre, et on appelle η le *morphisme structural.*
Si B et B' sont deux A-algèbres, on appelle *morphisme de* A*-algèbres* de B vers B' tout morphisme d'anneaux $f : B \longrightarrow B'$ vérifiant $f \circ \eta = \eta'$ (où η et η' sont les morphismes d'anneaux définissant les structures de A-algèbre de B et B' respectivement).
L'anneau A est une A-algèbre, le morphisme structural étant l'identité.

1.5. Exemples d'anneaux et d'algèbres

0) L'anneau nul.

L'ensemble réduit à un élément admet une unique structure d'anneau, appelée *anneau nul* et notée 0. L'anneau nul vérifie la propriété universelle suivante. Pour tout anneau A, il existe un unique morphisme d'anneaux de A vers 0.

1) L'anneau $\mathbb{Z}$.

L'ensemble $\mathbb{Z}$ des entiers relatifs, muni de l'addition et de la multiplication usuelles, est un anneau. Il vérifie la propriété universelle suivante. Pour tout anneau A, il existe un unique morphisme d'anneau de $\mathbb{Z}$ dans A.

Rappelons que si $(G, +)$ est un groupe abélien et $x \in G$, il existe un unique morphisme de groupes de $\mathbb{Z}$ vers G envoyant 1 en x. L'image par ce morphisme d'un entier n est notée $n \cdot x$, ou plus simplement nx. On a $n \cdot x = x + \cdots + x$, n fois, si $n > 0$, 0 si $n = 0$, et $-(-n)x$ si $n < 0$.
Soit A un anneau et $\phi : \mathbb{Z} \to A$ un morphisme d'anneaux. Alors $\phi(1) = 1$, donc $\phi(n) = n \cdot 1$ pour tout $n \in \mathbb{Z}$. On voit donc qu'un tel ϕ, s'il existe, est unique. Posons $\phi(n) = n \cdot 1$. Alors pour tout $x \in A$ et tout $n \in \mathbb{Z}$, on a $n \cdot x = \phi(n)x = x\phi(n)$; en particulier $\phi(nm) = (nm) \cdot 1 = n \cdot (m \cdot 1) = \phi(n)\phi(m)$. D'autre part $\phi(1) = 1$, donc ϕ est bien un morphisme d'anneaux.

Remarque. Soit A un anneau; l'unique morphisme d'anneaux $\phi : \mathbb{Z} \longrightarrow A$ fait de A une $\mathbb{Z}$-algèbre. En effet pour $n \in \mathbb{Z}$ et $x \in A$, on a $\phi(n)x = x\phi(n) = n \cdot x$.
Il revient donc au même de se donner un anneau ou une $\mathbb{Z}$-algèbre. De plus, soient A et B deux anneaux, qu'on peut donc voir comme des $\mathbb{Z}$-algèbres. Les morphismes de $\mathbb{Z}$-algèbres de A vers B ne sont autres que les morphismes d'anneaux de A vers B.
Ainsi les notions d'anneau et de $\mathbb{Z}$-algèbre sont équivalentes. De ce point de vue, la notion de A-algèbre est donc une généralisation de la notion d'anneau.

2) Produits d'anneaux.

Soient A et B deux anneaux. Le produit cartésien $A \times B$, muni des deux lois de composition internes $+$ et $\cdot$ définies par

$$(x, y) + (x', y') = (x + x', y + y') \text{ et } (x, y) \cdot (x', y') = (xx', yy')$$

pour $(x, y), (x', y') \in A \times B$, est un anneau appelé *anneau produit de A et de B*.
Plus généralement, soit I un ensemble et $(A_i)_{i \in I}$ une famille d'anneaux indexée par I. Alors l'ensemble produit $\prod_{i \in I} A_i$, muni des deux lois de composition interne $+$ et $\cdot$ définies par

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I} \text{ et } (x_i)_{i \in I} \cdot (y_i)_{i \in I} = (x_i y_i)_{i \in I}$$

est un anneau appelé *anneau produit des A_i*.

Remarque. L'unité de $\prod_{i \in I} A_i$ est l'élément $(1_{A_i})_{i \in I}$, et on a $(\prod_{i \in I} A_i)^* = \prod_{i \in I} {A_i}^*$.
Pour tout $j \in I$, la j-ième projection

$$\begin{aligned} p_j : \prod_{i \in I} A_i &\longrightarrow A_j \\ (x_i)_{i \in I} &\mapsto x_j \end{aligned}$$

est un morphisme d'anneaux, et $\prod_{i \in I} A_i$, muni des morphismes p_i, vérifie la propriété universelle suivante. Pour tout anneau B et toute famille $(f_i)_{i \in I}$, où chaque f_i est un morphisme d'anneaux $B \longrightarrow A_i$, il existe un unique morphisme d'anneaux $g : B \longrightarrow \prod_{i \in I} A_i$ vérifiant $\forall i \in I, p_i \circ g = f$. (C'est le morphisme défini par $x \mapsto (f_i(x))_{i \in I}$).

En particulier, soit I un ensemble et A un anneau. On peut considérer la famille constante d'anneaux $A_i = A$. Alors $\prod_{i \in I} A$ n'est autre que l'ensemble A^I des suites d'éléments de A indexées par I (autrement dit, l'ensemble des applications de I dans A), qui est donc muni d'une structure d'anneau. De plus, l'application $\eta : A \longrightarrow A^I$ définie par $a \mapsto (a)_{i \in I}$ est un morphisme d'anneaux; si A est commutatif, A^I est donc naturellement muni d'une structure de A-algèbre.
Soit $A^{(I)} \subset A^I$ l'ensemble des suites presque nulles d'éléments de A indexées par I. C'est l'ensemble des suites $(a_i)_{i \in I}$ telles que $\{i \in I \mid a_i \neq 0\}$ soit fini. Alors $A^{(I)}$ est un idéal bilatère de A^I. Si I est fini (ou $A = 0$), $A^{(I)} = A^I$, mais dans tout autre cas $A^{(I)}$ est distinct de A^I.

3) Endomorphismes d'un groupe abélien.

Soit $(M,+)$ un groupe abélien. Si f, g sont deux endomorphismes du groupe M, l'application $f+g : M \longrightarrow M$, $x \mapsto f(x)+g(x)$ est un endomorphisme de M, de même que $f \circ g$.
L'ensemble des endomorphismes du groupe M, muni des lois $+$ et $\circ$, est un anneau, en général non commutatif, qu'on note $\mathsf{End}(M)$.

4) Anneaux de matrices.

Soit A un anneau et n un entier naturel. Soit $M_n(A)$ l'ensemble des matrices $n \times n$ à coefficients dans A; c'est l'ensemble des familles d'éléments de A indexées par l'ensemble $\{1,\ldots,n\} \times \{1,\ldots,n\}$. On définit dans $M_n(A)$ deux lois de composition interne $+$ et $\cdot$ en posant, pour $M=(a_{i,j})_{1\le i,j\le n}$ et $N=(b_{i,j})_{1\le i,j\le n}$:

$$M+N=(a_{i,j}+b_{i,j})_{1\le i,j\le n} \text{ et } M\cdot N=(c_{i,j})_{1\le i,j\le n}\,, \text{ où } c_{i,j}=\sum_{k=1}^{n} a_{i,k}b_{k,j}\,.$$

On fait ainsi de $M_n(A)$ un anneau. L'application

$$\begin{aligned} \eta : A &\longrightarrow M_n(A) \\ a &\mapsto \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix} \end{aligned}$$

est un morphisme d'anneaux.
De plus, si A est commutatif, on a $\eta(a)M = M\eta(a)$ pour tout $a \in A$ et tout $M \in M_n(A)$, ce qui fait de $M_n(A)$ une A-algèbre. Notons cependant que $M_n(A)$ n'est jamais commutatif si $n \ge 2$ (sauf si A est l'anneau nul).

5) Polynômes en une indéterminée.

Soit A un anneau commutatif. On appelle *polynôme* toute suite presque nulle d'éléments de A indexée par $\mathbb{N}$. On note $A[X]$ l'ensemble des polynômes (qui n'est autre que $A^{(\mathbb{N})}$).
On définit sur $A[X]$ deux lois de composition interne $+$ et $\cdot$ en posant, pour $P=(a_n)_{n\in\mathbb{N}}$ et $Q=(b_n)_{n\in\mathbb{N}}$,

$$P+Q=(a_n+b_n)_{n\in\mathbb{N}} \text{ et } P\cdot Q=(c_n)_{n\in\mathbb{N}}\,, \text{ où } c_n=\sum_{k=0}^{n} a_k\, b_{n-k}\,.$$

La suite $(c_n)_{n\in\mathbb{N}}$ est presque nulle, car l'ensemble des couples (n,k) tels que $a_k b_{n-k}$ soit non nul est fini. Il est clair que $+$ fait de $A[X]$ un groupe abélien, et que $\cdot$ est distributive par rapport à $+$.
Pour $n,m \in \mathbb{N}$ soit $\delta_{n,m}=1$ si $m=n$, $=0$ sinon. Pour $a \in A$ et $d \in \mathbb{N}$, notons aX^d le polynôme $(a\delta_{d,n})_{n\in\mathbb{N}}$. Un tel polynôme est appelé *monôme de degré d et de coefficient a*.

Tout polynôme P s'écrit de façon unique

$$P = \sum_{n \in \mathbb{N}} a_n X^n ,$$

donc P est une somme finie de monômes. Montrons que $\cdot$ est commutative et associative, et que $1X^0$ est un élément neutre pour $\cdot$. Il suffit, par distributivité de $\cdot$ par rapport à $+$, de le vérifier sur les monômes. Or, on a $(aX^m) \cdot (bX^n) = (ab)X^{m+n}$, donc ces propriétés résultent des propriétés analogues de la multiplication de A et de l'addition de $\mathbb{N}$.
Ainsi, $A[X]$, muni de $+$ et $\cdot$, est un anneau commutatif. L'application $\eta : A \to A[X]$, $a \mapsto aX^0$ est clairement un morphisme d'anneaux injectif, et fait de $A[X]$ une A-algèbre. Nous ferons systématiquement l'abus consistant à considérer A comme un sous-anneau de $A[X]$ en identifiant l'élément $a \in A$ au polynôme $\eta(a) = aX^0$. Avec cette convention, et posant $X = 1X^1$, on a $aX^n = a \cdot X \cdot X \cdots X$ (où X figure n fois), ce qui justifie a posteriori nos notations.
La A-algèbre $A[X]$ est appelée *algèbre des polynômes en une indéterminée à coefficients dans* A. Cette algèbre, qui contient un élément particulier X, appelé l'*indéterminée*, vérifie la propriété universelle suivante.

1.5.1. Proposition. (Propriété universelle de $A[X]$)
Soit A un anneau commutatif, et B une A-algèbre. Soit x un élément de B. Alors il existe un unique morphisme de A-algèbres $e : A[X] \longrightarrow B$ vérifiant $e(X) = x$.

Demonstration. Soit $\eta : A \longrightarrow B$ le morphisme structural. Soit $e : A[X] \longrightarrow B$ un morphisme d'algèbres, et supposons $e(X) = x$. Soit $P = \sum_{n \in \mathbb{N}} a_n X^n$ un élément de $A[X]$; alors

$$e(P) = \sum_{n \in \mathbb{N}} e(a_n X^n) = \sum_{n \in \mathbb{N}} e(a_n) e(X)^n = \sum_{n \in \mathbb{N}} \eta(a_n) x^n ,$$

donc un tel e, s'il existe, est unique. D'autre part, on vérifie facilement que l'application $e : A[X] \longrightarrow B$ définie par

$$\sum_{n \in \mathbb{N}} a_n X^n \longmapsto \sum_{n \in \mathbb{N}} \eta(a_n) x^n$$

est un morphisme de A-algèbres qui envoie X sur x (cette vérification utilise le fait que $x\,\eta(a_n) = \eta(a_n)\,x$). $\square$

Exemple. Pour $x \in A$, il existe un unique morphisme de A-algèbres $A[X] \longrightarrow A$ qui envoie X sur x ; c'est l'application qui à $P = \sum_n a_n X^n \in A[X]$ associe $P(x) = \sum_n a_n x^n$. On l'appelle *morphisme d'évaluation en* x.

1.5.2. Définitions. Soit $P = \sum_{n \in \mathbb{N}} a_n X^n \in A[X]$ un polynôme non nul. Soit d le plus grand entier naturel tel que le coefficient a_d soit non nul. Alors d est appelé *degré de* P, et noté $\deg P$; et a_d est appelé *coefficient directeur de* P. On dit que P est *unitaire* si son coefficient directeur vaut 1. Si P est nul, on pose $\deg P = -\infty$.

1.5.3. Proposition. *Pour tous P, $Q \in A[X]$, on a :*
(1) $\deg(PQ) \leq \deg P + \deg Q$ *;*
(2) $\deg(P+Q) \leq \sup(\deg P, \deg Q)$.
De plus (1) est une égalité sauf dans le cas suivant : P et Q sont non nuls, et le produit de leurs coefficients directeurs est nul.
De même (2) est une égalité sauf dans le cas suivant : P, Q sont non nuls, de même degré, et la somme de leurs coefficients directeurs est nulle.

DEMONSTRATION. Si P ou Q est nul, c'est immédiat. Supposons donc P et Q non nuls, soit m (resp. n) le degré de P (resp. Q) et a (resp. b) son coefficient directeur.
On a $P = aX^m +$ termes de degré $< m$, et $Q = bX^n +$ termes de degré $< n$, donc $PQ = abX^{m+n} +$ termes de degré $< m+n$. De même, si par exemple $m > n$, $P + Q = aX^m +$ termes de degré $< m$, mais si $m = n$, $P + Q = (a+b)X^m +$ termes de degré $< m$. □

2. Généralités sur les anneaux commutatifs

Désormais, tous les anneaux seront supposés commutatifs, sauf mention explicite du contraire. Dans un anneau commutatif, les notions d'idéal à gauche, d'idéal à droite, et d'idéal bilatère, coïncident. On utilisera donc le mot idéal pour désigner cette notion.

2.1. Identités remarquables et éléments nilpotents

Soit A un anneau et soient x, $y \in A$, et $n \in \mathbb{N}$. On a alors la *formule du binôme de Newton* :

2.1.1
$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k} \,,$$

où C_n^k désigne le coefficient binômial $\dfrac{n!}{k!(n-k)!}$.
D'autre part, on a

2.1.2
$$(x-y)(x^n + x^{n-1}y + \cdots + xy^{n-1} + y^n) = x^{n+1} - y^{n+1} \,.$$

En particulier, on a pour tout $x \in A$:

2.1.3
$$(x-1)(x^n + x^{n-1} + \cdots + 1) = x^{n+1} - 1 \,.$$

Si A n'est pas commutatif, les formules (**2.1.1**) et (**2.1.2**) restent vraies si $yx = xy$, et en particulier (**2.1.3**) est toujours vraie.

2.1.4. Définitions. Soit A un anneau. Un élément x de A est dit *nilpotent* s'il existe un entier naturel n tel que x^n soit nul. Si x est nilpotent, le plus petit entier naturel n vérifiant $x^n = 0$ est appelé *degré de nilpotence de x*. On note $\mathsf{Nil}(A)$ l'ensemble des éléments nilpotents de A.

2.1.5. Remarques.

1) Si x est nilpotent, $-x$ est nilpotent, de même degré de nilpotence que x. (En effet, $(-x)^n = (-1)^n x^n$).

2) Si $A \neq 0$, un élément inversible n'est jamais nilpotent.

3) Soit x un élément nilpotent de A, de degré de nilpotence n. Alors en vertu de (**2.1.3**) on a $(1-x)(1+x+\cdots+x^{n-1}) = 1-x^n = 1$, donc $1-x$ est inversible, d'inverse $1+x+\cdots+x^{n-1}$.

2.1.6. Proposition. *L'ensemble* $\mathsf{Nil}(A)$ *est un idéal de* A.

Demonstration. L'ensemble $\mathsf{Nil}(A)$ est non vide, car 0 est nilpotent. D'autre part, si $a \in A$ et $x \in \mathsf{Nil}(A)$, soit n tel que $x^n = 0$. On a $(ax)^n = a^n x^n$ (car A est commutatif) $= 0$, donc $ax \in \mathsf{Nil}(A)$. Enfin soient x, y des nilpotents de A de degrés de nilpotence respectifs m et n. D'après (**2.1.1**), on a

$$(x+y)^{m+n-1} = \sum_{k=0}^{m+n-1} C_{n+m-1}^k x^k y^{m+n-1-k}$$

$$= (\sum_{k=0}^{m-1} C_{n+m-1}^k x^k y^{m-1-k}) y^n + (\sum_{k=m-k}^{m+n-1} C_{n+m-1}^k x^{k-m} y^{m+n-1-k}) x^m = 0,$$

donc $x+y \in \mathsf{Nil}(A)$. De même $x-y = x+(-y) \in \mathsf{Nil}(A)$. Ainsi, $\mathsf{Nil}(A)$ est bien un idéal de A. $\square$

2.1.7. Remarque. Soit $A = M_2(\mathbb{R})$. Posons $x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Alors $x^2 = y^2 = 0$, mais $z = x+y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ vérifie $z^2 = 1$, donc z, inversible, n'est pas nilpotent. L'ensemble des éléments nilpotents de A n'est donc pas un idéal, ce qui montre que la commutativité de A est essentielle dans **2.1.6.**

2.2. Diviseurs de zéro, anneaux intègres

Soit A un anneau.

2.2.1. Définition. Un élément x de A est dit *régulier* si la multiplication par x, c'est-à-dire l'application $A \longrightarrow A$, $y \mapsto xy$, est injective. Dans le cas contraire, on dit que x est un *diviseur de zéro*. Autrement dit, x est un diviseur de 0 s'il existe un élément y non nul de A tel que $xy = 0$.

2.2.2. Définition. On dit que l'anneau A est *intègre* si l'ensemble des éléments réguliers de A est $A - \{0\}$.

2.2.3. Remarques.
1) Dans l'anneau nul, 0 n'est pas diviseur de zéro; l'anneau nul n'est donc pas intègre.
2) Si A n'est pas l'anneau nul, 0 est toujours diviseur de zéro, donc A est intègre si et seulement si tout élément non nul est régulier. Cette condition équivaut à :

$$\forall(x,y)\in A^2, xy=0 \Longrightarrow (x=0 \text{ ou } y=0).$$

3) En particulier, tout sous-anneau d'un anneau intègre est intègre.
4) Tout élément inversible est régulier, donc tout corps est intègre : en particulier, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux intègres, ainsi que $\mathbb{Z}$, en tant que sous-anneau de $\mathbb{Q}$.

2.2.4 Proposition. *Si A est un anneau intègre, l'anneau $A[X]$ est intègre. De plus, pour P, $Q\in A[X]$, on a* $\deg(PQ)=\deg P+\deg Q$.

Demonstration. Si $P\in A[X]$, on a $P=0 \Longleftrightarrow \deg P=-\infty$, donc la première assertion résulte de la seconde. Démontrons celle-ci.
Soient P, $Q\in A[X]$. On a $\deg(PQ)=\deg P\deg Q$ dans les cas suivants (cf. **1.5.3**) :
— P ou Q est nul;
— P et Q sont non nuls, et le produit de leurs coefficients directeurs est non nul.
C'est donc toujours le cas si A est intègre. □

2.3. Propriétés des idéaux

2.3.1. SORITES ET NOTATIONS. Soit A un anneau, commutatif comme il se doit. L'ensemble des idéaux de A est ordonné par l'inclusion. Il contient notamment A lui-même, et l'idéal $\{0\}$, qu'on note abusivement 0. Une intersection quelconque d'idéaux de A est un idéal de A.
Si X est une partie de A, il existe un plus petit idéal de A contenant X : c'est l'intersection de tous les idéaux de A contenant X. On note cet idéal $\langle X\rangle$.
On peut décrire $\langle X\rangle$ plus précisément. On appelle *combinaison linéaire d'éléments de X (à coefficients dans A)* tout élément de A de la forme

$$\sum_{i\in F} a_i x_i\,,$$

où F est un ensemble fini, et pour $i\in F$, $a_i\in A$ et $x_i\in X$.
Avec cette définition, $\langle X\rangle$ n'est autre que l'ensemble des combinaisons linéaires d'éléments de X à coefficients dans A. En effet, il est clair que tout idéal contenant X doit contenir les combinaisons linéaires d'éléments de X; d'autre part, ces combinaisons linéaires constituent un idéal qui n'est donc autre que $\langle X\rangle$.
Si $(x_i)_{i\in I}$ est une famille quelconque d'éléments de A, on notera $(\,(x_i)_{i\in I}\,)$ l'idéal engendré par l'ensemble des x_i.

2.3.2 Définitions. Un idéal de A est dit *de type fini* s'il est engendré par une famille finie d'éléments de A. Il est dit *principal* s'il est engendré par un seul élément; autrement dit, s'il est de la forme (x), pour $x\in A$. On a $(x)=xA=\{ax, a\in A\}$.

2.3.3. REMARQUE. L'anneau A est un corps si et seulement s' il admet exactement deux idéaux (à savoir A tout entier, et 0).

Définitions. Soient I, J deux idéaux de A. On appelle *somme de* I *et de* J, et on note $I+J$, l'idéal engendré par $I \cup J$. On a donc $I+J=\{x+y; x \in I \text{ et } y \in J\}$.
On appelle *produit de* I *et de* J, et on note IJ, l'idéal engendré par les xy, pour x décrivant I et y décrivant J. Ainsi, IJ est l'ensemble des sommes (finies) d'éléments de la forme xy, $x \in I$ et $y \in J$.

EXERCICES
1) Le produit de deux idéaux principaux est-il principal? Qu'en est-il de leur somme?
2) Soit A l'anneau non commutatif $M_2(\mathbb{R})$. Montrer que A admet exactement deux idéaux bilatères, A et 0, mais ce n'est pas un corps.

2.3.4. Proposition. *Soit* $f : A \longrightarrow B$ *un morphisme d'anneaux.*
1) Si J *est un idéal de* B, $f^{-1}(J)$ *est un idéal de* A *contenant* $\mathsf{Ker}\, f$.
2) Si f *est surjectif, l'image par* f *d'un idéal de* A *est un idéal de* B. *De plus, l'application qui à un idéal* J *de* B *associe* $f^{-1}(J)$ *est une bijection*

$$\{\textit{idéaux de } B\} \longrightarrow \{\textit{idéaux de } A \textit{ contenant } \mathsf{Ker}\, f\}.$$

DEMONSTRATION.
1) Il est clair que $f^{-1}(J)$ est un sous-groupe de $(A,+)$ contenant $f^{-1}(0)=\mathsf{Ker}\, f$. Soit $x \in f^{-1}(J)$ et $a \in A$. Alors $f(ax)=f(a)f(x) \in J$, donc $ax \in f^{-1}(J)$. Ainsi $f^{-1}(J)$ est un idéal de A.
2) De même, $f(I)$ est un sous-groupe de $(B,+)$. Soit $y \in f(I)$ et $b \in B$. Alors y s'écrit $f(x)$, pour un $x \in I$, et puisque f est surjectif, b s'écrit $f(a)$, pour un $a \in A$. Ainsi $by=f(a)f(x)=f(ax) \in f(I)$, donc $f(I)$ est un idéal de B.
Soit $\mathcal{A}=\{\text{idéaux de } A \text{ contenant } \mathsf{Ker}\, f\}$ et $\mathcal{B}=\{\text{idéaux de } B\}$. Si $J \in \mathcal{B}$, $f^{-1}(J) \in \mathcal{A}$, et si $I \in \mathcal{A}$, $f(I) \in \mathcal{B}$. D'autre part, f étant surjectif, on a $f(f^{-1}(J))=J$ pour tout $J \in \mathcal{B}$. Pour $I \in \mathcal{A}$, on a clairement $I \subset f^{-1}(f(I))$. Montrons l'inclusion inverse. Si $x \in f^{-1}(f(I))$, il existe $x' \in I$ tel que $f(x)=f(x')$. On a $x'-x \in \mathsf{Ker}\, f \subset I$, et comme $x' \in I$, on en déduit $x \in I$. Ainsi, $f^{-1}(f(I))=I$. En résumé, f^{-1} définit une bijection de $\mathcal{B}$ vers $\mathcal{A}$ dont l'inverse est donné par f. $\square$

REMARQUE. L'ensemble A est un idéal de A, et $f(A)$ contient l'unité de B; donc $f(A)$ ne peut être un idéal de B que lorsque f est surjectif. Par exemple, l'image de $\mathbb{Z}$ dans $\mathbb{Q}$ par l'inclusion n'est pas un idéal de $\mathbb{Q}$.

2.4. Idéaux premiers et maximaux

2.4.1. Définition. Soit I un idéal de A.
On dit que I est *premier* si A/I est intègre.
On dit que I est *maximal* si A/I est un corps.

Puisque tout corps est intègre, tout idéal maximal est premier.

2.4.2. Proposition. *Pour I idéal de A, on a les équivalences suivantes :*
(i) I est premier $\Longleftrightarrow$ $I \neq A$ et $\forall x, y \in A$, $xy \in I \Longrightarrow x \in I$ ou $y \in I$;
(ii) I est maximal $\Longleftrightarrow$ $I \neq A$ et $\forall J$ idéal de A, $I \subset J \Longrightarrow J = I$ ou $J = A$. (Autrement dit I est un idéal maximal si et seulement si c'est un élément maximal de l'ensemble des idéaux de A distincts de A).

DEMONSTRATION. Soit $\pi : A \longrightarrow A/I$ la surjection canonique, et si $x \in A$, notons $\overline{x}$ son image par π.
(i) On a I premier $\Longleftrightarrow$ A/I intègre $\Longleftrightarrow$ ($A/I \neq 0$ et $\forall u, v \in A/I$, $uv = 0 \Longrightarrow u = 0$ ou $v = 0$). Or tout élément de A/I est de la forme $\overline{x}$, avec $x \in A$, et on a $\overline{x} = 0 \Longleftrightarrow x \in I$; d'où l'équivalence (i).
(ii) En vertu de la proposition **2.3.4,** les idéaux de A/I sont en bijection avec les idéaux de A contenant I; on a donc : I maximal $\Longleftrightarrow$ A/I est un corps $\Longleftrightarrow$ A/I admet exactement deux idéaux, qui sont 0 et A/I (cf. **2.3.3**) $\Longleftrightarrow$ il y a exactement deux idéaux de A contenant I, qui sont I et A. $\square$

2.4.3. Proposition. *Soit A un anneau, et I un idéal de A distinct de A. Alors il existe un idéal maximal de A contenant I.*

DEMONSTRATION. On utilise le lemme suivant.

2.4.4. Lemme. *Soit A un anneau, et S une partie de A vérifiant : $\forall x, y \in S$, $xy \in S$ et $1 \in S$. Soit I un idéal de A ne rencontrant pas S, et notons $\mathcal{T}$ l'ensemble des idéaux de A contenant I et ne rencontrant pas S. Alors*
1) $\mathcal{T}$ admet un élément maximal pour l'inclusion;
2) Tout élément maximal de $\mathcal{T}$ est un idéal premier de A.

DEMONSTRATION.
1) Rappelons l'énoncé du théorème de Zorn, qui est équivalent à l'axiome du choix : un ensemble ordonné dont toute partie totalement ordonnée(*) est majorée admet un élément maximal.
On applique ceci à l'ensemble $\mathcal{T}$, muni de l'inclusion.
Soit $\mathcal{B} \subset \mathcal{T}$ une partie totalement ordonnée; nous allons montrer que T admet un majorant dans $\mathcal{T}$. Si $\mathcal{B}$ est vide, il est majoré par $I \in \mathcal{T}$. Sinon, soit $\mathfrak{a}$ la réunion des éléments de $\mathcal{B}$. C'est un idéal de A, en vertu du lemme suivant.

2.4.5. Lemme. *Soit A un anneau, et $\mathcal{B}$ un ensemble non vide d'idéaux de A totalement ordonné par l'inclusion. Alors $\mathfrak{a} = \bigcup_{I \in \mathcal{B}} I$ est un idéal de A.*

DEMONSTRATION. Il existe $I \in \mathcal{B}$, donc $\mathfrak{a}$, qui contient I, est non vide. Si $x \in \mathfrak{a}$ et $a \in A$, il existe $I \in \mathcal{B}$ tel que $x \in I$. Alors $ax \in I \subset \mathfrak{a}$. Enfin si x, $y \in \mathfrak{a}$, il existe I, $J \in \mathcal{B}$ tels que $x \in I$ et $y \in J$. Puisque $\mathcal{B}$ est totalement ordonné, on a $I \subset J$ ou $J \subset I$, donc $x - y \in I \cup J \subset \mathfrak{a}$, ce qui achève la démonstration du lemme **2.4.5.** $\square$

(*) Les connaisseurs savent qu'on peut remplacer 'totalement ordonnée' par 'bien ordonnée', mais nous n'aurons pas besoin de cette version forte.

D'autre part $\mathfrak{a}$ ne rencontre pas S. Soit $J \in \mathcal{B}$; on a $I \subset J \subset \mathfrak{a}$, donc $\mathfrak{a}$ est un élément de $\mathcal{T}$, et par construction, c'est un majorant de $\mathcal{B}$ (en fait, $\mathfrak{a}$ est la borne supérieure de $\mathcal{B}$). Le théorème de Zorn s'applique donc, d'où l'assertion 1) du lemme **2.4.4.**
2) Soit $\mathfrak{p}$ un élément maximal de $\mathcal{T}$. On a $1 \notin \mathfrak{p}$ donc $\mathfrak{p} \neq A$. Soit x un élément de $A - \mathfrak{p}$. Par maximalité de $\mathfrak{p}$, l'idéal $\mathfrak{p} + (x)$ n'est pas un élément de $\mathcal{T}$, et puisqu'il contient I, il doit rencontrer S. Il existe donc $s \in S$, $u \in \mathfrak{p}$ et $a \in A$ tels que $s = u + ax$. De même si $y \in A - \mathfrak{p}$, il existe $t \in S$, $v \in \mathfrak{p}$ et $b \in A$ tels que $t = v + by$. Alors $st = uv + axv + byu + abxy$. Si on avait $xy \in \mathfrak{p}$, st, qui appartient à S, serait aussi un élément de $\mathfrak{p}$; c'est impossible car $\mathfrak{p}$ et S sont disjoints. On a donc montré :

$$x, y \in A - \mathfrak{p} \Longrightarrow xy \in A - \mathfrak{p},$$

ce qui achève la démonstration du lemme **2.4.4.** □

Revenons maintenant à la démonstration de la proposition. On n'utilisera pour le moment que l'assertion 1) du lemme, mais l'assertion 2) nous sera utile plus tard. Soit I un idéal de A, et supposons $I \neq A$. L'ensemble $S = \{1\}$ vérifie les conditions du lemme, donc l'ensemble $\mathcal{T}$ admet un élément maximal $\mathfrak{m}$. Or, $\mathcal{T}$ est l'ensemble des idéaux J de A vérifiant $I \subset J \neq A$; donc $\mathfrak{m}$ est est un idéal contenant I, et il est maximal parmi les idéaux de A distincts de A, donc c'est un idéal maximal. □

2.4.6. Corollaire. *L'ensemble des éléments non inversibles de A est la réunion des idéaux maximaux de A.*

Demonstration. On a $x \in A^* \Longleftrightarrow Ax = A$, donc $x \in A - A^* \Longleftrightarrow Ax \neq A$. Or d'après **2.4.3,** $Ax \neq A \Longleftrightarrow Ax$ est contenu dans un idéal maximal de A. □

2.4.7. Proposition. *L'intersection des idéaux maximaux de A est l'ensemble des $x \in A$ vérifiant : $\forall y \in A$, $1 + xy$ est inversible.*

Demonstration. Soit x un élément de l'intersection des idéaux maximaux de A. Soit $y \in A$. Si $1 + xy \notin A^*$, il existe un idéal maximal $\mathfrak{m}$ tel que $1 + xy \in \mathfrak{m}$. Puisque $\mathfrak{m}$ contient x, on a $1 \in \mathfrak{m}$, d'où contradiction. Donc $1 + xy$ est inversible.
Soit maintenant $x \in A$ tel que pour tout $y \in A$, $1 + xy \in A^*$. Soit $\mathfrak{m}$ un idéal maximal de A, $K = A/\mathfrak{m}$, et notons $y \mapsto \overline{y}$ la surjection canonique de A sur K. Supposons $x \notin \mathfrak{m}$. Puisque K est un corps, $\overline{x}$ est inversible; il existe donc $y \in A$ tel que $\overline{y} = -\overline{x}^{-1}$, et on a $1 + \overline{xy} = 0$, donc $1 + xy \in \mathfrak{m}$, ce qui contredit l'inversibilité de cet élément. Par conséquent on a bien $x \in \mathfrak{m}$. □

2.4.8. Proposition. *L'intersection des idéaux premiers de A est l'idéal $\mathsf{Nil}(A)$.*

Demonstration. Soit $\mathfrak{p}$ un idéal premier de A. L'image d'un élément nilpotent x de A par la surjection canonique $A \longrightarrow A/\mathfrak{p}$ est un élément nilpotent de $A/\mathfrak{p}$, qui est intègre. Or, dans un anneau intègre, tout élément nilpotent est nul, car diviseur de zéro. Ainsi, $x \in \mathfrak{p}$, et donc $\mathsf{Nil}(A)$ est contenu dans l'intersection des idéaux premiers de A.
A présent, soit x un élément non nilpotent de A, et soit $S = \{x^n, n \in \mathbb{N}\}$. On peut appliquer le lemme **2.4.4.** à la partie S, et à l'idéal $I = 0$ (qui ne la rencontre pas, car x n'est pas nilpotent). Alors $\mathcal{T}$ est l'ensemble des idéaux de A ne contenant aucune

puissance de x. Il existe donc un idéal $\mathfrak{p}$ de A ne contenant aucune puissance de x, et maximal pour cette propriété. Un tel idéal est premier, et on a $x \notin \mathfrak{p}$.
Autrement dit, un élément de l'intersection de tous les idéaux premiers de A est nécéssairement nilpotent. □

2.5. Anneaux de fractions

Le corps $\mathbb{Q}$ des rationnels se construit à partir de l'anneau $\mathbb{Z}$ comme ensemble des fractions p/q, avec $p \in \mathbb{Z}$ et $q \in \mathbb{Z} - \{0\}$.
Nous allons généraliser cette construction en associant à un anneau A et une partie S de A un nouvel anneau $S^{-1}A$ dont les éléments seront des 'fractions' $\frac{x}{s}$, avec $x \in A$ et $s \in S$. Le point clé est de préciser à quelle condition deux fractions $\frac{x}{s}$ et $\frac{x'}{s'}$ sont égales. Nous allons voir que, si l'on veut faire fonctionner la construction dans un cadre assez général, on doit envisager une condition d'égalité des fractions légèrement plus compliquée que dans $\mathbb{Q}$.(*)
Soit A un anneau.

Définition. Une partie S de A est dite *multiplicative* si elle vérifie : $\forall x, y \in S, xy \in S$, et $1 \in S$.
Etant donnée une partie multiplicative S de A, on se propose de construire une certaine A-algèbre, notée $S^{-1}A$.
On munit l'ensemble $S \times A$ de la relation $\mathcal{R}$ définie par

$$(s, x)\,\mathcal{R}\,(s', x') \Longleftrightarrow \exists \sigma \in S \text{ tel que } \sigma s' x = \sigma s x' .$$

On observe que $\mathcal{R}$ est une relation d'équivalence. En effet, elle est clairement réflexive et symétrique. Soient (s, x), (s', x') et (s'', x'') trois éléments de $S \times A$, et supposons $(s, x)\,\mathcal{R}\,(s', x')$ et $(s', x')\,\mathcal{R}\,(s'', x'')$. Cela signifie qu'il existe σ, $\sigma' \in S$ vérifiant : $\sigma s' x = \sigma s x'$ et $\sigma' s'' x' = \sigma' s' x''$. Multipliant la première de ces identités par $\sigma' s''$ et la seconde par σs, il vient : $\sigma\sigma' s' s'' x = \sigma\sigma' s s'' x' = \sigma\sigma' s' s x''$, et comme $\sigma\sigma' s' \in S$, on a $(s, x)\,\mathcal{R}\,(s'', x'')$, d'où la transitivité de $\mathcal{R}$.
On note $S^{-1}A$ le quotient de $S \times A$ par la relation $\mathcal{R}$, et x/s la classe d'un élément (s, x) de $S \times A$. Les éléments de $S^{-1}A$ sont appelés des *fractions*. On observe que si (s, x) et (s', x') sont deux éléments de $S \times X$, les fractions $(s'x + sx')/(ss')$ et $(xx')/(ss)$ ne dépendent que des fractions x/s et x'/s'. Ainsi, on définit deux lois de composition interne $+$ et $\cdot$ sur $S^{-1}A$ en posant :

$$\frac{x}{s} + \frac{x'}{s'} = \frac{s'x + sx'}{ss'} \text{ et } \frac{x}{s} \cdot \frac{x'}{s'} = \frac{xx'}{ss'} .$$

D'autre part, notons η l'application

$$\begin{aligned} A &\longrightarrow S^{-1}[A] , \\ x &\mapsto x/1 . \end{aligned}$$

(*) La raison apparaîtra à ceux qui, ayant lu la remarque 2.5.3, feront l'exercice suivant.

2.5.1. Proposition-définition. *L'ensemble $S^{-1}A$, muni des lois $+$ et $\cdot$, est un anneau commutatif, et η est un morphisme d'anneaux. Ceci fait donc de $S^{-1}A$ une A-algèbre, appelée* algèbre des fractions de A à dénominateur dans S. *De plus, si $s \in S$, $\eta(s)$ est un élément inversible de $S^{-1}A$, d'inverse $1/s$.*

DEMONSTRATION. Simple vérification. On remarque tout d'abord qu'on a $a/s + b/s = (a+b)/s$. On peut donc simplifier les calculs comportant des additions en utilisant le principe de "réduction au même dénominateur" : si $u_1, \ldots, u_n$ sont des éléments de $S^{-1}A$, il existe $s \in S$ et des éléments $a_1, \ldots, a_n$ de A tels que $u_i = a_i/s$ pour tout $i = 1, \ldots, n$. Le zéro de $S^{-1}A$ est $0/1$, l'unité, $1/1$, et si $s \in S$, on a $(s/1)(1/s) = s/s = 1/1$. $\square$

La A-algèbre $S^{-1}A$ vérifie la propriété universelle suivante.

2.5.2. Proposition. *Soit A un anneau, et S une partie multiplicative de A. Pour toute A-algèbre B telle que l'image dans B de tout élément de S soit inversible, il existe un unique morphisme de A-algèbres de $S^{-1}A$ vers B.*

DEMONSTRATION. Soit $\eta' : A \longrightarrow B$ le morphisme d'anneaux qui fait de B une A-algèbre. Soit f un morphisme de A-algèbres de $S^{-1}A$ vers B. Alors pour $a \in A$, $f(\eta(a)) = f(a/1) = \eta'(a)$; et pour $s \in S$, $f(1/s) = f(\eta(s)^{-1}) = f(\eta(s))^{-1} = \eta'(s)^{-1}$, donc $f(a/s) = \eta'(a)\eta'(s)^{-1}$; d'où l'unicité d'un tel f. Inversement, cette formule, qui a bien un sens car $\eta'(s)$ est inversible dans B pour tout $s \in S$, définit un morphisme de A-algèbres de $S^{-1}A$ vers B. $\square$

2.5.3. REMARQUES.
1) Il faut prendre garde au fait que le morphisme η n'est pas toujours injectif. En effet, le noyau de η est $\{x \in A \text{ t. q. } \exists s \in S \mid sx = 0\}$. Ainsi η est injectif si et seulement si S ne contient aucun diviseur de zéro.
2) Si S ne contient aucun diviseur de zéro, on a

$$(s,x)\,\mathcal{R}\,(s',x') \Longleftrightarrow s'x = sx'\,.$$

Autrement dit, on retrouve le calcul de fractions "classique".
3) Si $0 \in S$, $S^{-1}A$ est l'anneau nul. Si $S \subset A^*$, η est un isomorphisme d'anneaux de A sur $S^{-1}A$.

EXERCICE. Soit $\mathcal{R}_0$ la relation sur $A \times S$:

$$(s,x)\,\mathcal{R}_0(s',x') \Longleftrightarrow s'x = sx'\,.$$

1) Montrer que si S contient un diviseur de 0, $\mathcal{R}_0$ n'est pas transitive.
2) Montrer que $\mathcal{R}$ est la plus petite relation d'équivalence sur $A \times S$ contenant $\mathcal{R}_0$.

2.5.4. Corps des fractions d'un anneau intègre

Soit A un anneau intègre. L'ensemble $A - \{0\}$ est une partie multiplicative de A (d'ailleurs, cette condition équivaut à l'intégrité de A).

2.5.5 Proposition-définition.
Soit A un anneau intègre.
1) L'anneau $\mathsf{Frac}\,A = (A-\{0\})^{-1}A$ *est un corps, appelé* corps des fractions de A. *L'anneau A s'identifie à un sous-anneau de* $\mathsf{Frac}\,A$ *via le morphisme d'anneaux injectif $a \longrightarrow a/1$.*
2) De plus si S est une partie multiplicative de A ne contenant pas 0, $S^{-1}A$ s'identifie au sous-anneau de $\mathsf{Frac}\,A$ *constitué des fractions x/s, pour $x \in A$ et $s \in S$.*
3) Pour tout corps K et tout morphisme d'anneaux injectif $j : A \hookrightarrow K$, il existe un unique morphisme d'anneaux de $\mathsf{Frac}\,A$ *vers K prolongeant j.*

DEMONSTRATION.
1) Soit $q = x/y$ un élément de $\mathsf{Frac}\,A$. On a $x/y = 0 \Longleftrightarrow x = 0$, en vertu de la remarque **2.5.3.** 2). Si $q \neq 0$, q est donc inversible, d'inverse y/x. Il résulte encore de **2.5.3** que le morphisme $\eta : A \longrightarrow \mathsf{Frac}\,A$ est injectif, ce qui permet d'identifier A à un sous-anneau de $\mathsf{Frac}\,A$.
2) Par la propriété universelle de $S^{-1}A$, il existe un unique morphisme de A-algèbres $S^{-1}A \longrightarrow \mathsf{Frac}\,A$. C'est l'application qui à la fraction x/s de $S^{-1}A$ associe la fraction x/s de $\mathsf{Frac}\,A$. Ce morphisme est injectif, car on a vu que $x/s = 0$ dans $\mathsf{Frac}\,A \Longrightarrow x = 0$; par conséquent on peut identifier $S^{-1}A$ à l'image de ce morphisme.
3) C'est une conséquence directe de la propriété universelle de $S^{-1}A$, appliquée à $S = A - \{0\}$. □

EXEMPLES Le corps $\mathsf{Frac}\,\mathbb{Z}$ n'est autre que $\mathbb{Q}$. Si K est un corps, le corps $\mathsf{Frac}(K[X])$ est le corps $K(X)$ des fractions rationnelles à coefficients dans K.

3. Anneaux euclidiens, principaux et factoriels

3.1. Divisibilité dans les anneaux intègres

Soit A un anneau intègre. Alors 0 est un idéal premier, autrement dit $A - \{0\}$ est une partie multiplicative de A.

3.1.1. Définitions. Soient x, y deux éléments de $A - \{0\}$. On dit que x *divise* y, ou que x est un *diviseur de* y, et on écrit $x \mid y$, s'il existe $z \in A - \{0\}$ tel que $y = xz$.
On a les équivalences $x \mid y \Longleftrightarrow y \in (x) \Longleftrightarrow (y) \subset (x)$.
La relation $\mid$ est une relation de préordre sur $A - \{0\}$ (autrement dit, elle est réflexive et transitive).
De plus si x, y, a sont des éléments non nuls de A, on a $x \mid y \Longleftrightarrow ax \mid ay$.
On dit que x est *associé à* y, et on écrit $x \sim y$, si on a $x \mid y$ et $y \mid x$. La relation $\sim$ est une relation d'équivalence.
On a $x \sim y \Longleftrightarrow (x) = (y) \Longleftrightarrow \exists u \in A^*$ t. q. $y = ux$.
On a pour tout $x \in A - \{0\}$: $1 \mid x$, et donc $x \mid 1 \Longleftrightarrow x \sim 1 \Longleftrightarrow x \in A^*$.

3.1.2. Définition. Un élément $f \in A - \{0\}$ est dit *irréductible* s'il vérifie : $f \notin A^*$ et $\forall x, y \in A - \{0\}$, $f = xy \Longrightarrow x \in A^*$ ou $y \in A^*$.

3.1.3. EXEMPLE L'anneau $\mathbb{Z}$ vérifie les propriétés suivantes.
— Dans $\mathbb{Z}$, on peut pratiquer la division euclidienne : si x, $y \in \mathbb{Z}$, avec $y \neq 0$, il existe un couple (q,r) unique, $q \in \mathbb{Z}$, $r \in \{0,1,\ldots,|y|-1\}$, tel que $x = qy + r$.
— Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{N}$. En effet, soit I un idéal de $\mathbb{Z}$, qu'on peut supposer non nul, et soit n le plus petit élément strictement positif de I ; on a $n\mathbb{Z} \subset I$. Soit $x \in I$; par division euclidienne, x s'écrit $qn + r$ avec $q \in \mathbb{Z}$ et $0 \leq r < n$. On a $r = x - qn \in I$, donc r doit être nul pour ne pas contredire le choix de n. Ainsi $x = qn \in n\mathbb{Z}$, d'où $I = n\mathbb{Z}$. Autrement dit tout idéal de $\mathbb{Z}$ est principal.
— Pour $n > 0$, $\mathbb{Z}/n\mathbb{Z}$ est intègre $\iff$ $\mathbb{Z}/n\mathbb{Z}$ est un corps $\iff$ n est un nombre premier.
— $\mathbb{Z}^* = \{+1,-1\}$, et les irréductibles de $\mathbb{Z}$ sont les $\pm p$, p décrivant l'ensemble des nombres premiers.
— Tout élément non nul de $\mathbb{Z}$ s'écrit au signe près comme un produit fini de nombre premiers,(*) et ce, de façon unique à l'ordre près.
Nous allons à présent étudier certaines classes d'anneaux vérifiant tout ou partie de ces propriétés de $\mathbb{Z}$.

3.2. Anneaux noethériens — Anneaux principaux et factoriels

3.2.1. Proposition-définition. *Soit A un anneau (commutatif). Les deux conditions suivantes sont équivalentes :*
(i) toute suite croissante d'idéaux de A est stationnaire;
(ii) tout idéal de A est de type fini, c'est-à-dire engendré par une partie finie de A.
On dit que A est noethérien *s'il vérifie (i) ou (ii).*

DEMONSTRATION.
(i) $\Longrightarrow$ (ii). Si un idéal I de A n'est pas de type fini, on peut construire une suite $(x_n)_{n\in\mathbb{N}}$ telle qu'on ait pour tout n : $x_n \in I$ et $x_{n+1} \notin (x_0,\ldots,x_n)$. Soit $I_n = (x_0,\ldots,x_n)$. Alors $(I_n)_{n\in\mathbb{N}}$ est une suite strictement croissante d'idéaux de A, ce qui contredit (i).
(ii) $\Longrightarrow$ (i). Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A, et $I = \bigcup I_n$ sa réunion. C'est un idéal de A (cf. lemme **2.4.5**), donc il est de la forme $(x_1,\ldots,x_m)$. La suite des I_n étant croissante, il existe N tel que pour tout $k = 1,\ldots,m$ on ait $x_k \in I_N$; on a donc $I_N = I$, et la suite des I_n est stationnaire à partir de $n = N$. □

3.2.2. Définition. Un anneau A est dit *principal* s'il est intègre, et si tous ses idéaux sont principaux.

REMARQUE. Tout anneau principal est noethérien, car il vérifie la condition (ii) de **3.2.1.**

ILLUSTRATION On a vu que $\mathbb{Z}$ est principal.
Par contre, l'anneau $A = \mathbb{Z}[X]$ ne l'est pas. En effet, considérons l'idéal $I = (2,X)$ de A. On a $I \neq A$, car le coefficient de degré 0 de tout élément de I est pair. Supposons qu'il existe $P \in A$ tel que $(P) = I$. Alors $2 = PQ$ pour un certain $Q \in A$. On a $0 = \deg 2 = \deg P + \deg Q$, donc $P \in \mathbb{Z}$. D'autre part $P \mid X$, donc l'entier P divise les coefficients de X. On a donc $P = \pm 1$, et $(P) = A \neq I$, d'où contradiction.

(*) Étant entendu que le produit de la famille vide vaut 1.

3.2.3. Définition. Soit A un anneau intègre. On dit que A est *factoriel* s'il vérifie les deux conditions suivantes :

(F1) tout élément non nul de A est associé à un produit fini[(*)] d'éléments irréductibles;

(F2) soient m, $n \in \mathbb{N}$, $p_1, \ldots, p_m$ et $q_1, \ldots, q_n$ des éléments irréductibles de A. Si le produit des p_i et le produit des q_j sont associés, alors $m = n$, et on peut renuméroter les q_j de sorte qu'on ait $p_i \sim q_i$ pour tout $i = 1, \ldots, m$.

3.2.4. Proposition-définition. *Soit A un anneau factoriel.*
1) Soit p un élément irréductible de A. Soit $a \in A - \{0\}$. Alors il existe un entier naturel n unique tel qu'on ait

$$a = \alpha p^n \ \textit{avec}\ \alpha \in A - (p) \quad .$$

On appelle valuation p-adique *de a, et on note $\nu_p(a)$, cet entier n. On pose $\nu_p(0) = -\infty$.*
2) On a pour p irréductible et $a, b \in A$: $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.
3) Soit $\mathcal{P}$ un ensemble d'éléments irréductibles de A tel que pour tout élément irréductible f de A, il existe un unique $p \in \mathcal{P}$ vérifiant $f \sim p$. On dira alors que $\mathcal{P}$ est un système de représentants des irréductibles de A.
Pour tout élément non nul a de A, la famille $(\nu_p(a))_{p\in \mathcal{P}}$ est presque nulle, et a s'écrit :

$$x = u \prod_{p\in \mathcal{P}} p^{\nu_p(a)}, \ \textit{avec}\ u \in A^* \quad .$$

Demonstration. Choisissons un système de représentants des irréductibles $\mathcal{P}$. Il résulte de la factorialité de A que tout $a \in A - \{0\}$ s'écrit de façon unique $x = u \prod_{p\in P} p^n(p)$, avec $u \in A^*$, les $n(p)$ étant des entiers naturels presque tous nuls. On a $a = \alpha p^{n(p)}$, où $\alpha = u \prod_{q\in \mathcal{P}-\{p\}} q^{n(q)}$ n'est pas multiple de p. Ainsi $n(p) = \nu_p(a)$. Le reste se vérifie sans peine. □

La définition d'un anneau factoriel que nous avons adoptée s'avère souvent utile lorsqu'on sait qu'un anneau est factoriel et qu'on veut exploiter cette information, mais il est en général malaisé de vérifier qu'un anneau satisfait aux conditions (F1) et (F2).
Il y a un critère plus facile à mettre en œuvre pour démontrer qu'un anneau est factoriel.

Définition. Soit A un anneau intègre, et p un élément non nul de On dit que p est *premier* si l'idéal (p) est premier. Cela équivaut à dire que p n'est pas inversible et satisfait la condition :

$$\forall a, b \in A, p \mid ab \Longrightarrow p \mid a \text{ ou } p \mid b.$$

3.2.5. Proposition. *Soit A un anneau intègre.*
1) Tout élément premier de A est irréductible.
2) L'anneau A est factoriel si et seulement si les deux conditions suivantes sont remplies :
(F'1) toute suite croissante d'idéaux principaux de A est stationnaire;
(F'2) Tout élément irréductible de A est premier.

[(*)] Rappelons que 1 est le produit de la famille vide.

Remarque. La condition (F'1) est automatique si A est noethérien. Or, la plupart des anneaux que l'on manipule habituellement sont noethériens, pour des raisons d'ordre tout à fait général (voir les résultats de la section **II, 2.3**).
Ainsi, le plus souvent, l'étude de la factorialité d'un anneau se ramène à déterminer si les éléments irréductibles sont premiers.

Demonstration.
1) Soit $f \in A - \{0\}$, et supposons (f) premier. On a $(f) \neq A$, donc $f \notin A^*$. D'autre part si $f = xy$, alors $xy \in (f)$ donc x ou $y \in (f)$. Par exemple, $x \in (f)$. Alors $x \mid f$ et $f \mid x$, i. e. $x \sim f$, donc y est inversible, ce qui démontre l'irréductibilité de f.
2) On procède par étapes.
(i) (F'1) $\Longrightarrow$ (F1).
Nous dirons qu'un élément non nul f de A est *décomposable* s'il est associé à un produit fini d'irréductibles de A. L'assertion (F1) affirme que tout élément non nul est décomposable. Soit f_0 un élément non décomposable. N'étant ni inversible, ni irréductible, f_0 est produit de deux éléments non inversibles, dont l'un au moins n'est pas décomposable. Il existe donc f_1 non décomposable tel que $(f_0) \subset (f_1)$ et $(f_0) \neq (f_1)$. Itérant ce processus, on construit une suite strictement croissante d'idéaux principaux, ce qui contredit (F'1).
(ii) (F'2) $\Longrightarrow$ (F2). Supposons $p_1 p_2 \cdots p_m \sim q_1 q_2 \cdots q_n$, et montrons : $n = m$ et, quitte à renuméroter les q_j, $q_i \sim p_i$.
On procède par récurrence sur m. Pour $m = 0$, c'est clair : si le produit des q_j est inversible, chacun des q_i est inversible; et puisqu'ils sont irréductibles, $n = 0$.
Soit $m > 0$, et montrons comment l'on passe de $m-1$ à m. Supposons $p_1 p_2 \cdots p_m \sim q_1 q_2 \cdots q_n$. Puisque p_m est premier et divise le produit des q_j, il divise l'un d'entre eux. Quitte à renuméroter les q_j, on peut supposer que c'est q_n. On a donc $p_m \sim q_n$, et $p_1 p_2 \cdots p_{m-1} \sim q_1 q_2 \cdots q_{n-1}$. On conclut alors par récurrence.
(iii) A factoriel $\Longrightarrow$ (F'1).
Supposons A factoriel et soient $a, b \in A - \{0\}$. Choisissons un système de représentants des irréductibles $\mathcal{P}$. Alors d'après 3.2.4, $b \mid a$ si et seulement si pour tout $p \in \mathcal{P}$, $\nu_p(b) \leq \nu_p(a)$. Puisque $\nu_p(a)$ est nul sauf pour un nombre fini de valeurs de p, a admet un nombre fini de diviseurs à association près.
Autrement dit, l'ensemble des ideaux principaux contenant (a) est fini. Il n'existe donc pas de suite strictement croissante d'idéaux principaux.
(iv) A factoriel $\Longrightarrow$ (F'2). Soit p un irréductible de A; il n'est pas inversible, donc $(p) \neq A$. D'autre part soient x, $y \in A - (p)$, On a donc $\nu_p(x) = \nu_p(y) = 0$, et par **3.2.4,** $\nu_p(xy) = 0$ donc donc $xy \notin (p)$. $\square$

3.2.6. Corollaire. *Tout anneau principal est factoriel.*

Demonstration.
Soit A principal. Puisqu'il est noethérien, il vérifie (F'1). Reste à montrer (F'2). Soit f un élément irréductible de A. On a $(f) \neq A$. D'autre part soient x, $y \in A$ tels que $f \mid xy$, et montrons $f \mid x$ ou $f \mid y$. Soit $I = \{u \in A \text{ t. q. } f \mid uy\}$. Alors I est un idéal de A, donc de la forme (a) avec $a \in A$. On a $f \in I$, donc $a \mid f$. Par conséquent $a \sim 1$ ou $a \sim f$. Si $a \sim 1$, $I = A$ donc $f \mid y$. Sinon, $I = (f)$. Or $x \in I$, puisque $f = xy$, donc $f \mid x$. Ainsi (f) est premier. $\square$

3.2.7. Corollaire. *Soit A un anneau principal. Les idéaux premiers de A sont l'idéal nul, et les idéaux engendrés par les éléments irréductibles de A.*
Si A n'est pas un corps, les idéaux maximaux de A sont les idéaux engendrés par les éléments irréductibles de A.

DEMONSTRATION. Résulte immédiatement de ce qui précède. □

REMARQUE. On peut formuler la définition d'un anneau factoriel de manière bien plus agréable conceptuellement. Soit A un anneau intègre, et $K = \mathsf{Frac}\, A$. Alors A^* est un sous-groupe de K^*; notons $\mathsf{Div}(A)$ le groupe quotient K^*/A^*, et $\mathsf{div} : K^* \longrightarrow \mathsf{Div}\, A$ la surjection canonique. Le groupe $\mathsf{Div}(A)$ est appelé *groupe des diviseurs de A*.
Soit $\mathsf{Div}^+(A)$ l'image par div de $A - \{0\}$; $\mathsf{Div}^+(A)$ n'est autre que l'ensemble des classes d'éléments de $A - \{0\}$ modulo $\sim$. Les éléments de $\mathsf{Div}^+(A)$ sont appelés *diviseurs effectifs*.
Enfin notons $\mathsf{Irr}(A) \subset \mathsf{Div}^+(A)$ l'ensemble des classes d'éléments irréductibles de A modulo $\sim$.
Soit Γ le morphisme de groupes

$$\begin{aligned} \mathbb{Z}^{(\mathsf{Irr}(A))} &\longrightarrow \mathsf{Div}(A) \\ (n_p)_{p \in \mathsf{Irr}(A)} &\longmapsto \prod_{p \in \mathsf{Irr}(A)} p^{n_p} \,; \end{aligned}$$

On observe que si les n_p sont des entiers naturels, $\Gamma((n_p)_{p \in \mathsf{Irr}(A)}) \in \mathsf{Div}^+(A)$. Par conséquent Γ induit par restriction une application

$$\Gamma^+ : \mathbb{N}^{(\mathsf{Irr}(A))} \longrightarrow \mathsf{Div}^+(A)\,.$$

Avec ces notations, A vérifie (F1) (resp. (F2)) $\Longleftrightarrow$ Γ^+ est surjective (resp. injective). En particulier A est factoriel $\Longleftrightarrow$ Γ^+ est une bijection. En outre, si A est factoriel, Γ est un isomorphisme de groupes.

3.3. Eléments premiers entre eux, PGCD, PPCM

Soit A un anneau.

3.3.1. Définition. Soient $x_1, x_2, \ldots, x_n$ des éléments de A. On dit que les x_i sont *premiers entre eux* si A est le plus petit idéal principal qui les contienne tous. Si deux éléments x et y sont premiers entre eux, on dit aussi que x est *premier à y* (et réciproquement).

3.3.2. Définitions. Soient x, y deux éléments de A. On appelle *plus grand commun diviseur,* ou *PGCD de x et y* tout élément c de A tel que (c) soit le plus petit idéal principal de A contenant $(x) + (y)$. On appelle *plus petit commun multiple,* ou *PPCM de x et de y* tout élément d de A tel que $(d) = (x) \cap (y)$.
Un PGCD (resp. un PPCM) de x et de y n'existe pas toujours; mais s'il existe, il est unique à association près. On le note alors $x \wedge y$ (resp. $x \vee y$). Notons que 1 est PGCD de x et de y si et seulement si x et y sont premiers entre eux.

3.3.3. Proposition. *Soit A un anneau factoriel.*
1) Les PGCD et les PPCM existent dans A.
2) Si x et y sont deux éléments non nuls de A, posons $\delta = x \wedge y$, $x_0 = x/\delta$ et $y_0 = y/\delta$. Alors x_0 et y_0 sont des éléments de A premiers entre eux, et $x \vee y \sim x_0 y_0 \delta$, de sorte qu'on a $xy \sim (x \wedge y)(x \vee y)$.
3) Si x, y, z sont trois éléments non nuls de A, on a :

$$x \mid yz \text{ et } x \text{ premier à } z \implies x \mid y\,.$$

DEMONSTRATION.
1) Si $x = 0$, on a $x \wedge y \sim y$ et $x \vee y \sim 0$. On peut donc supposer x et y non nuls. On utilise le lemme **3.2.4.** Soit $\mathcal{P}$ un système de représentants des irréductibles de A. Soit $z \in A - \{0\}$. Alors $(z) \in (x) \cap (y) \iff \forall p \in \mathcal{P}\,, \nu_p(x) \leq \nu_p(z)$ et $\nu_p(y) \leq \nu_p(z)$. Ainsi,

$$\prod_{p \in \mathcal{P}} p^{\sup(\nu_p(x), \nu_p(y))}$$

est un PPCM de x et y.
De même, $(x) + (y) \subset (z) \iff \forall p \in \mathcal{P}\,, \nu_p(x) \geq \nu_p(z)$ et $\nu_p(y) \geq \nu_p(z)$, donc

$$\prod_{p \in \mathcal{P}} p^{\inf(\nu_p(x), \nu_p(y))}$$

est un PGCD de x et y.
2) Résulte immédiatement de 1), ainsi que 3). □

3.3.4. REMARQUE. Dans un anneau factoriel, on a donc $x \wedge y \sim y \wedge x$, $(x \wedge y) \wedge z \sim x \wedge (y \wedge z)$, et $(xz) \wedge (yz) \sim (x \wedge y)z$. En particulier on peut former le PGCD d'une famille finie d'éléments de A. L'opération $\vee$ vérifie les mêmes propriétés.

3.3.5. Théorème. (Bezout)
Soit A un anneau principal. Soient x, $y \in A$. Alors il existe u, $v \in A$ tels que $ux + vy \sim x \wedge y$. En particulier, x et y sont premiers entre eux si et seulement s'il existe u, $v \in A$ tels que $ux + by = 1$.

DEMONSTRATION. Il est clair que si (x, y) est un idéal principal, un générateur de cet idéal est un PGCD de x et y. C'est toujours le cas si A est principal. □

3.3.6. Proposition. (Lemme Chinois)
Soit A un anneau, et I, J deux idéaux de A vérifiant $I + J = A$. Alors les anneaux $A/(I \cap J)$ et $A/I \times A/J$ sont isomorphes.
En particulier, si A est principal et si f, g sont deux éléments de A premiers entre eux, on a $A/(fg) \simeq A/(f) \times A/(g)$.

DEMONSTRATION. Soient $\pi : A \longrightarrow A/I$ et $\pi' : A \longrightarrow A/J$ les surjections canoniques, et soit ϕ le morphisme d'anneaux

$$\begin{aligned} A &\longrightarrow A/I \times A/J \\ x &\longrightarrow (\pi(x), \pi'(x)). \end{aligned}$$

On a $\operatorname{Ker}\phi = I \cap J$, donc ϕ induit par passage au quotient un morphisme injectif $\widetilde{\phi}$: $A/(I \cap J) \hookrightarrow A/I \times A/J$, ayant même image que ϕ. Or $I + J = A$, donc il existe $u \in J$, $v \in I$, tels que $1 = u + v$. On a donc

$$u \equiv 1 \ (I), \quad u \equiv 0 \ (J), \quad v \equiv 0 \ (I), \quad v \equiv 1 \ (J).$$

Tou élément de $A/I \times A/J$ est de la forme $(\pi(x), \pi'(y))$ avec x, $y \in A$, car π et π' sont surjectives. Or on a $\phi(ux + vy) = (\pi(ux + vy), \pi'(ux + vy)) = (\pi(x), \pi'(y))$ car $ux + vy \equiv x \ (I)$ et $ux + vy \equiv y \ (J)$, d'où la surjectivité de ϕ.
Le cas particulier résulte immédiatement de Bezout, et du fait que si $f \wedge g \sim 1$, $fg \sim f \vee g$ (cf. **3.3.3**). □

3.4. Anneaux euclidiens

3.4.1. Définition. Soit A un anneau intègre. On dit que A est *euclidien* s'il existe une application $N : A \longrightarrow \mathbb{N}$ vérifiant :

— $\forall x \in A,\ N(x) = 0 \Longleftrightarrow x = 0$;
— $\forall x \in A, \forall y \in A - \{0\},\ \exists q, r \in A$ tels que $x = qy + r$, avec $N(r) < N(y)$.

3.4.2. EXEMPLES.

1) L'anneau $\mathbb{Z}$ des entiers rationnels

est euclidien (pour $N(x) = |x|$, cf. **3.1.3**).

2) L'anneau des entiers de Gauss

C'est l'ensemble, noté $\mathbb{Z}[i]$, des nombres complexes de la forme $a + ib$, avec a, $b \in \mathbb{Z}$. On vérifie sans peine que c'est un sous-anneau de $\mathbb{C}$, et à ce titre, il est intègre.
Soit $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$ l'application $z = a + ib \mapsto N(z) = z\bar{z} = |z|^2 = a^2 + b^2$.
Montrons que cette fonction fait de $\mathbb{Z}[i]$ un anneau euclidien.
On a clairement $N(z) = 0 \Longleftrightarrow z = 0$.
On observe que si ξ est un nombre complexe, il existe $z \in \mathbb{Z}[i]$ tel que $|\xi - z|^2 \leq 1/2$. En effet, ξ s'écrit $x + iy$, avec x, $y \in \mathbb{R}$. Soit a la partie entière de $x - 1/2$, et b celle de $y - 1/2$. On a $|x - a| \leq 1/2$ et $|y - b| \leq 1/2$, donc si on pose $z = a + ib$, $|\xi - z|^2 \leq 1/4 + 1/4 = 1/2$.
Soient x, $y \in \mathbb{Z}[i]$, avec $y \neq 0$. Appliquons ce qui précède à $\xi = x/y$; il existe $q \in \mathbb{Z}[i]$ tel que $|\xi - q|^2 \leq 1/2$. Posons $r = x - qy$; on a donc $x = qy + r$, avec $r \in \mathbb{Z}[i]$, et $N(r) = |x - qy|^2 = |\xi - q|^2 |y|^2 \leq 1/2 N(y) < N(y)$, ce qui montre que $\mathbb{Z}[i]$ est un anneau euclidien.

REMARQUE.
1) Dans ce cas, il n'y a pas unicité du couple (q, r) (par exemple, $1 + i = 0 \cdot 2 + (1 + i) = 1 \cdot 2 + (-1 - i)$, avec $N(1 + i) = N(-1 + i) = 2 < N(2) = 4$).
2) La fonction $N : \mathbb{Z}[i] \to \mathbb{N}$ vérifie $N(xy) = N(x)N(y)$ et $N(1) = 1$, ce qui nous sera utile plus tard.

3) L'anneau $K[X]$.

Soit K un corps. Pour $P \in K[X]$, posons $N(P) = \deg P + 1$ si $P \neq 0$, 0 sinon. Cette fonction fait de N un anneau euclidien. En effet, on a $N(P) = 0 \iff P = 0$ par construction, et la seconde condition résulte immédiatement de la proposition suivante.

3.4.3. Proposition. (Division euclidienne dans $A[X]$) *Soit A un anneau non nul, $P \in A[X]$ un polynôme, et $T \in A[X]$ un polynôme dont le coefficient directeur est inversible. Alors il existe un couple unique $(Q, R) \in A[X]^2$ vérifiant $P = TQ + R$, avec $\deg R < \deg T$.*

DEMONSTRATION. Posons $t = \deg T$.
1) Unicité : supposons $TQ + R = TQ' + R'$, avec $\deg R$ et $\deg R' < t$. On a $R' - R = T(Q - Q')$. Or, le coefficient directeur de T étant inversible, $\deg T(Q - Q') = t + \deg(Q - Q')$; et d'autre part, $\deg(R' - R) < t$; d'où $Q - Q' = 0$, et $R = R'$.
2) Existence : on procède par récurrence sur le degré n de P. Si $n < t$, $R = P$ et $Q = 0$ conviennent. Plaçons-nous dans le cas $n \geq t$, et supposons l'existence acquise pour un degré moindre. Soit a le coefficient directeur de P, et u celui de T, supposé inversible. Alors $P - (a/u)X^{n-t}T$ est de degré $< n$, donc de la forme $TQ_0 + R$, avec $\deg R < t$. Ainsi $P = T(Q_0 + (a/u)X^{n-t}) + R$, ce qui achève la démonstration. □

REMARQUES.
1) On a $P \in (T) \iff R = 0$.
2) Le polynôme T n'est pas un diviseur de 0 dans $A[X]$.
3) Le cas $T = X - a$, $a \in A$ est particulièrement intéressant : pour tout $P \in A[X]$, il existe $Q \in A[X]$ et $r \in A$ uniques tels qu'on ait $P = Q(X - a) + r$. On a $r = P(a)$. En particulier, on a :

$$P \in (X - a) \iff P(a) = 0 .$$

L'application $P \mapsto P(a)$ induit par passage au quotient un isomorphisme d'anneaux $A[X]/(X - a) \xrightarrow{\sim} A$.

3.4.4. Théorème. *Tout anneau euclidien est principal.*

DEMONSTRATION. Soit A euclidien, et N une fonction comme dans la définition **3.4.1.** Soit I un idéal de A, supposé non nul, et y un élément non nul de I minimisant N. On a $(y) \subset I$. Soit $x \in I$. Il existe q, $r \in A$ avec $x = qy + r$, $N(r) < N(y)$. Puisque $r = x - qy$, r est un élément de I; il vérifie $N(r) < N(y)$, donc il est nul (car sinon il contredirait le choix de y); ainsi on a $x \in (y)$, d'où $I = (y)$. □

3.4.5. Algorithme d'euclide.

Soit A un anneau euclidien, et N une fonction comme dans la définition **3.4.1.** Soient x et y deux éléments de A. Le procédé suivant permet de calculer le PGCD de x et y.
Quitte à échanger les rôles de x et y, on peut supposer $N(x) \geq N(y)$. Si $x = 0$, $y = 0$ et le PGCD est nul.
Supposons $x \neq 0$.

On construit une suite finie d'éléments de A

$$x_0 = x, x_1 = y, x_2, \dots, x_N, x_{N+1} = 0$$

par récurrence. Si $x_0, \dots, x_n$ sont déja construits, et si $x_n = 0$, on pose $N = n - 1$ et on s'arrête là. Si par contre x_n est non nul, on choisit des éléments q_n et $x_{n+1} \in A$ vérifiant

$$x_{n-1} = q_n x_n + x_{n+1}$$

avec $N(x_{n+1}) < N(x_n)$. La suite des $N(x_n)$ est strictement décroissante à partir de $n = 1$, donc la construction s'arrête au bout d'un nombre fini d'étapes.
Alors $\delta = x_N$ est un PGCD de x et y. En effet, on a pour tout $n = 1, \dots, N$: $(x_{n-1}, x_n) = (x_n, q_n x_n + x_{n+1}) = (x_n, x_{n+1})$, donc $(x, y) = (x_0, x_1) = (x_N, x_{N+1}) = (\delta)$.

Ce procédé permet aussi de déterminer des éléments u, $v \in A$ tels que $\delta = ux + vy$. Si $q \in A$, notons M_q la matrice inversible $\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}$. On a pour $n = 1, \dots, N$:

$$\begin{pmatrix} x_{n-1} \\ x_n \end{pmatrix} = M_{q_n} \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix},$$

donc

$$\begin{pmatrix} x \\ y \end{pmatrix} = M_{q_1} M_{q_2} \cdots M_{q_N} \begin{pmatrix} \delta \\ 0 \end{pmatrix}.$$

Soit

$$\begin{pmatrix} u & v \\ u' & v' \end{pmatrix} = M_{q_N}^{-1} \cdots M_{q_1}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_N \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix};$$

alors on a : $\delta = ux + vy$.

3.5. Etude de quelques anneaux

3.5.1. L'anneau $K[X]$

Soit K un corps. On a vu que $K[X]$ est euclidien; il est donc principal. Les éléments inversibles de $K[X]$ sont les polynômes de degré 0, c'est-à-dire les constantes non nulles. Tout idéal non nul de $K[X]$ est donc engendré par un polynôme unitaire unique. En particulier, l'étude des polynômes irréductibles se ramène à celle des polynômes unitaires irréductibles.
Soit P un polynôme unitaire de degré $d \geq 1$.
a) Si $d = 1$, P est irréductible; P est alors de la forme $X - a$, avec $a \in K$.
b) Si $d \geq 2$, et si P admet une racine, P n'est pas irréductible. En effet,

$$P(a) = 0 \Longrightarrow X - a \mid P.$$

c) Si $d = 2$ ou 3, P est irréductible $\Longleftrightarrow$ P n'admet pas de racine dans K. En effet, si P était réductible, il s'écrirait $P = QR$ avec $1 \leq \deg Q \leq \deg R$, et $\deg Q + \deg R \leq 3$, donc $\deg Q = 1$ et Q admettrait une racine dans K, ainsi que P.

On sait par le théorème de d'Alembert que tout polynôme non constant à coefficients dans $\mathbb{C}$ admet une racine complexe. Il résulte de a) et b) que dans $\mathbb{C}[X]$, les polynômes irréductibles unitaires sont les seuls $X-a$, $a \in \mathbb{C}$.
Dans $\mathbb{R}[X]$, les $X-a$ $(a \in \mathbb{R})$ sont irréductibles, ainsi que les polynômes de la forme $X^2-2aX+b$ $(a,\ b \in \mathbb{R})$ sans racines réelles (ce qui équivaut à la condition $a^2 < b$). Il n'y a pas d'autres polynômes irréductibles unitaires. En effet, si P est de degré > 2, il admet une racine complexe z. Si $z \in \mathbb{R}$, on conclut par b). Sinon, $\bar{z}$ est aussi une racine de P, donc $Q=(X-z)(X-\bar{z})$ divise P dans $\mathbb{C}[X]$. Mais $Q = X^2-(z+\bar{z})X+z\bar{z} \in \mathbb{R}[X]$ donc Q divise P dans $\mathbb{R}[X]$.
Observons que $(X^2+1)^2$ n'a pas de racines dans $\mathbb{R}$, mais il n'est pas pour autant irréductible dans $\mathbb{R}[X]$.
Le cas de $\mathbb{Q}[X]$ est bien plus compliqué : nous verrons plus loin que dans $\mathbb{Q}[X]$, il existe des polynômes irréductibles en tout degré ≥ 1.

3.5.2. Les entiers de Gauss revisités

On a vu que l'anneau $\mathbb{Z}[i]$ est euclidien, pour la fonction

$$N : z = a+ib \longrightarrow N(z) = z\bar{z} = |z|^2 = a^2+b^2 \in \mathbb{N},$$

qui vérifie en outre $N(xy) = N(x)N(y)$ et $N(1) = 1$.
Il est donc principal, et a fortiori factoriel.
Soit $z = a+ib$ un élément inversible de $\mathbb{Z}[i]$; on a $N(z)N(z^{-1}) = N(zz^{-1}) = N(1) = 1$, donc $a^2+b^2 = N(z) = 1$. Ceci équivaut à $a = \pm 1$ et $b = 0$, ou $a = 0$ et $b = \pm 1$. Inversement si $N(z) = 1$, $z\bar{z} = 1$ donc $\bar{z} = a-ib$ est un inverse de z.
On a donc

$$\mathbb{Z}[i]^* = \{1, i, -1, -i\}\,.$$

Quels sont les éléments irréductibles de $\mathbb{Z}[i]$?
Soit f un tel élément. L'idéal $(f) = \mathbb{Z}[i]f$ est premier, car $\mathbb{Z}[i]$ est factoriel.

3.5.3. Proposition. *Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Si $\mathfrak{p}$ est un idéal premier de B, $f^{-1}(\mathfrak{p})$ est un idéal premier de A.*

DEMONSTRATION. Soit π la surjection canonique $B \longrightarrow B/\mathfrak{p}$. Le morphisme $\pi \circ f : A \longrightarrow B/\mathfrak{p}$ a pour noyau $f^{-1}(\mathfrak{p})$, donc induit un morphisme d'anneaux injectif

$$A/f^{-1}(\mathfrak{p}) \longrightarrow B/\mathfrak{p}\,.$$

Ainsi $A/f^{-1}(\mathfrak{p})$, isomorphe à un sous-anneau de l'anneau intègre $B/\mathfrak{p}$, est intègre lui aussi; d'où la proposition. □

On applique **3.5.3.** à l'inclusion de $\mathbb{Z}$ dans $\mathbb{Z}[i]$: $\mathbb{Z} \cap (f)$ est un idéal premier de $\mathbb{Z}$. Il n'est pas nul, car il contient $f\bar{f} = N(f)$; il est donc de la forme $\mathbb{Z}p$, pour un certain nombre premier p.
On a $p \in (f)$, donc il existe $g \in \mathbb{Z}[i]$ tel que $p = fg$. Ainsi $p^2 = N(p) = N(f)N(g)$, et puisque f n'est pas inversible, $N(f) \neq 1$, donc on a soit $N(f) = p$, soit $N(f) = p^2$.

Si $N(f) = f\bar{f} = p^2$, f, étant irréductible, divise p dans $\mathbb{Z}[i]$. Ainsi, f est associé à p, et en particulier p est irréductible dans $\mathbb{Z}[i]$.
Si par contre $N(f) = p$, $p = f\bar{f}$ n'est pas un élément irréductible de $\mathbb{Z}[i]$.

Quels sont les nombres premiers p qui sont irréductibles dans $\mathbb{Z}[i]$?

Si p est irréductible, il n'est pas de la forme $(a+ib)(a-ib) = a^2+b^2$. Si p n'est pas irréductible, soit $f = a+ib$ un facteur irréductible de p : d'après la discussion qui précède, $p = N(f) = a^2+b^2$.
Ainsi p est irréductible dans $\mathbb{Z}[i] \iff$ l'équation $a^2+b^2 = p$ n'admet pas de solutions dans $\mathbb{Z}^2$. Par exemple, $2 = 1^2+1^2 = (1+i)(1-i)$ n'est pas irréductible, non plus que $5 = 2^2+1^2$, mais 3, lui, est irréductible.
D'autre part, p est un irréductible de $\mathbb{Z}[i] \iff$ l'anneau $\mathbb{Z}[i]/(p)$ est intègre. Pour pouvoir en dire plus, nous aurons besoin d'une autre description de l'anneau $\mathbb{Z}[i]$.
Soit ψ le morphisme d'anneaux $\mathbb{Z}[X] \longrightarrow \mathbb{Z}[i]$, $P \mapsto P(i)$. L'image de ψ est $\mathbb{Z}[i]$, et son noyau, l'idéal de $\mathbb{Z}[X]$ engendré par X^2+1. En effet, tout $P \in \mathbb{Z}[X]$ s'écrit de manière unique (dans la division euclidienne par X^2+1) $P = Q(X^2+1)+R$, avec Q, $R \in \mathbb{Z}[X]$ et $\deg R < 2$; R est de la forme $aX+b$, avec a, $b \in \mathbb{Z}$. On a $P(i) = R(i) = ai+b$, donc $P(i) = 0 \iff R = 0 \iff P$ est un multiple de X^2+1.
Autrement dit, $\mathbb{Z}[i]$ s'identifie au quotient de l'anneau $\mathbb{Z}[X]$ par l'idéal engendré par le polynôme X^2+1.

3.5.4. Proposition. *Soit A un anneau, et I, J deux idéaux de A. Soit $\overline{J}$ l'image de J par la surjection canonique $A \longrightarrow A/I$. Alors l'anneau $A/(I+J)$ est isomorphe à $(A/I)/\overline{J}$.*

DEMONSTRATION. Soit π la surjection canonique $A \longrightarrow A/I$, et π' la surjection canonique $A/I \longrightarrow (A/I)/\overline{J}$; alors $p = \pi' \circ \pi$ est un morphisme d'anneaux surjectif $A \longrightarrow (A/I)/\overline{J}$; d'où un isomorphisme $A/\operatorname{Ker} p \xrightarrow{\sim} (A/I)/\overline{J}$. Or $x \in \operatorname{Ker} p \iff \pi(x) \in \overline{J} \iff \exists z \in J$ t. q. $\pi(x) = \pi(z) \iff \exists y \in I, z \in J$ t. q. $x = y+z$. Autrement dit, $\operatorname{Ker} p = I+J$. □

Appliquant **3.5.4** à $A = \mathbb{Z}[X]$, $I = A(X^2+1)$ et $J = pA$, il vient un isomorphisme

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[X]/(p, X^2+1)$$

puis, appliquant à nouveau **3.5.4** en échangeant cette fois les rôles de I et J, il vient un isomorphisme

$$\mathbb{Z}[X]/(p, X^2+1) \simeq (\mathbb{Z}[X]/p\mathbb{Z}[X])/(X^2+1).$$

3.5.5. Proposition. *Soit A un anneau, et I un idéal de A. Alors un a un isomorphisme d'anneaux*

$$(A/I)[X] \simeq A[X]/IA[X],$$

où $IA[X]$ désigne l'idéal engendré par I dans $A[X]$.

Demonstration. Notons $x \mapsto \overline{x}$ la surjection canonique $A \longrightarrow A/I$, et soit Π le morphisme d'anneaux

$$\begin{aligned} A[X] &\longrightarrow (A/I)[X] \\ P = \sum_{n\in\mathbb{N}} a_n X^n &\longmapsto \overline{P} = \sum_{n\in\mathbb{N}} \overline{a_n} X^n \,. \end{aligned}$$

Alors Π est clairement surjectif, et le noyau de Π est l'ensemble des polynômes dont les coefficients sont tous dans I; c'est précisément l'idéal engendré par I dans $A[X]$. D'où par passage au quotient l'isomorphisme annoncé. $\square$

Par **3.5.5,** on a $\mathbb{Z}[X]/(p) \simeq (\mathbb{Z}/p\mathbb{Z})[X]$; notant $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, et mettant bout à bout tous ces isomorphismes, on en déduit :

$$\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2+1)\,.$$

On a donc les équivalences suivantes :
p est un irréductible de $\mathbb{Z}[i] \iff \mathbb{Z}[i]/(p)$ est intègre $\iff \mathbb{F}_p[X]/(X^2+1)$ est intègre $\iff X^2+1$ est irréductible dans $\mathbb{F}_p[X] \iff X^2+1$ n'a pas de racines dans $\mathbb{F}_p \iff -1$ n'est pas un carré dans $\mathbb{F}_p$.
Ce qui nous ramène à la question : -1 est-il un carré dans le corps $\mathbb{F}_p$?

3.5.6. Proposition. *Soit p un nombre premier impair, et x un élément non nul de $\mathbb{F}_p$. Alors x est un carré dans $\mathbb{F}_p$ si et seulement si $x^{(p-1)/2} = 1$. En particulier, -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv 1 \ (4)$.*

Demonstration. Soit G le groupe ${\mathbb{F}_p}^*$, qui est d'ordre $p-1$, et soit C l'ensemble des $x \in G$ qui sont des carrés. L'application $c : G \longrightarrow G, x \mapsto x^2$ est un morphisme de groupes, de noyau $\{1,-1\}$, et d'image C. Ainsi, C est de cardinal $(p-1)/2$.
D'autre part, tout $x \in G$ vérifie $x^{p-1} = 1$; si $x \in C$, il est de la forme y^2, donc $x^{(p-1)/2} = y^{p-1} = 1$. Ainsi C est contenu dans l'ensemble S des racines du polynôme $Q = X^{(p-1)/2} - 1$ dans $\mathbb{F}_p$. Or le cardinal de S est au plus $\deg Q = (p-1)/2 = \# C$, donc $C = S$. $\square$
Ainsi, si $p \equiv 3 \ (4)$, p est irréductible dans $\mathbb{Z}[i]$. Sinon, p n'est pas irréductible dans $\mathbb{Z}[i]$. Le théorème suivant résume nos conclusions.

3.5.7. Théorème. *Soit p un nombre premier.*
1) Si p est congru à 3 modulo 4, p est irréductible dans $\mathbb{Z}[i]$.
2) Si p est congru à 1 modulo 4, il existe $f \in \mathbb{Z}[i]$ tel que $N(f) = p$, et f et $\bar{f}$ sont deux irréductibles de $\mathbb{Z}[i]$ non associés.
3) on a $2 = -i(1+i)^2$, et $1+i$ est un irréductible de $\mathbb{Z}[i]$.
Cette liste constitue un système de représentants des éléments irréductibles de $\mathbb{Z}[i]$. $\square$

3.5.8. Un anneau intègre non factoriel

Soit $\mathbb{Z}[i\sqrt{5}]$ l'ensemble des nombres complexes de la forme $a + ib\sqrt{5}$, avec $a,\ b \in \mathbb{Z}$. On vérifie aisément que c'est un sous-anneau de $\mathbb{C}$, et donc un anneau intègre. Pour $z = a + ib\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$, posons $N(z) = z\bar{z} = |z|^2 = a^2 + 5b^2$. Cette application prend ses valeurs dans $\mathbb{N}$ et vérifie $N(xy) = N(x)N(y)$ et $N(1) = 1$. Les éléments inversibles de $\mathbb{Z}[i\sqrt{5}]$ sont 1 et -1. D'autre part, 2 est un élément irréductible de $\mathbb{Z}[i\sqrt{5}]$. Soit $x = (1 + i\sqrt{5})$. Alors $x\bar{x} = 6$ appartient à l'idéal engendré par 2, sans que ni x, ni $\bar{x}$ ne lui appartiennent; donc 2 n'est pas premier. Ainsi $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

3.6. Questions d'irréductibilité dans $A[X]$

Soit A un anneau intègre. Les éléments inversibles de $A[X]$ sont ceux de A, et les éléments irréductibles de degré 0 de $A[X]$ sont les éléments irréductibles de A.
Puisqu'on identifie A à un sous-anneau de son corps des factions $\mathsf{Frac}\, A$, $A[X]$ est un sous-anneau de $(\mathsf{Frac}\, A)[X]$. Si $P \in A[X]$, P peut très bien être irréductible dans $(\mathsf{Frac}\, A)[X]$, sans l'être dans $A[X]$: ainsi, $2X-2$ est irréductible dans $\mathbb{Q}[X]$, mais pas dans $\mathbb{Z}[X]$.

3.6.1. Définition. Soit A un anneau intègre, et $P \in A[X]$. On dit que P est *primitif* si les coefficients de P sont premiers entre eux dans leur ensemble, ce qui revient à dire que le plus petit idéal principal de A contenant les coefficients de P est A lui-même.

Remarque. Un polynôme P est primitif si et seulement s'il est non nul, et ses seuls diviseurs de degré 0 dans $A[X]$ sont les éléments de A^*.

3.6.2. Proposition. *Soit A un anneau intègre, et $P \in A[X]$ un polynôme de degré ≥ 1.*
1) Si P est irréductible dans $A[X]$, il est primitif.
2) Si P est primitif, et s'il est irréductible dans $(\mathsf{Frac}\, A)[X]$, il est irréductible dans $A[X]$.

Demonstration.
1) Si P n'est pas primitif, il existe un élément a non nul et non inversible de A qui divise tous les coefficents de P. Ainsi P s'écrit aQ, avec $Q \in A[X]$; et $\deg Q = \deg P \geq 1$, donc Q n'est pas plus inversible que a dans $A[X]$, ce qui contredit l'irréductibilité de P.
2) Supposons P réductible dans $A[X]$; il s'écrit donc QR, avec $Q,\ R \in A[X]$. Puisque P est primitif, Q et R sont de degré ≥ 1, donc ils ne sont pas inversibles dans $(\mathsf{Frac}\, A)[X]$, ce qui contredit l'irréductibilité de P dans cet anneau. □

Si $P \in A[X]$ est irréductible de degré ≥ 1, est-il irréductible dans $(\mathsf{Frac}\, A)[X]$? Nous verrons plus loin que c'est le cas si A est factoriel.

Soit A un anneau, et I un idéal de A. Notons $x \mapsto \overline{x}$ la surjection canonique $A \longrightarrow A/I$. Considérons le morphisme d'anneaux

$$\begin{aligned} \Pi : A[X] &\longrightarrow (A/I)[X] \\ P = \sum_{n\in\mathbb{N}} a_n X^n &\longmapsto \overline{P} = \sum_{n\in\mathbb{N}} \overline{a}_n X^n . \end{aligned}$$

Si P est un élément de $A[X]$, on appelle *réduction de P modulo I* l'image de P par Π. Cette opération permet parfois de montrer facilement l'irréductibilité d'un polynôme.

3.6.3. Proposition. *Soit A un anneau intègre, et $\mathfrak{p}$ un idéal premier de A. Soit P un polynôme primitif de degré ≥ 1 à coefficients dans A, et dont le coefficient directeur n'est pas un élément de $\mathfrak{p}$.*
Alors si la réduction de P modulo $\mathfrak{p}$ est irréductible dans $(A/\mathfrak{p})[X]$, P est irréductible dans $A[X]$.

Demonstration. Supposons P réductible dans $A[X]$; alors $P = QR$, où Q et R sont des éléments de $A[X]$ de degré ≥ 1 (car P est primitif). D'autre part les coefficients directeurs de Q et R ne sont pas des éléments de $\mathfrak{p}$. On a dans $(A/\mathfrak{p})[X]$: $\overline{P} = \overline{QR}$, et $\overline{Q}$ et $\overline{R}$ sont de degré ≥ 1, ce qui contredit l'irréductibilité de $\overline{P}$. □

Exemple. Soit $P = 1000X^3+999X^2+998X+997$. Alors P est primitif dans $\mathbb{Z}[X]$, et son coefficient directeur n'est pas multiple de 3. La réduction de P modulo 3 est $X^3 - X + 1$, qui est un élément irréductible de $(\mathbb{Z}/3\mathbb{Z})[X]$ car il n'a pas de racine dans $\mathbb{Z}/3\mathbb{Z}$. Donc P est irréductible dans $\mathbb{Z}[X]$.

À présent, nous nous intéressons plus particulièrement aux anneaux factoriels.

Notons que si A est factoriel, et $P \in A[X]$, alors P est primitif si et seulement si aucun élément irréductible de A ne divise tous ses coefficients non nuls, ce qui équivaut à dire que pour tout élément irréductible f de A, la réduction de P modulo (f) est non nulle. Or si f est un élément irréductible de A, l'anneau $(A/(f))[X]$ est intègre. On en déduit donc la proposition suivante.

3.6.4. Proposition. *Si A est factoriel, le produit de deux polynômes primitifs de $A[X]$ est un polynôme primitif.* □

3.6.5. Proposition. *Soit A un anneau factoriel, et $K = \mathsf{Frac}\, A$.*
1) Pour tout $P \in K[X]$ non nul, il existe $c \in K^*$ et un polynôme primitif Q dans $A[X]$ tels que $P = cQ$.
De plus, un tel élément $c \in K^*$ est unique à multiplication par un élément de A^* près. On le notera $c(P)$.
2) Pour $P \in K[X]$ non nul, on a $P \in A[X] \Longleftrightarrow c(P) \in A - \{0\}$, et P est un élément primitif de $A[X] \Longleftrightarrow c(P) \in A^*$.
3) Pour P_1, $P_2 \in K[X]$ non nuls, on a $c(P_1P_2) = c(P_1)c(P_2)$ à multiplication par un élément de A^* près.

Demonstration.
1) Existence. Supposons tout d'abord $P \in A[X]$, et soit c le $PGCD$ de tous les coefficients non nuls de P. Alors P s'écrit cQ, avec $Q \in A[X]$, et Q est primitif.
Dans le cas général, il existe $d \in A - \{0\}$ tel que $dP \in A[X]$. On a alors $dP = \gamma Q$, avec $\gamma \in A - \{0\}$ et Q primitif; et $c = \gamma/d$ convient.
Unicité. Il s'agit de montrer que si on a $c_1Q_1 = c_2Q_2$ avec c_1, $c_2 \in K^*$ et Q_1, $Q_2 \in A[X]$ primitifs, alors $c_2/c_1 \in A^*$. Quitte à les multiplier tous deux par un même élément de $A - \{0\}$, on peut supposer que c_1 et c_2 appartiennent à $A - \{0\}$. Alors c_1 est un PGCD des coefficients de c_1Q_1, et c_2, un PGCD des coefficients de c_2Q_2. On a donc $c_1 \sim c_2$, d'où $c_2/c_1 \in A^*$.
2) Résulte de ce qui précède.
3) On a $P_1 = c(P_1)Q_1$, et $P_2 = c(P_2)Q_2$, avec Q_1 et Q_2 primitifs dans $A[X]$. Ainsi $P_1P_2 = c(P_1)c(P_2)Q_1Q_2$, et Q_1Q_2 est primitif par **3.6.4,** donc $c(P_1)c(P_2) = c(P_1P_2)$ à multiplication par un élément de A^* près. □

3.6.6. Théorème. *Soit A un anneau factoriel. Alors*
1) $A[X]$ est factoriel.
2) les éléments irréductibles de $A[X]$ de degré 0 sont les éléments irréductibles de A;
3) les éléments irréductibles de $A[X]$ de degré ≥ 1 sont les polynômes primitifs de $A[X]$ qui sont irréductibles dans $(\mathsf{Frac}\, A)[X]$.

DEMONSTRATION. Posons $K = \mathsf{Frac}\, A$. Montrons 2) et 3), puis 1).
2) On a déjà fait cette remarque.
3) En vertu de **3.6.2,** il suffit de montrer que si P est irréductible dans $A[X]$, de degré ≥ 1, il est irréductible dans $K[X]$. Supposons le contraire. Alors $P = P_1 P_2$, où P_1 et P_2 sont des éléments de $K[X]$ de degré ≥ 1. On a $P_1 = c(P_1)Q_1$, et $P_2 = c(P_2)Q_2$, avec Q_1, Q_2 primitifs dans $A[X]$. Ainsi, $P = c(P_1)c(P_2)Q_1 Q_2 = c(P)Q_1 Q_2$, avec $c(P) \in A - \{0\}$, et Q_1, $Q_2 \in A[X]$ sont de degré ≥ 1, ce qui contredit l'irréductibilité de P dans $A[X]$.
1) Montrons que si A vérifie la condition (F'1), $A[X]$ la vérifie aussi. Supposons que $A[X]$ ne vérifie pas (F'1). Alors il existe une suite $(P_n)_{n\in\mathbb{N}}$ d'éléments non nuls de $A[X]$ telle que la suite des idéaux (P_n) soit strictement croissante. On a $P_{n+1} \mid P_n$ pour tout n, donc la suite des degrés des polynômes P_n est décroissante. Par conséquent cette suite est stationnaire. D'autre part, soit c_n le coefficient directeur de P_n. Alors pour tout n, c_{n+1} divise c_n, donc la suite $(c_n A)_{n\in\mathbb{N}}$ est une suite croissante d'idéaux principaux de A. L'anneau A vérifiant (F'1), cette suite est stationnaire. Il existe donc $N \in \mathbb{N}$ tel que pour $n \geq N$, on ait $a_n \sim a_N$ et $\deg P_n = \deg P_N$. Alors $P_n / P_N = a_n / a_N \in A^*$, donc $(P_n) = (P_N)$ ce qui contredit nos hypothèses.
Montrons maintenant que si A est factoriel, $A[X]$ vérifie (F'2). Un irréductible de $A[X]$ de degré 0 est un irréductible de A. Soit f un tel élément. Alors $A[X]/fA[X] \simeq (A/fA)[X]$, et puisque A est factoriel, A/fA est intègre, ainsi que $(A/fA)[X]$; donc $fA[X]$ est un idéal premier de $A[X]$.
A présent soit P un irréductible de $A[X]$ de degré ≥ 1, et montrons que $PA[X]$ est un idéal premier de $A[X]$. Soient Q, R deux éléments non nuls de $A[X]$ tels que P divise QR dans $A[X]$. Montrons qu'alors P divise Q ou R dans $A[X]$. On observe que P divise QR dans $K[X]$; or $K[X]$ est factoriel, et P est irréductible dans $K[X]$ (assertion 3), donc P divise Q ou R dans $K[X]$.
Il suffit donc, pour conclure, de montrer que si P divise Q dans $K[X]$, il le divise dans $A[X]$. Supposons donc $Q = PT$, avec $T \in K[X]$. On a $c(Q) = c(P)c(T)$. Or, $c(Q) \in A - \{0\}$, car $Q \in A[X]$, et $c(P) \in A^*$, car P est primitif dans $A[X]$; donc $c(T) \in A - \{0\}$, d'où $T \in A[X]$, ce qui démontre que P divise Q dans $A[X]$. $\square$

Un dernier critère d'irréductibilité...

3.6.7. Proposition. (Critère d'Eisenstein) *Soit A un anneau factoriel, et f un élément irréductible de A.*
Soit $P \in A[X]$ un polynôme de degré $n \geq 1$, de la forme
$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 .$$
On fait les hypothèses suivantes : $a_n \not\equiv 0\ (f)$, $a_k \equiv 0\ (f)$ pour tout $k = 0, 1, \ldots, n-1$, et $a_0 \not\equiv 0\ (f^2)$.
Alors P est irréductible dans $(\mathsf{Frac}\, A)[X]$, et, s'il est primitif, il est aussi irréductible dans $A[X]$.

DEMONSTRATION. Supposons tout d'abord P primitif. Si P est réductible dans $A[X]$, il s'écrit QR, avec Q, $R \in A[X]$ de degré ≥ 1; et les coefficients directeurs de Q et de R ne sont pas des multiples de f. Considérons les réductions modulo (f) de ces polynômes. On a $\overline{P} = \overline{QR}$, et $\overline{Q}$, $\overline{R}$ sont de degré ≥ 1. Or, $\overline{P} = \overline{a_n} X^n$, les autres coefficients de P étant congrus à zéro modulo f. Ainsi $\overline{P}$ est un monôme non nul.

3.6.8. Lemme. *Soit A un anneau intègre, et $P \in A[X]$ non nul. Si P est un monôme, ses diviseurs sont aussi des monômes.*

DEMONSTRATION. On a $P = aX^n$, avec $a \in A - \{0\}$ et $n \in \mathbb{N}$. Montrons par récurrence sur n que si $P = QR$, Q et R sont eux aussi des monômes. Pour $n = 0$, c'est immédiat car Q et R sont alors de degré 0. Soit $n \geq 1$, et supposons le cas $n-1$ déja démontré. Alors $P \in (X)$. Or l'idéal (X) est premier, car $A[X]/(X) \simeq A$; donc on a Q ou $R \in (X)$. Par exemple, Q est de la forme $Q_0 X$. On a $P = aX^{n-1}X = Q_0 RX$, donc $aX^{n-1} = Q_0 R$. Par hypothèse de récurrence, Q_0 et R sont des monômes, ainsi que $Q = XQ_0$. □

Ceci s'applique à $\overline{P}$, car $A/(f)$ est intègre, donc $\overline{Q}$ et $\overline{R}$ sont des monômes de degré ≥ 1. En particulier leurs coefficients de degré 0 sont nuls, ce qui signifie que ceux de Q et R sont des éléments de (f); leur produit a_0 est donc congru à 0 modulo (f^2), d'où contradiction. Ainsi P est irréductible dans $A[X]$ et dans $(\mathsf{Frac}\, A)[X]$.
Si P n'est pas primitif, il s'écrit $c(P)Q$, avec Q primitif. Puisque $c(P)$ divise a_n, il est premier à f, de sorte que Q vérifie les hypothèses de l'énoncé, donc il est irréductible dans $(\mathsf{Frac}\, A)[X]$, ainsi que P. □

3.6.9. EXEMPLE. Soit p un nombre premier, et $n \geq 1$. Alors $X^n - p$ est primitif dans $\mathbb{Z}[X]$, et satisfait aux conditions de la proposition relativement à l'élément irréductible p de $\mathbb{Z}$, donc il est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$. On voit donc que dans $\mathbb{Q}[X]$, il existe en tout degré une infinité d'éléments irréductibles deux à deux non associés.

4. Polynômes en plusieurs indéterminées

4.1. Construction

Soit I un ensemble quelconque, et soit $M = \mathbb{N}^{(I)}$ l'ensemble des suites presque nulles d'entiers naturels indexées par I. Un élément de M est appelé *multi-indice.* On définit sur $A^{(M)}$ deux lois de composition interne, $+$ et $\cdot$, en posant, pour $P = (a_n)_{n \in M}$ et $Q = (b_n)_{n \in M}$:

$$P + Q = (a_n + b_n)_{n \in M} \text{ et } P \cdot Q = (c_n)_{n \in M}, \text{ où } c_n = \sum_{\substack{l,m \in M \\ l+m=n}} a_l\, b_m \,.$$

L'ensemble des couples $(l, m) \in M^2$ tels que $a_l b_m$ soit non nul étant fini, la suite $(c_n)_{n \in M}$ est bien définie, et elle est presque nulle.
Il est clair que $+$ fait de $A^{(M)}$ un groupe abélien, et que $\cdot$ est distributive par rapport à $+$.
Pour $n, m \in M$ notons $\delta_{n,m}$ l'élément de A égal à 1 si $m = n$, et à 0 sinon.
Pour $a \in A$ et pour un multi-indice d, notons aX^d l'élément $(a\delta_{d,n})_{n \in M}$. Cet élément est appelé *monôme de multi-degré d et de coefficient a.*
Tout $P \in A^{(M)}$ s'écrit de façon unique

$$P = \sum_{m \in M} a_m X^m \,,$$

donc P est une somme finie de monômes. Montrons que la loi $\cdot$ est commutative et associative, et admet $1X^0$ pour élément neutre. Il suffit, par distributivité de $\cdot$ par rapport à $+$, de le vérifier sur les monômes. Or, on a $(aX^m)\cdot(bX^n) = (ab)X^{m+n}$, donc ces propriétés résultent des propriétés analogues de la multiplication de A et de l'addition de M.
Ainsi, $A^{(M)}$, muni de $+$ et $\cdot$, est un anneau commutatif.
L'application

$$\begin{aligned} \eta : A &\longrightarrow A^{(M)} \\ a &\longmapsto aX^0 \end{aligned}$$

est clairement un morphisme d'anneaux injectif, ce qui fait de $A^{(M)}$ une A-algèbre.
Nous ferons systématiquement l'abus consistant à considérer A comme un sous-anneau de $A^{(M)}$ en identifiant l'élément $a \in A$ à son image par η. On pose $X^m = 1X^m$, de sorte qu'on a $aX^m = a \cdot X^m$.
Pour $i \in I$, notons δ_i l'élément de M défini par $(\delta_i)_j = 1$ si $i = j$, 0 sinon. Posons $X_i = X^{\delta_i}$.
Avec cette convention, on a, pour tout multi-indice $M = (m_i)_{i\in I}$:

$$X^m = \prod_{i\in I} X_i^{m_i} ,$$

ce produit ayant un sens car il ne comporte qu'un nombre fini de facteurs autres que 1.

4.1.1. Définition. La A-algèbre $A^{(M)}$ est appelée *algèbre des polynômes en les indéterminées $(X_i)_{i\in I}$ à coefficients dans A*, et notée $A[(X_i)_{i\in I}]$.
Cette A-algèbre, qui contient pour chaque $i \in I$ un élément particulier X_i, appelé la *i-ième indéterminée*, vérifie la propriété universelle suivante.

4.1.2. Proposition. *Soit A un anneau, I un ensemble quelconque, et B une A-algèbre commutative. Alors pour toute famille $(x_i)_{i\in I}$ d'éléments de B indexée par I, il existe un unique morphisme de A-algèbres $e : A[(X_i)_{i\in I}] \longrightarrow B$ vérifiant $e(X_i) = x_i$ pour tout $i \in I$.*

Demonstration. Soit $\eta : A \longrightarrow B$ le morphisme d'anneaux qui fait de B une A-algèbre. Soit e un morphisme de A-algèbres $A[(X_i)_{i\in I}] \longrightarrow B$, vérifiant $e(X_i) = x_i$.
Tout $P \in A[(x_i)_{i\in I}]$ s'écrit de façon unique $P = \sum_{m\in M} a_m X^m$; on a donc

$$e(P) = \sum_{m\in M} e(a_m X^m) = \sum_{m\in M} \eta(a_m) e(X^m) .$$

Or tout monôme X^m s'écrit $\prod_{i\in I} X_i^{m_i}$; donc

$$e(X^m) = \prod_{i\in I} e(X_i)^{m_i} = \prod_{i\in I} x_i^{m_i} ,$$

ce qui achève de déterminer entièrement e. Inversement, ce qui précède définit une application e, dont on vérifie aisément que c'est un morphisme d'algèbres qui convient. $\square$

4.1.3. Remarque. Si I est l'ensemble vide, $A[(X_i)_{i\in I}]$ est égal à A. Si I est réduit à un élément i_0, il existe un unique isomorphisme de A-algèbres $A[X] \xrightarrow{\sim} A[(X_i)_{i\in I}]$ envoyant X sur X_{i_0}.

4.2. L'anneau $A[X_1, \ldots, X_n]$

On s'intéresse désormais au cas où l'ensemble I est fini. Pour $n \in \mathbb{N}$, notons $[n]$ l'ensemble $\{1, 2, \ldots, n\}$, en convenant que $[0]$ est vide; ainsi $[n]$ est de cardinal n pour tout n.
On note $A[X_1, \ldots, X_n]$ la A-algèbre $A[(X_i)_{i\in[n]}]$. On s'autorise à changer le nom des indéterminées X_i. Par exemple, $A[X_1, X_2, X_3]$ pourra être noté indifféremment $A[X, Y, Z]$, $A[Y_1, Y_2, T]$ ...

4.2.1. Proposition. (Regroupement par paquets)
Soient n, p, q trois éléments de $\mathbb{N}$ tels que $n = p+q$. Soient $i : [p] \hookrightarrow [n]$ et $j : [q] \hookrightarrow [n]$ deux applications injectives telles que $[n]$ soit la réunion disjointe des images de i et de j. Alors il existe un unique isomorphisme de A-algèbres

$$\Phi : A[Y_1, \ldots, Y_p][Z_1 \ldots, Z_q] \xrightarrow{\sim} A[X_1, \ldots, X_n]$$

vérifiant $Y_k \mapsto X_{i(k)}$ pour $k \in [p]$, et $Z_l \mapsto X_{j(l)}$ pour $l \in [q]$.

Demonstration. Par la propriété universelle de $A[Y_1, \ldots, Y_p]$, il existe un unique morphisme de A-algèbres $\Phi_0 : A[Y_1, \ldots, Y_p] \longrightarrow A[X_1, \ldots, X_n]$ vérifiant $a \mapsto a$ pour $a \in A$ et $Y_k \mapsto X_{i(k)}$ pour $k \in [p]$. De plus Φ_0 fait de $A[X_1, \ldots, X_n]$ une $A[Y_1, \ldots, Y_p]$-algèbre. Par la propriété universelle de $A[Y_1, \ldots, Y_p][Z_1, \ldots, Z_q]$, il existe donc un unique morphisme de $A[Y_1, \ldots, Y_p]$-algèbres $\Phi : A[Y_1, \ldots, Y_p][Z_1 \ldots, Z_q] \longrightarrow A[X_1, \ldots, X_n]$ vérifiant $Z_l \mapsto X_{j(l)}$ pour $l \in [q]$; or dire que Φ est un morphisme de $A[Y_1, \ldots Y_p]$-algèbres revient à dire que c'est un morphisme de A-algèbres vérifiant $Y_k \mapsto X_{i(k)}$ pour $k \in [p]$.
Reste à montrer que ce Φ est un isomorphisme.
D'après la propriété universelle de $A[X_1, \ldots, X_n]$, il existe un unique morphisme de A-algèbres

$$\Psi : A[X_1, \ldots, X_n] \longrightarrow A[Y_1, \ldots, Y_p][Z_1 \ldots, Z_q]$$

vérifiant pour $m \in [n]$: $X_m \mapsto Y_k$ si $m = i(k)$, $X_m \mapsto Z_l$ si $m = j(l)$.
On vérifie que Ψ est un inverse de Φ. Par exemple, $\Phi \circ \Psi$ est un morphisme de A-algèbres de $A[X_1, \ldots, X_n]$ dans lui même, qui laisse fixes les X_i; c'est donc l'identité de $A[X_1, \ldots, X_n]$. □

4.2.2. Corollaire. *On a pour tout $n \geq 1$:*

$$A[X_1, \ldots, X_n] \simeq A[X_1, \ldots, X_{n-1}][X_n]. \qquad \square$$

4.2.3. Théorème. *Soit A un anneau, et $n \in \mathbb{N}$.*
Si A est intègre, $A[X_1, \ldots, X_n]$ est intègre.
Si A est factoriel, $A[X_1, \ldots, X_n]$ est factoriel.
Si A est noethérien, $A[X_1, \ldots, X_n]$ est noethérien.

DEMONSTRATION. Soit $\mathcal{P}$ une propriété d'anneaux. On dit qu'elle est *héréditaire* si chaque fois que $\mathcal{P}$ est vraie pour un anneau A, elle l'est pour tout anneau isomorphe à A, et pour $A[X]$. Si $\mathcal{P}$ est héréditaire, et si $\mathcal{P}$ est vraie pour A, elle est encore vraie pour $A[X_1, \ldots, X_n]$ quel que soit $n \in \mathbb{N}$. (Cela résulte immédiatement de **4.2.2** par récurrence sur n.) Or, on sait que "A est intègre" et "A est factoriel"sont des propriétés héréditaires. On démontrera plus tard que "A est noethérien" est elle aussi héréditaire. □

4.2.3. Fonctions polynomiales et évaluation

Soit $P \in A[X_1, \ldots, X_n]$. Alors P s'écrit de façon unique

$$P = \sum_{m_1, \ldots, m_n \in \mathbb{N}} a_{m_1, \ldots, m_n} X_1^{m_1} \cdots X_n^{m_n} \,;$$

pour $x_1, \ldots, x_n \in A$, on appelle *valeur de P en* $(x_1, \ldots, x_n)$, et on note $P(x_1, \ldots, x_n)$, l'élément

$$\sum_{m_1, \ldots, m_n \in \mathbb{N}} a_{m_1, \ldots, m_n} x_1^{m_1} \cdots x_n^{m_n} \in A \,.$$

L'application de $A[X_1, \ldots, X_n]$ dans A qui associe à un polynôme P sa valeur en $(x_1, \ldots, x_n)$ est un morphisme de A-algèbres appelé *évaluation en* $(x_1, \ldots, x_n)$.
Ainsi, tout $P \in A[X_1, \ldots, X_n]$ définit une application

$$\begin{aligned} \widetilde{P} : A^n &\longrightarrow A \\ (x_1, \ldots, x_n) &\longmapsto P(x_1, \ldots, x_n) \end{aligned}$$

appellée *fonction polynomiale associée à P*.
L'ensemble des applications de A^n dans A, qui n'est autre que A^{A^n}, est naturellement muni d'une structure de A-algèbre (cf. **1.5.3**). L'application

$$A[X_1, \ldots, X_n] \longrightarrow A^{A^n}$$

qui associe à un polynôme P la fonction polynomiale $\widetilde{P}$ est un morphisme de A-algèbres.

4.2.4. REMARQUE. Il faut prendre garde au fait qu'en général, l'application $P \mapsto \widetilde{P}$ n'est pas injective. Par exemple, soit $P = X^p - X \in (\mathbb{Z}/p\mathbb{Z})[X]$. Alors pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, $P(x) = 0$, donc $\widetilde{P} = 0$ bien que P ne soit pas nul.
En général, on ne peut donc pas identifier un polynôme à la fonction polynomiale qui lui est associée.

4.2.5. Proposition. *Soit K un corps, et $n \geq 1$. Soit E le morphisme de K-algèbres*

$$\begin{gathered} K[X_1, \ldots, X_n] \longrightarrow K^{K^n} \\ P \mapsto \widetilde{P} \,; \end{gathered}$$

alors
1) E est injectif si et seulement si K est de cardinal infini;
2) si K est de cardinal fini q, E est surjectif, et le noyau de E est l'idéal de $K[X_1, \ldots, X_n]$ engendré par les polynômes $X_i^q - X_i$ pour $i = 1, \ldots, n$.

DEMONSTRATION. Laissée en exercice. □

4.2.6. Substitution

Soient A un anneau, n et p deux entiers, et $Q_1, \ldots, Q_n$ des éléments de $A[Y_1, \ldots, Y_p]$. Alors il existe un unique morphisme de A-algèbres

$$A[X_1, \ldots, X_n] \longrightarrow A[Y_1, \ldots, Y_p]$$

vérifiant $X_i \mapsto Q_i$; on l'appelle *substitution de* $Q_1, \ldots, Q_n$ *aux indéterminées* $X_1, \ldots, X_n$. L'image de $P \in A[X_1, \ldots, X_n]$ est notée $P(Q_1, \ldots, Q_n)$.

4.2.7. Proposition. *Soit A un anneau, $n \in \mathbb{N}$ et $i \in [n]$. Alors*
1) $\forall P \in A[X_1, \ldots, X_n]$, $P \in (X_i) \Longleftrightarrow P(X_1, \ldots, X_{i-1}, 0, X_{i+1}, \ldots, X_n) = 0$;
2) $A[X_1, \ldots, X_n]/(X_i) \simeq A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$;
3) l'élément X_i est régulier dans $A[X_1, \ldots, X_n]$;
4) si A est intègre, (X_i) est premier.

DEMONSTRATION. Posons $B = A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ et $X = X_i$, de sorte que $A[X_1, \ldots, X_n] \simeq B[X]$. On se ramène ainsi aux polynômes en une indéterminée, et c'est alors immédiat. □

4.3. Notion de degré et polynômes homogènes

Soit A un anneau et $n \in \mathbb{N}$. Rappelons qu'à chaque multi-indice $m = (m_1, \ldots, m_n) \in \mathbb{N}^n$ est associé un monôme $X^m = X_1^{m_1} \cdots X_n^{m_n} \in A[X_1, \ldots, X_n]$. Tout $P \in A[X_1, \ldots, X_n]$ s'écrit de manière unique sous la forme $\sum_{m \in \mathbb{N}^n} a_m X^m$. On dira que le monôme X^m *figure dans* P si le coefficient a_m est non nul.

4.3.1. Définitions. On appelle *degré du monôme* $X^m = X_1^{m_1} \cdots X_n^{m_n}$ l'entier naturel $m_1 + m_2 + \cdots + m_n$. Pour $P \in A[X_1, \ldots, X_n]$, on appelle *degré de* P, et on note $\deg P$, le plus grand degré d'un monôme qui y figure. Si P est nul, on convient que son degré est $-\infty$.
On dit que P est *homogène de degré* d si tous les monômes qui y figurent sont de degré d.

REMARQUE. Le polynôme nul est homogène de degré d pour tout $d \in \mathbb{N}$, bien que son degré soit $-\infty$. Tout autre polynôme homogène de degré d est un polynôme de degré d.

4.3.2. Proposition.
1) Si P et Q sont deux polynômes homogènes de degré d, $aP + bQ$ est un polynôme homogène de degré d pour tous a, $b \in A$.
2) Si P est un polynôme homogène de degré d et Q, un polynôme homogène de degré d', alors PQ est un polynôme homogène de degré $d + d'$.
3) Les polynômes homogènes de degré 0 sont les éléments de A.
4) Tout $P \in A[X_1, \ldots, X_n]$ s'écrit de façon unique sous la forme $P = \sum_{d \in \mathbb{N}} P_d$, où $(P_d)_{d \in \mathbb{N}}$ est une famille de polynômes presque nulle, P_d étant pour tout d un polynôme homogène de degré d.
Le polynôme P_d est appelé composante homogène de degré d de P .

DEMONSTRATION. C'est immédiat. $\square$

4.3.3. Proposition. *Soient P, $Q \in A[X_1, \dots, X_n]$. Alors*
1) $\deg(P+Q) \leq \sup(\deg P, \deg Q)$*;*
2) $\deg(PQ) \leq \deg P + \deg Q$*, avec égalité si A est intègre.*

DEMONSTRATION. Si P ou Q est nul, c'est clair. Sinon, soit $p = \deg P$, $q = \deg Q$. On a $P = \sum_{h \in \mathbb{N}} P_h$, et $Q = \sum_{h \in \mathbb{N}} Q_h$, avec P_h, Q_h homogènes de degré h; de plus $P_p \neq 0$, et $P_h = 0$ pour $h > p$, de même $Q_q \neq 0$, et Q_h est nul pour $h > q$. On en déduit $P + Q = \sum_{h=0}^{\sup(p,q)} P_h + Q_h$, d'où 1).
D'autre part $PQ = \sum_{h,h' \in \mathbb{N}} P_h Q_{h'}$, donc la composante homogène de degré h de PQ est $P_h Q_0 + P_{h-1} Q_1 + \cdots + P_0 Q_h$. En particulier cela donne $P_p Q_q$ si $h = p + q$, et 0 si $h > p + q$. On a donc $\deg(P+Q) \leq p + q$. De plus on a l'égalité si et seulement si $P_p Q_q \neq 0$: c'est bien le cas si A est intègre, car il en va alors de même de $A[X_1, \dots, X_n]$.
$\square$

4.3.4. Proposition. *Soit A un anneau intègre, et $P \in A[X_1, \dots, X_n]$ un polynôme homogène non nul. Si $P = QR$, Q et R sont des polynômes homogènes.*

DEMONSTRATION.
Considérons le morphisme de A-algèbres de $A[X_1, \dots, X_n]$ vers $A[X_1, \dots, X_n][T]$ qui envoie le polynôme P sur $\widehat{P} = P(X_1 T, \dots, X_n T)$. Si $P = \sum_{h \in \mathbb{N}} P_h$, avec P_h homogène de degré h, on a $\widehat{P} = \sum_{h \in \mathbb{N}} P_h T^h$ (en effet pour P homogène de degré d, $\widehat{P} = PT^d$). Le morphisme $P \mapsto \widehat{P}$ est injectif, car $P = \widehat{P}(X_1, \dots, X_n, 1)$.
De plus, P est homogène $\iff$ $\widehat{P}$ est un monôme (en l'indéterminée T).
Si $P = QR$ est homogène et non nul, $\widehat{P} = \widehat{Q}\widehat{R}$ est un monôme non nul, donc en vertu du lemme **3.6.8,** $\widehat{Q}$ et $\widehat{R}$ sont aussi des monômes, et Q et R sont homogènes. $\square$

4.3.5. EXEMPLE. Cette proposition peut aider notemment à démontrer qu'un polynôme homogène est irréductible. Considérons par exemple $P = X^2 + Y^2 + Z^2 \in \mathbb{C}[X, Y, Z]$. Si P n'était pas irréductible, il admettrait un diviseur de degré 1, nécéssairement homogène, donc de la forme $aX + bY + cZ$. On aurait $P(-b, a, 0) = 0$, donc $b^2 = -a^2$. Par raison de symétrie, on aurait aussi $c^2 = -b^2$ et $c^2 = -a^2$, d'où $a = b = c = 0$, ce qui est exclu. Ainsi, P est irréductible.

4.4. Dérivation

4.4.1. Caractéristique d'un anneau

Soit A un anneau, et η l'unique morphisme d'anneaux de $\mathbb{Z}$ vers A. Le noyau de η est un idéal de $\mathbb{Z}$; il existe donc un unique entier naturel n tel que $\operatorname{Ker} \eta = n\mathbb{Z}$.

Définition. L'entier n est appelé *caractéristique de A*, et noté $\operatorname{car} A$.
Par passage au quotient, η induit un morphisme d'anneaux injectif $\mathbb{Z}/n\mathbb{Z} \hookrightarrow A$; donc si A est intègre, $n\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. Par conséquent, la caractéristique d'un anneau intègre est soit nulle, soit égale à un nombre premier p.

EXEMPLES. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux de caractéristique nulle. Pour tout $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ est un anneau de caractéristique n. En particulier pour p premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps de caractéristique p.

4.4.2. Proposition. *Soit A un anneau (commutatif) de caractéristique un nombre premier p. L'application $F : A \longrightarrow A$, $x \mapsto x^p$ est un morphisme d'anneaux, appelé* (morphisme de) Frobenius.

DEMONSTRATION. On a clairement $F(xy) = F(x)F(y)$, et $F(1) = 1$. D'autre part,

$$F(x+y) = \sum_{k=0}^{p} C_p^k x^k y^{p-k}$$

par la formule du binôme de Newton. Or C_p^k est un multiple de p pour $0 < k < p$, donc son image dans A est nulle, de sorte que $F(x+y) = x^p + y^p = F(x) + F(y)$. $\square$

4.4.3. Dérivation en une variable

Soit A un anneau.

4.4.4. Définition. Soit $P = \sum_{n\in\mathbb{N}} a_n X^n \in A[X]$. On appelle *dérivée de P* le polynôme

$$\sum_{n\in\mathbb{N}} (n+1)a_{n+1}X^n \,,$$

qu'on note DP, ou P'.

L'application $D : A[X] \longrightarrow A[X]$ vérifie les propriétés suivantes :
(D1) $\forall P, Q \in A[X]$, $D(P+Q) = DP + DQ$;
(D2) $\forall a \in A, \forall P \in A[X]$, $D(aP) = aDP$;
(D3) $\forall P, Q \in A[X]$, $D(PQ) = PDQ + QDP$.
Les conditions (D1) et (D2) signifient que D est A-linéaire (cf. partie II); et (D3) s'appelle la formule de Leibnitz.
On a de plus $DX = 1$, ce qui, joint à (D1), (D2), (D3), suffit à caractériser D.
On a $Da = 0$ pour tout $a \in A$, et on vérifie par récurrence (en utilisant (D1) et (D3)) qu'on a pour tout $Q \in A[X]$ et tout $n \geq 1$, $D(Q^n) = nQ^{n-1}DQ$.
Il en résulte que pour tous P, $Q \in A[X]$, on a $D(P(Q)) = (DP)(Q)DQ$.
D'autre part si $P \neq 0$, on a $\deg(DP) < \deg P$.

REMARQUE. Soit $P \in A[X]$ et $x \in A$. On dit que x est une *racine de P* (resp. une *racine multiple de P*) si $P \in (X - x)$ (resp. $P \in ((X-x)^2)$).
On a vu que x est une racine de $P \iff P(x) = 0$. Il est facile de montrer que x est une racine multiple de $P \iff P(x) = DP(x) = 0$. Mais nous allons voir maintenant qu'en général, on ne peut pas en dire plus.

4.4.5. Théorème. *Soit A un anneau intègre, et $P \in A[X]$.*
1) Si $\mathsf{car}\, A$ *est un nombre premier p, on a*

$$DP = 0 \iff P \in A[X^p]\,.$$

2) Si $\mathsf{car}\, A = 0$*, on a*

$$DP = 0 \iff P \in A\,.$$

En outre, pour tout $n \in \mathbb{N}$, $n!$ divise $D^n P$ dans $A[X]$, et on a pour tout $x \in A$ la formule de Taylor

$$P = \sum_{n\in\mathbb{N}} 1/n!\; D^n P(x)(X-x)^n\,.$$

Demonstration. Soit $P = \sum_{n\in\mathbb{N}} a_n X^n$. On a $DP = 0 \iff \forall n \in \mathbb{N},\ (n+1)a_{n+1} = 0 \iff \forall n \in \mathbb{N},\ a_{n+1} = 0$ ou $n+1 = 0$ dans A, puisque A est intègre.
Si la caractéristique est nulle, $n+1$ n'est jamais nul dans A donc on a bien $DP = 0 \iff P \in A$.
Si $\mathsf{car}\, A = p$ premier, $DP = 0 \iff \forall n$ non multiple de p, $a_n = 0 \iff P = a_0 + a_p X^p + \cdots a_{mp} X^{mp} + \cdots \iff P \in A[X^p]$.
D'autre part, on a $D^n(X^m) = m!/(m-n)!\,X^{(m-n)} = n!\,C_m^n\,X^{m-n}$ si $n \leq m$, 0 sinon; donc $D^n P$ peut s'écrire $n!\,Q$ pour un certain $Q \in A[X]$.
Vérifions maintenant la formule de Taylor, pour $\mathsf{car}\, A = 0$, par récurrence sur $\deg P$. Si $P = 0$, c'est clair. On suppose donc $\deg P \geq 0$. Alors $\deg DP < \deg P$, donc on a

$$DP = \sum_{n\in\mathbb{N}} 1/n!\; D^n DP(x)(X-x)^n = \sum_{n\in\mathbb{N}} 1/n!\; D^{n+1} P(x)(X-x)^n$$

par hypothèse de récurrence. Soit

$$Q = \sum_{n\in\mathbb{N}} 1/n!\; D^n P(x)(X-x)^n\,;$$

alors

$$DQ = \sum_{n>0} n/n!\; D^n P(x)(X-x)^{n-1} = \sum_{m\in\mathbb{N}} 1/m!\; D^{m+1} P(x)(X-x)^m = DP\,.$$

On a donc $D(Q-P) = 0$, et $Q-P$ est une constante puisque $\mathsf{car}\, A = 0$; or on a $Q(x) = P(x)$, donc $Q = P$. $\square$

4.4.5. Corollaire. *Si A est intègre de caractéristique 0, on a*

$$P \in ((X-x)^n) \iff P(x) = DP(x) = \cdots = D^{n-1} P(x) = 0\,. \quad \square$$

Remarque. C'est faux en caractéristique p. Par exemple, $P = X^p \in \mathbb{F}_p[X]$ vérifie $D^n P(0) = 0$ pour tout n, mais $P \notin (X^{p+1})$.

4.4.6. Dérivées partielles.

Soit A un anneau, $n \in \mathbb{N}$. Soit $i \in [n]$. Tout $P \in A[X_1, \ldots, X_n]$ peut être vu comme un polynôme en X_i à coefficients dans $B_i = A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$; autrement dit P s'écrit de façon unique

$$P = \sum_{m \in \mathbb{N}} C_m X_i^m ,$$

avec $C_m \in B_i$. On appelle *i-ième dérivée partielle de P*, et on note $D_i P$, ou $\frac{\partial}{\partial X_i} P$, le polynôme

$$\sum_{m \in \mathbb{N}} (m+1) C_{m+1} X_i^m .$$

L'application $D_i : A[X_1, \cdots, X_n] \longrightarrow A[X_1, \cdots X_n]$ n'est jamais que l'application dérivée de l'anneau de polynômes en une variable $B_i[X_i]$.
D'autre part, on a pour tous $i,\ j \in [n]$: $D_j \circ D_i = D_i \circ D_j$.

4.4.7. Théorème. *Soit A un anneau intègre de caractéristique 0, et $P \in A[X_1, \ldots, X_n]$. Soit $x = (x_1, \ldots, x_n) \in A^n$. On a alors la formule de taylor*

$$P = \sum_{m_1, \ldots, m_n \in \mathbb{N}} \frac{1}{m_1! \cdots m_n!} \frac{\partial^{m_1}}{\partial {X_1}^{m_1}} \cdots \frac{\partial^{m_n}}{\partial {X_n}^{m_n}} P(x) (X_1 - x_1)^{m_1} \cdots (X_n - x_n)^{m_n} .$$

Demonstration. Résulte de la formule en une variable par une récurrence évidente. □

4.4.8. Proposition. *Soit A un anneau, et $P \in A[X_1, \ldots X_n]$ un polynôme homogène de degré d. Alors on a*

$$\sum_{i=1}^{n} X_i \frac{\partial}{\partial X_i} P = dP .$$

Demonstration. Il suffit de le vérifier sur un monôme. Soit $M = X_1^{m_1} \cdots X_n^{m_n}$. On a $X_i \frac{\partial}{\partial X_i} M = m_i M$, donc $\sum_{i=1}^{n} X_i \frac{\partial}{\partial X_i} M = \deg(M) M$, d'où l'assertion. □

5. Polynômes symétriques

5.1. Généralités

Soit n un entier naturel, et $\mathfrak{S}_n$ le n-ième groupe de permutations; c'est le groupe des bijections de $[n]$ dans $[n]$. Notons e l'élément neutre de ce groupe.
Soit A un anneau. Pour tout $\sigma \in \mathfrak{S}_n$, soit ρ_σ l'unique morphisme de A-algèbres

$$\begin{aligned} A[X_1, \ldots, X_n] &\longrightarrow A[X_1, \ldots, X_n] \\ X_i &\longmapsto X_{\sigma(i)} . \end{aligned}$$

Pour $P \in A[X_1, \ldots, X_n]$, notons ${}^\sigma P$ l'image de P par ρ_σ ; on a donc

$${}^\sigma P = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) .$$

Pour tout P, on a : $\forall \sigma, \tau \in \mathfrak{S}_n, {}^{\sigma\tau} P = {}^\sigma({}^\tau P)$, et ${}^e P = P$. Autrement dit, nous avons défini une action à gauche de $\mathfrak{S}_n$ sur $A[X_1, \ldots, X_n]$.

5.1.1. Définition. Un polynôme $P \in A[X_1, \ldots, X_n]$ est dit *symétrique* si pour tout $\sigma \in \mathfrak{S}_n$, ${}^\sigma P = P$. On note $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ l'ensemble des polynômes symétriques.

5.1.2. Proposition. *L'ensemble $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ est un sous-anneau de $A[X_1, \ldots X_n]$ qui contient A. Il est donc muni d'une structure de A-algèbre.*

DEMONSTRATION. Les applications ρ_σ sont des morphismes de A-algèbres. Pour $a \in A$, on a $\forall \sigma \in \mathfrak{S}_n, {}^\sigma a = a$; donc a est symétrique. Soient P, Q deux polynômes symétriques. Alors pour tout $\sigma \in \mathfrak{S}_n$ on a ${}^\sigma(P-Q) = {}^\sigma P - {}^\sigma Q = P - Q$, et ${}^\sigma(PQ) = {}^\sigma P {}^\sigma Q = PQ$, donc $P - Q$ et PQ sont symétriques. □

EXEMPLES.
1) $X_1 + \cdots + X_n$.
2) $X_1 \cdots X_n$.
3) $X_1^k + \cdots + X_n^k$ pour $k \in \mathbb{N}$.
4) $\displaystyle\sum_{\substack{1 \le i,j \le n \\ i \ne j}} X_i^2 X_j$.
5) $\displaystyle\prod_{\substack{1 \le i,j \le n \\ i \ne j}} (X_i - X_j)$.

5.1.3. Polynômes symétriques élémentaires

Considérons dans $A[X_1, \ldots, X_n, T]$ le polynôme

$$P = \prod_{i=1}^{n} (T + X_i) .$$

Vu comme un polynôme en $X_1, \ldots X_n$ à coefficients dans $A[T]$, P est symétrique. Vu comme un polynôme en T à coefficients dans $A[X_1, \ldots X_n]$, P est unitaire de degré n. Il s'écrit donc

$$P = \sum_{k=0}^{n} T^{n-k} \Sigma_k(X_1, \ldots, X_n) ,$$

et chaque Σ_k est un polynôme symétrique en les X_i.

5.1.4. Définition. Pour $k \in \{0, \ldots, n\}$ le polynôme $\Sigma_k \in A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ est appelé *k-ième polynôme symétrique élémentaire.*

REMARQUE. On a $\Sigma_0 = 1$, $\Sigma_1 = X_1 + \cdots + X_n$, $\Sigma_n = X_1 \cdots X_n$, et plus généralement :

$$\Sigma_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} X_{i_1} X_{i_2} \cdots X_{i_k} .$$

Ainsi Σ_k est homogène de degré k.

5.2. Théorème fondamental

Soit A un anneau, et $A[S_1, \ldots S_n]$ l'anneau des polynômes en n indéterminées $S_1, \ldots S_n$ à coefficients dans A.

5.2.1. Définitions. Soit $P = S_1^{m_1} \cdots S_n^{m_n}$ un monôme. On appelle *poids de P* l'entier naturel $m_1 + 2m_2 + \cdots + nm_n = \sum_{k=1}^{n} km_k$. Soit $P \in A[S_1, \ldots S_n]$. On appelle *poids de P*, et on note $w(P)$, le plus grand poids d'un monôme figurant dans P; si P est nul, on convient que $w(P) = -\infty$. On dit que P est *isobare de poids d* si tous les monômes figurant dans P sont de poids d.

5.2.2. Théorème. *Soit n un entier naturel, A un anneau, et soit $\mathfrak{s}_n$ le morphisme de A-algèbres*

$$\begin{aligned} A[S_1, \ldots, S_n] &\longrightarrow A[X_1, \ldots, X_n] \\ Q &\longmapsto Q(\Sigma_1, \ldots, \Sigma_n) . \end{aligned}$$

Alors $\mathfrak{s}_n$ est injectif, d'image $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$.
De plus pour $Q \in A[S_1, \ldots S_n]$, Q est de poids d (resp. isobare de poids d) si et seulement si $\mathfrak{s}_n(Q)$ est de degré d (resp. homogène de degré d).

DEMONSTRATION.
Tout d'abord quelques considérations sur les poids et les degrés. Pour $Q = S_1^{m_1} \cdots S_n^{m_n}$, monôme de poids $m_1 + 2m_2 + \cdots + nm_n$, on a $\mathfrak{s}_n(Q) = {\Sigma_1}^{m_1} \cdots {\Sigma_n}^{m_n}$, qui est un polynôme homogène de degré $m_1 + 2m_2 + \cdots + nm_n$; ainsi, si Q est isobare de poids d, $\mathfrak{s}_n(Q)$ est homogène de degré d.
Il en résulte immédiatement que, pour Q quelconque, on a toujours $\deg \mathfrak{s}_n(Q) \leq w(Q)$.
Si de plus $\mathfrak{s}_n$ est injectif, on a l'égalité, et dans ce cas Q est isobare de degré d si et seulement si son image par $\mathfrak{s}_n$ est homogène de degré d.
Pour démontrer le théorème, on procède par récurrence sur n; notons $\Sigma_k^{(n)}$ le k-ième polynôme symétrique élémentaire en les variables $X_1, \ldots\ X_n$.
L'énoncé est évident pour $n = 0$ car $\mathfrak{s}_0$ n'est autre que l'identité de A.
Supposons l'énoncé vrai pour $n-1$, avec $n \geq 1$, et montrons-le pour n.
Pour $P \in A[X_1, \ldots, X_n]$, notons $\widetilde{P}$ le polynôme $P(X_1, \ldots, X_{n-1}, 0) \in A[X_1, \ldots X_{n-1}]$.
Observons qu'on a $\deg \widetilde{P} \leq \deg P$, et que si P est symétrique, il en va de même de $\widetilde{P}$. En particulier, on a $\widetilde{\Sigma}_k^{(n)} = \Sigma_k^{(n-1)}$ pour $k = 0, 1, \ldots, n-1$, et $\widetilde{\Sigma}_n^{(n)} = 0$.

Supposons $\mathfrak{s}_n$ non injectif, et soit Q un élément non nul de son noyau; on choisit Q de degré minimal.
On a par hypothèse $Q(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}) = 0$; substituant 0 à X_n dans cette identité, ce qui revient à lui appliquer le morphisme de A-algèbres $P \mapsto \widetilde{P}$, il vient

$$Q(\Sigma_1^{(n-1)}, \ldots, \Sigma_{n-1}^{(n-1)}, 0) = 0\,,$$

ce qui revient à dire que $Q(S_1, \ldots, S_{n-1}, 0)$ est un élément du noyau du morphisme $\mathfrak{s}_{n-1}$.
Ce dernier étant par hypothèse de récurrence injectif, on en déduit : $Q(S_1, \ldots, S_{n-1}, 0) = 0$.
En vertu de **4.2.7,** Q est de la forme $S_n Q'$, avec $Q' \in A[S_1, \ldots, S_n]$.
On a $\deg Q' = \deg Q - 1 < \deg Q$. D'autre part, $\mathfrak{s}_n(Q) = 0 = \mathfrak{s}_n(S_n)\,\mathfrak{s}_n(Q') = X_1 \cdots X_n\, \mathfrak{s}_n(Q')$; puisque les X_i sont réguliers dans $A[X_1, \ldots, X_n]$ (toujours par **4.2.7**), on en déduit $\mathfrak{s}_n(Q') = 0$, ce qui contredit le choix de Q.
D'où l'injectivité de $\mathfrak{s}_n$. En particulier, $\mathfrak{s}_n$ vérifie la propriété sur les poids et les degrés.
Il est clair que l'image de $\mathfrak{s}_n$ est constituée de polynômes symétriques. Supposons qu'il existe un polynôme $P \in A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ qui ne soit pas dans l'image de $\mathfrak{s}_n$, et choisissons-le de degré minimal.
Par hypothèse de récurrence, $\widetilde{P}$, qui est symétrique, est de la forme $\mathfrak{s}_{n-1}(Q)$ pour un certain $Q \in A[S_1, \ldots, S_{n-1}]$. De plus, on a $w(Q) = \deg \widetilde{P} \leq \deg P$. On peut voir Q comme un polynôme en $S_1, \ldots, S_n$ où l'indéterminée S_n n'apparaît pas. Posons $P_0 = \mathfrak{s}_n(Q)$; alors on a $\widetilde{P_0} = \widetilde{P}$, et d'autre part, P_0 est de degré $= w(Q) \leq \deg P$. Posons $P_1 = P - P_0$. Alors P_1 est symétrique, de degré $\leq \deg P$, et vérifie $\widetilde{P_1} = 0$; c'est donc un élément de l'idéal (X_n).
Ce qui veut dire que dans tout monôme figurant dans P_1, l'indéterminée X_n apparaît avec un exposant ≥ 1. Il en va de même de toutes les indéterminées, car P_1 est symétrique.
Autrement dit, P_1 s'écrit $P_1 = X_1 \cdots X_n P' = \Sigma_n^{(n)} P'$, avec $P' \in A[X_1, \ldots, X_n]$. De plus une telle écriture est unique, car les X_i sont réguliers dans $A[X_1, \ldots, X_n]$. Il en résulte que P' est symétrique, puisque pour tout $\sigma \in \mathfrak{S}_n$, on a $P = {}^{\sigma}P = \Sigma_n^{(n)\sigma} P'$.
Puisque P' est symétrique de degré $\deg P_1 - n < \deg P$, il appartient à l'image de $\mathfrak{s}_n$ d'après le choix de P. Or on a $P = \mathfrak{s}_n(Q) + P'\mathfrak{s}_n(S_n)$ donc P appartient à l'image de $\mathfrak{s}_n$, ce qui contredit l'hypothèse. □

5.2.3. Exemples.
1) Soit $P = \sum_{\substack{1 \leq i,j \leq n \\ i \neq j}} X_i^2 X_j$, et supposons $n \geq 3$.

Puisque P est symétrique, il existe un unique polynôme $G \in \mathbb{Z}[S_1, \ldots, S_n]$ tel que $P = G(\Sigma_1, \ldots, \Sigma_n)$; et, P étant homogène de degré 3, G est isobare de poids 3, donc de la forme $a{S_1}^3 + bS_1S_2 + cS_3$. On a $P(1, 0, \ldots, 0) = 0 = a$, donc $a = 0$; $P(1, 1, 0, \ldots, 0) = 2 = 2b$, donc $b = 1$, et $P(1, 1, 1, 0, \ldots, 0) = 6 = 9b + c$, donc $c = -3$. D'où

$$P = \Sigma_1\Sigma_2 - 3\Sigma_3\,.$$

2) Soit $S^k = {X_1}^k + {X_2}^k + \cdots + {X_n}^k$.
On a alors les formules de récurrence suivantes :

$$(1) \quad \text{si } k \leq n\ :\quad S^k - \Sigma_1 S^{k-1} + \Sigma_2 S^{k-2} + \cdots + (-1)^{k-1}\Sigma_{k-1}S_1 + (-1)^k k\Sigma_k = 0\,,$$

$$(2) \qquad \text{si } k \geq n : \quad S^k - \Sigma_1 S^{k-1} + \Sigma_2 S^{k-2} + \cdots + (-1)^{k-1}\Sigma_{k-1}S_1 + (-1)^k \Sigma_k S_0 = 0\,.$$

Démontrons ces formules. On a dans $A[X_1,\ldots,X_n][T]$: $\prod_{i=1}^{n}(T + X_i) = \sum_{k=0}^{n} T^{n-k}\Sigma_k$.
Substituant $-X_j$ à T, il vient :

$$X_j^n - X_j^{n-1}\Sigma_1 + \cdots + (-1)^{n-1}X_j\Sigma_{n-1} + (-1)^n\Sigma_n = 0\,.$$

Si $k \geq n$, on obtient la formule (2) en multipliant cette équation par X_j^{k-n}, et en sommant sur j.
Supposons $k \leq n$, et posons

$$P = S^k - \Sigma_1 S^{k-1} + \Sigma_2 S^{k-2} + \cdots + (-1)^{k-1}\Sigma_{k-1}S_1 + (-1)^k k\Sigma_k\,.$$

Alors $P(X_1,\ldots,X_k,0,\ldots,0)$, vu comme un polynôme symétrique en $X_1,\ldots,X_k$, n'est autre que le membre de gauche de l'équation (2) en k variables, avec $n = k$. Il est donc nul.
Puisque P est symétrique, il en résulte que chaque fois qu'on substitue 0 à $n-k$ des indéterminées $X_1,\ldots,X_n$, on obtient zéro. Cela signifie que dans tout monôme figurant dans P, il apparaît au moins $k+1$ des indéterminées. Or, P est homogène de degré k, et dans un monôme de degré k apparaissent au plus k des indéterminées, donc P est nul.

5.2.4. Fractions rationnelles symétriques

Soit K un corps, et $n \in \mathbb{N}$. Le corps des fractions de $K[X_1,\ldots,X_n]$ est appelé *corps des fractions rationnelles en les indéterminées $X_1,\ldots X_n$ à coefficients dans K*. On le note $K(X_1,\ldots,X_n)$.
Puisque $K[X_1,\ldots,X_n]$ est factoriel, tout $q \in K(X_1,\ldots,X_n)$ non nul s'écrit $q = P/Q$, avec P, $Q \in K[X_1,\ldots X_n]$ non nuls, et on peut supposer P et Q premiers entre eux; une telle écriture est alors unique à multiplication de P et Q par un scalaire non nul près.
C'est un fait général que si $f : A \longrightarrow B$ un morphisme d'anneaux injectif, avec B intègre (et donc A aussi), f se prolonge de manière unique en un morphisme de corps $\mathsf{Frac}(A) \longrightarrow \mathsf{Frac}(B)$; c'est le morphisme défini par $p/q \mapsto f(p)/f(q)$.)
En particulier pour $\sigma \in \mathfrak{S}$, l'automorphisme $\rho(\sigma)$ de $K[X_1,\ldots,X_n]$ se prolonge de manière unique en un automorphisme de $K(X_1,\ldots,X_n)$. Concrètement, cela revient à poser ${}^\sigma q =^\sigma P/^\sigma Q$ pour $q = P/Q$, avec P, $Q \in K[X_1,\ldots,X_n]$, $Q \neq 0$.
Cela définit une action à gauche de $\mathfrak{S}_n$ sur $K(X_1,\ldots,X_n)$. On dit que q est *symétrique* si pour tout $\sigma \in \mathfrak{S}_n$, on a ${}^\sigma q = q$. L'ensemble des fractions rationnelles symétriques, noté $K(X_1,\ldots,X^n)^{\mathfrak{S}_n}$, est un sous-corps de $K(X_1,\ldots X_n)$.
Le morphisme injectif de K-algèbres $K[S_1,\ldots,S_n] \longrightarrow K[X_1,\ldots,X_n]$, $S_i \mapsto \Sigma_i$, se prolonge de façon unique en un morphisme de K-algèbres

$$K(S_1,\ldots,S_n) \longrightarrow K(X_1,\ldots,X_n)\,.$$

Si $p = F/G$, avec F, $G \in K[S_1,\ldots,S_n]$, $G \neq 0$, son image, $F(\Sigma_1,\ldots,\Sigma_n)/G(\Sigma_1,\ldots,\Sigma_n)$, sera notée $p(\Sigma_1,\ldots,\Sigma_n)$.

5.2.5. Théorème. *Le morphisme de corps*

$$\begin{aligned} \mathfrak{s} : K(S_1, \ldots, S_n) &\longrightarrow K(X_1, \ldots, X_n) \\ p &\longmapsto p(\Sigma_1, \ldots, \Sigma_n) \end{aligned}$$

est injectif, d'image $K(X_1, \ldots, X_n)^{\mathfrak{S}_n}$.

DEMONSTRATION. Tout morphisme de corps est injectif (l'image d'un élément non nul, donc inversible, est inversible, donc non nulle); c'est en particulier le cas de $\mathfrak{s}$.
Montrons la surjectivité de $\mathfrak{s}$. En vertu de **5.2.1,** il suffit de montrer que toute fraction rationnelle symétrique $q \in K(X_1, \ldots, X_n)$ s'écrit P/Q, avec P, $Q \in K[X_1, \ldots, X_n]^{\mathfrak{S}_n}$, et $Q \neq 0$. Or q s'écrit P_0/Q_0, avec P_0, $Q_0 \in K[X_1, \ldots, X_n]$ et $Q_0 \neq 0$. Posons

$$Q = \prod_{\sigma \in \mathfrak{S}_n} {}^{\sigma}Q_0 \text{ et } P = P_0 \prod_{\sigma \in \mathfrak{S}_n - \{e\}} {}^{\sigma}Q_0 \, ;$$

alors on a $q = P_0/Q_0 = P/Q$, et Q est symétrique. On a pour tout $\sigma \in \mathfrak{S}_n$: ${}^{\sigma}q = q$, donc ${}^{\sigma}P/{}^{\sigma}Q = {}^{\sigma}P/Q = P/Q$, d'où ${}^{\sigma}P = P$, et P est lui aussi symétrique. □

5.3. Polynômes antisymétriques

Soit A un anneau, et $n \in \mathbb{N}$.
Posons

$$\delta = \prod_{1 \leq i < j \leq n} (X_j - X_i) \in A[X_1, \ldots X_n] \, .$$

Supposons que dans A, on ait $1 \neq -1$ (c'est le cas si $A = \mathbb{Z}$).
Soit $\sigma \in \mathfrak{S}_n$; alors ${}^{\sigma}\delta = \prod_{1 \leq i < j \leq n} (X_{\sigma(j)} - X_{\sigma(i)})$; on constate que les facteurs de ce produit sont, au signe près, les mêmes que ceux figurant dans l'expression de δ. Il existe donc un unique élément $\varepsilon(\sigma) \in \{1, -1\}$ tel qu'on ait ${}^{\sigma}\delta = \varepsilon(\sigma)\delta$. Plus précisément,

$$\varepsilon(\sigma) = (-1)^{\#\{(i,j) | 1 \leq i < j \leq n \text{ et } \sigma(i) > \sigma(j)\}} \, .$$

Pour σ, $\tau \in \mathfrak{S}_n$, on a ${}^{\sigma\tau}\delta = {}^{\sigma}({}^{\tau}\delta)$, d'où : $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. Ainsi, $\varepsilon : \mathfrak{S}_n \longrightarrow \{1, -1\}$ est un morphisme de groupes. Si σ est la transposition échangeant i et $i+1$ ($i = 1, \ldots, n-1$) on a $\varepsilon(\sigma) = -1$; donc ε n'est autre que la signature.

5.3.1. Définition. On dit que $P \in A[X_1, \ldots X_n]$ est *antisymétrique* si pour tout $\sigma \in \mathfrak{S}_n$, ${}^{\sigma}P = \varepsilon(\sigma)P$.

5.3.2. Théorème. *Soit A un anneau où la multiplication par 2 est injective.*
Tout polynôme antisymétrique $P \in A[X_1, \ldots, X_n]$ s'écrit de manière unique $P = \delta Q$, où $Q \in A[X_1, \ldots, X_n]$ est un polynôme symétrique.

DEMONSTRATION. Soit P un polynôme antisymétrique, et soient i, j des entiers tels que $1 \leq i < j \leq n$. Soit σ la transposition qui échange i et j. On a ${}^{\sigma}P = \varepsilon(\sigma)P = -P$, autrement dit $P +^{\sigma} P = 0$. Substituant X_i à X_j dans cette égalité, il vient

$$2P(X_1, \dots, X_{i-1}, X_i, X_{i+1}, \dots, X_{j-1}, X_i, X_{j+1}, \dots, X_n) = 0\,,$$

donc on a :

$$P(X_1, \dots, X_{i-1}, X_i, X_{i+1}, \dots, X_{j-1}, X_i, X_{j+1}, \dots, X_n) = 0$$

puisque la multiplication par 2 est injective dans A.

5.3.3. Lemme. *Soit A un anneau, et $P \in A[X_1, \dots, X_n]$. Si pour tous i, j, $1 \leq i < j \leq n$, on a $P(X_1, \dots, X_{i-1}, X_i, X_{i+1}, \dots, X_{j-1}, X_i, X_{j+1}, \dots, X_n) = 0$, il existe un unique $Q \in A[X_1, \dots, X_n]$ tel que $P = \delta Q$.*

Avant de démontrer ce lemme, montrons comment il permet de conclure. Le polynôme P s'écrit de façon unique δQ. Pour tout $\sigma \in \mathfrak{S}_n$, on a $P = \varepsilon(\sigma)^{\sigma}P = \varepsilon(\sigma)^{\sigma}\delta^{\sigma}Q = \delta^{\sigma}Q$, et, par unicité de Q, ${}^{\sigma}Q = Q$, donc Q est symétrique, ce qui achève la démonstration du théorème. □

DEMONSTRATION DE **5.3.3.** Soit $1 \leq i < j \leq n$. On peut voir P comme un polynôme en X_j à coefficients dans $B_j = A[X_1, \dots, X_{j-1}, X_{j+1}, \dots, X_n]$, La condition de l'énoncé signifie que $X_i \in B_j$ est une racine de ce polynôme. Autrement dit, lorsqu'on pose la division euclidienne de P par $X_j - X_i$ dans l'anneau $B_j[X_j]$, P s'écrit de manière unique sous la forme $P = Q_{i,j}(X_j - X_i) + R$, avec $R \in B_j$, le reste R est nul. On a donc $P = Q_{i,j}(X_j - X_i)$, De plus $X_j - X_i$ n'est pas diviseur de 0. On utilisera le lemme suivant.

Lemme. *Soit A un anneau, $f_1, \dots, f_n$ des éléments de A. On suppose que les f_k sont réguliers, et qu'on a pour $k \neq k'$: $(f_k) \cap (f_{k'}) = (f_k f_{k'})$. Alors $(f_1) \cap (f_2) \cap \dots \cap (f_n) = (f_1 f_2 \cdots f_n)$.*

DEMONSTRATION. On a toujours l'inclusion $(f_1 \cdots f_n) \subset (f_1) \cap \dots \cap (f_n)$; il s'agit donc de montrer l'inclusion inverse. On procède par récurrence sur n. C'est immédiat si $n = 1$. Soit $n \geq 2$, supposons le lemme vrai pour $n-1$, et vérifions-le pour n. Soit $g \in (f_1) \cap \dots \cap (f_n)$; alors g appartient à $(f_1) \cap \dots \cap (f_{n-1})$, donc il s'écrit $af_1 \cdots f_{n-1}$ par hypothèse de récurrence. D'autre part, g appartient à $(f_1) \cap (f_n) = (f_1 f_n)$, donc il s'écrit $bf_1 f_n$. Puisque f_1 est régulier, on a $af_2 \cdots f_{n-1} = bf_n \in (f_2) \cap \dots \cap (f_n)$. Par hypothèse de récurrence, cet élément s'écrit donc $cf_2 \cdots f_n$, et on a $g = cf_1 \cdots f_n$. □

Revenons à la démonstration de **5.3.3.**
Les $X_j - X_i$ sont réguliers ($j > i$). D'autre part, soient $\alpha = X_j - X_i$ et $\beta = X_{j'} - X_{i'}$ deux tels éléments, supposés distincts. Montrons $(\alpha) \cap (\beta) \subset (\alpha\beta)$. Parmi les indices i, i', j, j', il en est un qui est distinct de tous les autres. Supposons, pour fixer les idées, que ce soit le cas de j. On a alors X_i, $X_{i'}$, $X_{j'} \in B_j$. Soit P un élément de $(\alpha) \cap (\beta)$. On le voit comme un polynôme en X_j à coefficients dans B_j. Puisqu'on a $P \in (\beta)$, P s'écrit βP_0. D'autre part, la division euclidienne de P_0 par $\alpha = X_j - X_i$

dans l'anneau $B_j[X_j]$ s'écrit $P_0 = P_1\alpha + P_0(X_i)$. Ainsi, $P = \alpha\beta P_1 + \beta P_0(X_i)$. Or on a $\beta P_0(X_i) = (X_{j'} - X_{i'})P_0(X_i) \in B_j$, donc cet élément est le reste dans la division euclidienne de P par α dans l'anneau $B_j[X_j]$; ce reste est nul, puisque $P \in (\alpha)$, donc $P = \alpha\beta P_1 \in (\alpha\beta)$.
On peut donc appliquer le lemme ci-dessus aux éléments $X_j - X_i$; il vient :

$$\bigcap_{1\le i<j\le n}(X_j - X_i) = (\prod_{1\le i<j\le n}(X_j - X_i)) = (\delta)$$

ce qui achève la démonstration de **5.3.3.** □

5.4. Rapport entre coefficients et racines d'un polynôme

5.4.1. Proposition. *Soit A un anneau, et $P = a_0X^n + a_1X^{n-1} + \cdots + a_n$ un polynôme en X à coefficients dans A. Supposons qu'il existe des éléments c, $x_1, \ldots, x_n$ de A tels qu'on ait*

$$P = c\prod_{i=1}^{n}(X - x_i)\,.$$

Alors pour tout $k = 0, \ldots, n$ on a

$$a_k = (-1)^k c\Sigma_k(x_1, \ldots, x_n)\,.$$

Demonstration. Par définition des polynômes symétriques élémentaires, on a dans $A[T, X_1, \ldots, X_n]$:

$$\prod_{i=1}^{n}(T + X_i) = \sum_{k=0}^{n} T^{n-k}\Sigma_k(X_1, \ldots, X_n)\,.$$

Quand on substitue $-x_i$ à X_i pour tout i, il vient :

$$\prod_{i=1}^{n}(T - x_i) = \sum_{k=0}^{n} T^{n-k}\Sigma_k(-x_1, \ldots, -x_n)\,.$$

Comme Σ_k est homogène de degré k, on obtient :

$$\prod_{i=1}^{n}(T - x_i) = \sum_{k=0}^{n}(-1)^k\Sigma_k(x_1, \ldots, x_n)T^{n-k}\,.$$

Par conséquent, on a

$$P(T) = \sum_{k=0}^{n} a_kT^{n-k} = c\prod_{i=1}^{n}(T - x_i) = \sum_{k=0}^{n}(-1)^k c\Sigma_k(x_1, \ldots, x_n)T^{n-k}\,;$$

on en déduit les formules annoncées en identifiant les coefficients de T^{n-k}. □

5.4.2. Définition. Soit L un corps et K un sous-corps de L. Soit $P \in K[X]$ un polynôme de degré $n > 0$. On dit que P *est scindé dans* L s'il existe des éléments $c, z_1, \ldots, z_n \in L$ tels qu'on ait :

$$P = c(X - z_1)(X - z_2)\ldots(X - z_n) \quad \text{dans} \quad L[X]\,.$$

Les éléments $z_1, \ldots, z_n$ sont appelés les *racines de* P *dans* L.

5.4.3. Proposition. *Soit* $P \in K[X]$ *; on l'écrit* $P(X) = a_0x^n + a_1x^{n-1} + \cdots + a_n$. *On suppose* P *scindé dans* L*; on a donc*

$$P(X) = c(X - z_1)\ldots(X - z_n) \quad \textit{dans} \quad L[X]\,.$$

Alors les coefficients $a_0, a_1, \ldots, a_n$ *sont donnés par les formules*

$$a_0 = c, \ \ \textit{et pour} \ \ k = 1, \ldots, n, \quad a_k = (-1)^k a_0 \Sigma_k(z_1, \ldots, z_n)\,.$$

Demonstration. Résulte immédiatement de **5.4.1.** □

5.5. Résultants et discriminant

5.5.1. Déterminant d'une matrice carrée

Soit A un anneau (commutatif) et $M = (a_{i,i})_{1\le i,j\le n} \in M_n(A)$. On appelle *déterminant de* M, et on note $\det M$, l'élément de A défini par la formule :

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

5.5.2. Remarques.
1) Le déterminant de l'unique élément de $M_0(A)$ est 1; en effet, $\mathfrak{S}_0$ est réduit à un seul élément, de signature 1, et le produit de la famille vide vaut 1.
2) On a les règles de calcul usuelles.

(i) Le déterminant de la transposée d'une matrice carrée M est égal à celui de M.

(ii) Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Soit $M = (a_{i,j})_{1\le i,j\le n} \in M_n(A)$, et notons $f(M)$ la matrice $(f(a_{i,j}))_{1\le i,j\le n} \in M_n(B)$. Alors $\det f(M) = f(\det(M))$.

(iii) Lorsqu'on permute les vecteurs colonnes d'une matrice, le déterminant de la matrice est multiplié par la signature de la permutation effectuée. (De même pour les vecteurs lignes.)

(iv) Si une matrice carrée M est triangulaire (supérieure ou inférieure) par blocs, son déterminant est le produit des déterminants des blocs diagonaux.
Autrement dit : soient n_1 et n_2 des entiers naturels tels que $n = n_1 + n_2$; on peut voir toute matrice $M \in M_n(A)$ comme une matrice par blocs

$$M = \begin{pmatrix} M_{1,1} & M_{1,2} \\ M_{2,1} & M_{2,2} \end{pmatrix},$$

où chaque $M_{i,j}$ est une matrice à n_i lignes et n_j colonnes. Si $M_{1,2} = 0$ ou $M_{2,1} = 0$, alors

$$\det M = \det M_{1,1} \det M_{2,2} .$$

(v) Le déterminant du produit de deux matrices est le produit de leurs déterminants (cf. appendice de la partie II).

5.5.2. Exemple. Soit A un anneau, $x_1, \ldots, x_n$ des éléments de A, et $W(x_1, \ldots, x_n)$ la matrice dont le coefficient i, j est ${x_j}^{i-1}$. On a :

$$\det W(x_1, \ldots, x_n) = \delta(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_j - x_i) .$$

Pour démontrer cela, on traite tout d'abord un cas particulier. Soit $\mathcal{A} = \mathbb{Z}[X_1, \ldots, X_n]$, et $W_0 = W(X_1, \ldots, X_n)$. Soit $D = \det W_0 \in \mathcal{A}$. Soit $\sigma \in \mathfrak{S}_n$. Alors

$${}^{\sigma}D = \det W(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = \varepsilon(\sigma) D$$

par (iii), donc D est un polynôme antisymétrique. En vertu du théorème **5.3.2,** $D = P\delta$, où P est un polynôme symétrique en $X_1, \ldots, X_n$. Or D est un polynôme homogène de degré $n(n-1)/2$, de même que δ. Le polynôme P est donc de degré 0 puisque $\mathcal{A}$ est intègre. D'autre part, on constate que le coefficient de $X_2 X_3^2 \ldots X_n^{n-1}$ dans D est 1, de même que dans δ. On a donc $P = 1$, d'où la formule annoncée.
En général, soit $f : \mathcal{A} \longrightarrow A$ le morphisme $P \longrightarrow P(x_1, \ldots, x_n)$. On a $f(W_0) = W(x_1, \ldots, x_n)$, donc $\det W(x_1, \ldots, x_n) = f(D)$ (par (ii)) $= f(\delta) = \delta(x_1, \ldots, x_n)$.

5.5.2. Résultant

Soit A un anneau, et m, n deux entiers naturels. Soient $a_0, \ldots, a_m$ et $b_0, \ldots, b_n$ des éléments de A, et considérons la matrice, dite *de Sylvester* :

$$\mathcal{S}(a_0, \ldots, a_m; b_0, \ldots, b_n) = \begin{pmatrix}
a_0 & & & & b_0 & & & & \\
a_1 & a_0 & & & b_1 & b_0 & & & \\
\vdots & a_1 & \ddots & & \vdots & b_1 & \ddots & & \\
\vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & \ddots & \\
\vdots & \vdots & & a_1 & b_n & \vdots & & \ddots & b_0 \\
a_m & \vdots & & \vdots & & b_n & & & b_1 \\
 & a_m & & \vdots & & & \ddots & & \vdots \\
 & & \ddots & \vdots & & & & \ddots & \vdots \\
 & & & a_m & & & & & b_n
\end{pmatrix}$$

C'est donc la matrice carrée d'ordre $n + m$, dont le coefficient i, j est a_{i-j} si $1 \leq j \leq n$ et $0 \leq i - j \leq m$, b_{m+i-j} si $n < j \leq n + m$ et $0 \leq j - i \leq n$, et 0 dans tous les autres cas.

5.5.3. Définition. Si $P = \sum_{k=0}^{m} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k$ sont deux polynômes à coefficients dans A de degrés respectifs m et n (donc a_m et b_n sont non nuls), on note $\mathcal{S}_{P,Q}$ la matrice de Sylvester $\mathcal{S}(a_0, \ldots, a_m; b_0, \ldots, b_n)$. On appelle *résultant de P et de Q*, et on note $\mathsf{Res}(P, Q)$ le déterminant de cette matrice.

5.5.4. Remarques.
1) Si P est de degré m et Q, de degré n, on a $\mathsf{Res}(Q, P) = (-1)^{mn} \mathsf{Res}(P, Q)$.
En effet, la matrice $\mathcal{S}(b_0, \ldots, b_n; a_0, \ldots, a_m)$ s'obtient en échangeant en bloc les n premières et les m dernières colonnes de la matrice de $\mathcal{S}(a_0, \ldots, a_m; b_0, \ldots, b_n)$, permutation qui se décompose en mn transpositions.
2) Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Pour $P \in A[X]$, notons $f(P)$ l'image de P par le morphisme d'anneaux $A[X] \longrightarrow B[X], \sum a_d X^d \mapsto \sum f(a_d) X^d$.
Si P et Q sont des éléments de $A[X]$ dont les coefficients directeurs ne sont pas des éléments du noyau de f, ce qui revient à dire que $f(P)$ et $f(Q)$ sont de degrés respectifs m et n, on a $\mathsf{Res}(f(P), f(Q)) = f(\mathsf{Res}(P, Q))$.
En particulier, si A est un sous-anneau de B, et si P et Q sont deux polynômes non nuls à coefficients dans A, il revient au même de calculer $\mathsf{Res}(P, Q)$ dans A ou dans B.

Nous nous intéresserons essentiellement aux polynômes à coefficients dans un corps K. Soient P, $Q \in K[X]$ non nuls avec $\deg P = n$, $\deg Q = m$. Soit $\mathcal{S}$ la matrice de Sylvester associée.
On peut interpréter $\mathcal{S}$ comme suit.
Pour $d \in \mathbb{N}$, soit $E_n = \{U \in K[X] \mid \deg U < n\}$. C'est un K-espace vectoriel, avec pour base canonique la famille des monômes X^i pour $0 \leq i < d$.
Considérons l'application linéaire

$$\begin{aligned} S : E_m \times E_n &\longrightarrow E_{m+n} \\ (U, V) &\longmapsto PU + QV \end{aligned}$$

On constate que la matrice de S dans les bases canoniques n'est autre que la matrice de Sylvester $\mathcal{S}$.
Si P et Q sont premiers entre eux, S est injective. En effet si $UP + VQ = 0$, $P \mid VQ$ donc $P \mid V$ et puisque $\deg V < \deg P$, $V = 0$; de même $U = 0$. Ainsi $\det \mathcal{S} \in K^*$. Inversement, supposons $\det \mathcal{S} \in K^*$. Alors S est bijective. Si $m + n \geq 1$, $\exists (U, V) \in E_m \times E_n \mid UP + VQ = 1$ donc P et Q sont premiers entre eux. C'est aussi le cas si $m = n = 0$.
On a donc démontré le théorème suivant.

5.5.4. Théorème. *Soit K un corps, et P, $Q \in K[X]$ deux polynômes non nuls. Alors P et Q sont premiers entre eux dans $K[X]$ si et seulement si* $\mathsf{Res}(P, Q)$ *est non nul.* □

5.5.5. Factorisation du résultant

5.5.6. Théorème. *Soit L un corps, K un sous-corps de L, et soient $P = \sum_{k=0}^{m} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k$ deux polynômes à coefficients dans K de degrés respectifs m et n.*

1) Si Q est scindé dans L, soient $y_1, \dots y_n$ ses racines. On a alors :

$$\mathsf{Res}(P,Q) = b_n^m \prod_{j=1}^{m} P(y_j)\,.$$

2) Si P est scindé dans L, soient $x_1, \dots x_m$ ses racines. On a alors :

$$\mathsf{Res}(P,Q) = (-1)^{mn} a_m^n \prod_{i=1}^{m} Q(x_i)\,.$$

3) Enfin si P et Q sont scindés dans L, de racines respectives $x_1, \dots, x_m$ et $y_1, \dots, y_n$, on a :

$$\mathsf{Res}(P,Q) = a_m^n b_n^m \prod_{i,j} (y_j - x_i)\,.$$

Remarque. L'intérêt de cet énoncé deviendra évident au chapitre III : nous verrons alors qu'étant donné un polynôme à coefficients dans un corps K, il existe toujours un corps plus grand L où P est scindé.

Demonstration. Tout d'abord, grâce à la remarque 2 ci-dessus, il revient au même de calculer le résultant de P et Q sur K ou sur L. On peut donc supposer $K = L$.
Remarquons maintenant que (2) et (3) résultent de (1).
En effet, grâce à la remarque 1, (2) se ramène à (1) en échangeant les rôles de P et de Q; enfin sous les hypothèses de (3), on a d'après (1) : $\mathsf{Res}(P,Q) = b_n^m \prod_{j=1}^m P(y_j)$, et remplaçant $P(y_i)$ par sa valeur $a_m \prod_{i=1}^m (y_j - x_i)$, on obtient (3).
L'assertion (1) sera conséquence immédiate du lemme suivant.

5.5.7. Lemme. (Multiplicativité du résultant)
Soient P_0, P_1, $Q \in K[X]$ non nuls. Alors

$$\mathsf{Res}(P_0P_1, Q) = \mathsf{Res}(P_0, Q)\ \mathsf{Res}(P_1, Q) \ \text{ et } \ \mathsf{Res}(Q, P_0P_1) = \mathsf{Res}(Q, P_0)\ \mathsf{Res}(Q, P_1)\,.$$

Demonstration. Cette propriété importante se lira facilement une fois que nous aurons ré-interprété le résultant.
Soit $Q \in K[X]$ de degré $n \geq$ fixé. Si $R \in K[X]$, notons $\overline{R}$ la classe de R modulo Q.
L'application $E_n \to K[X]/(Q)$, $R \mapsto \overline{R}$, est un isomorphisme de K-espaces vectoriels. C'est une conséquence de la division euclidienne : tout polynôme $W \in K[X]$ s'écrit de manière unique $W = q(W)Q + r(W)$, avec $q(W) \in K[X]$ et $r(W) \in E_n$.
Si $P \in K[X]$, la multiplication par $\overline{P}$ est un endomorphisme du K-espace vectoriel $K[X]/(Q)$. Notons $M_Q(P)$ cet endomorphisme.

5.5.8. Lemme. *Soit $P \in K[X]$ non nul et soit b_m le coefficient directeur de Q. Alors*

$$\mathsf{Res}(P,Q) = (b_m)^{\deg P} \det M_Q(P)\,.$$

DEMONSTRATION. Soit n le degré de P et $S : E_m \times E_n \to E_{m+n}$, $(U,V) \mapsto UP+VQ$. Dans les bases canoniques, $\det S = \mathsf{Res}(P,Q)$. Par ailleurs soit $D : E_{m+n} \to E_m \times E_n$, $W \mapsto (r(W), q(W))$.
On a $DS(U,V) = (r(UP+VQ), q(UP+VQ)) = (r(UP), q(UP)+Q)$. La matrice par blocs de DS est donc de la forme

$$\begin{pmatrix} A & 0 \\ * & 1_n \end{pmatrix},$$

où A est la matrice de $M_Q(P)$ dans la base $(\overline{X}^i)_{0\le i<m}$. On a donc $\det DS = \det A = \det M_Q(P)$. Par ailleurs $\det DS = \det D \det S$. Or, on a $D(X^i) = (X^i, 0)$ pour $i < m)$, donc la matrice de D dans les bases canoniques est de la forme

$$\begin{pmatrix} 1_m & * \\ 0 & T \end{pmatrix},$$

où T est une matrice $n \times n$. De plus pour $i \ge m$, $q(X^i) = {b_m}^{-1} X^{i-m} +$ termes de degré $< i-m$, donc T est triangulaire supérieure avec termes diagonaux égaux à ${b_m}^{-1}$. On a donc $\det D = {b_m}^{-n}$, d'où $\det S = {b_m}^{n} \det M_Q(P)$. □
Achevons la démonstration du lemme **5.5.7.** On a $\mathsf{Res}(P_0P_1, Q) = (b_m)^{\deg P_0P_1} \det M_Q(P_0P_1)$. Or $M_Q(P_0P_1) = M_Q(P_0) \circ M_Q(P_1)$; on a donc

$$\mathsf{Res}(P_0P_1, Q) = (b_m)^{\deg P_0 + \deg P_1} \det M_Q(P_0) \det M_Q(P_1) = \mathsf{Res}(P_0, Q)\, \mathsf{Res}(P_1, Q),$$

d'où la première identité; la seconde en résulte par la remarque 1. □

Démontrons maintenant l'assertion (1) du théorème. On a par hypothèse $Q = b_m(X - y_1)\dots(X-y_n)$, et grâce à la multiplicativité du résultant, il suffit de vérifier les cas $Q = b \in K^*$ et $Q = (X-y)$, $y \in K$. Si $Q = b$, $K/(Q) = 0$, $\det M_Q(P) = 1$ donc $\mathsf{Res}(P,Q) = b^{\deg P}$. Si $Q = X - y$, $K/(Q)$ est de dimension 1, $M_Q(P)$ est la multiplication par $P(y)$, donc $\mathsf{Res}(P, X-y) = P(y)$. □

5.5.6. Discriminant

Soit $\mathcal{A}$ l'anneau $\mathbb{Z}[A_0, \dots, A_n]$ et $P = A_nX^n + \cdots + A_0 \in \mathcal{A}[X]$. On a

$$Res(P, P') = \det \mathcal{S}(A_0, \dots, A_n; A_1, \dots nA_n).$$

La dernière ligne de $\mathcal{S}(A_0, \dots, A_n; A_1, \dots, nA_n)$ comporte un coefficient A_n et un coefficient nA_n; tous les autres coefficients de la ligne sont nuls.
Il existe donc un polynôme $\mathsf{Disc} \in \mathcal{A}$ tel qu'on ait

$$A_n\, \mathsf{Disc}(A_0, \dots, A_n) = (-1)^{n(n-1)/2}\, \mathsf{Res}(P, P').$$

5.5.7. Définition. Soit A un anneau et $P \in A[X]$ un polynôme de degré n, de la forme $P = a_n X^n + \cdots + a_0$. L'élément $\mathsf{Disc}(a_0, \ldots, a_n) \in A$ est appelé *discriminant de* P, et noté $\mathsf{Disc}\, P$.
Si P' est de degré $n-1$ (c'est-à-dire si $na_n \neq 0$), on a donc

$$\mathsf{Res}(P, P') = (-1)^{n(n-1)/2} a_n \,\mathsf{Disc}\, P\,.$$

5.5.8. Théorème. *Soit L un corps et K un sous-corps de L. Soit $P \in K[X]$ un polynôme de degré n de la forme $P = a_n X^n + \cdots + a_0$. Supposons P scindé dans L, et notons $x_1, \ldots, x_n$ ses racines.*
Alors on a

$$\mathsf{Disc}(P) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (x_j - x_i)^2 = (-1)^{n(n-1)/2} a_n^{n-2} \prod_i P'(x_i)\,.$$

Demonstration.
On a $\mathsf{Res}(P, P') = (-1)^{n(n-1)/2} a_n \,\mathsf{Disc}\, P$; d'autre part

$$\mathsf{Res}(P, P') = a_n^{n-1} \prod_{i=1}^{n} P'(x_i)\,.$$

D'où

$$\mathsf{Disc}\, P = (-1)^{n(n-1)/2} a_n^{n-2} \prod_i P'(x_i)\,.$$

Par ailleurs,

$$P'(x_i) = a_0 \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (x_i - x_j)\,,$$

donc

$$\mathsf{Disc}\, P = (-1)^{n(n-1)/2} a_n^{2n-2} \prod_{1 \leq i \neq j \leq n} (x_i - x_j) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (x_j - x_i)^2\,. \quad \square$$

En particulier, $\mathsf{Disc}(P) = 0 \iff P$ admet une racine multiple dans L.

Exemples.
Si $P = aX^2 + bX + c$, avec $a \neq 0$, $\mathsf{Disc}\, P = b^2 - 4ac$.
Si $P = X^3 + pX + q$, $\mathsf{Disc}\, P = -4p^3 - 27q^2$.

Chapitre II : Modules

1. Généralités sur les modules

Dans ce chapitre, les anneaux seront supposés commutatifs (sauf mention explicite du contraire).

1.1. Introduction de la notion de module

Soit A un anneau.

1.1.1. Définition. On appelle A-*module* la donnée d'un ensemble M muni d'une loi de composition interne $+$ et d'une loi de composition externe $\cdot : A \times M \longrightarrow M$ vérifiant les conditions suivantes :
1) $(M, +)$ est un groupe abélien;
2) pour tout $a \in A$, pour tous $x,\ y \in M$, $a \cdot (x+y) = a \cdot x + a \cdot y$;
2') pour tout $x \in M$, pour tous $a,\ b \in A$, $(a+b) \cdot x = a \cdot x + b \cdot x$;
3) pour tout $x \in M$ et pour tous $a,\ b \in A$, $a \cdot (b \cdot x) = (ab) \cdot x$
3') pour tout $x \in M$, $1 \cdot x = x$.

Pour $a \in A$ et $x \in M$, l'élément $a \cdot x$ sera généralement noté ax.

1.1.2. Remarques.
1) Si K est un corps, les K-modules ne sont autres que les K-*espaces vectoriels*.
2) Soit $(M, +)$ un groupe abélien. Les endomorphismes de groupes de M constituent un anneau, en général non commutatif, noté $\mathsf{End}(M)$.
La donnée d'une loi de composition externe $\cdot : A \times M \longrightarrow M$ équivaut à la donnée de l'application $\rho : A \longrightarrow M^M$ qui associe à tout élément a de A l'application

$$\begin{aligned} \rho(a) : M &\longrightarrow M \\ x &\mapsto a \cdot x\,. \end{aligned}$$

Dans ces conditions, l'axiome 2) signifie que pour tout a, $\rho(a)$ est un endomorphisme de groupes de M. Ainsi, ρ peut être vu comme une application de A dans $\mathsf{End}(M)$. Les axiomes 2'), 3) et 3') signifient que ρ est un morphisme d'anneaux de A vers $\mathsf{End}(M)$.
Autrement dit, se donner une structure de A-module sur un groupe abélien $(M, +)$ équivaut à se donner un morphisme d'anneaux de A vers $\mathsf{End}(M)$.
3) En particulier, se donner un $\mathbb{Z}$-module revient exactement à se donner un groupe abélien.
4) L'anneau A est un A-module. En effet, l'addition et la multiplication de A, vue comme une loi de composition externe, satisfont aux conditions de la définition **1.1.1.**

1.2. Sous-modules, applications linéaires

1.2.1. Définition. Soit M un A-module. On dit qu'une partie N de M est un *sous-module de* M si les conditions suivantes sont satisfaites :
1) N est un sous-groupe de $(M, +)$;
2) $\forall a \in A,\ \forall x \in N,\ a \cdot x \in N$.

1.2.2. Sorites et Notations.

On a vu que A est un A-module. Les sous-module de A ne sont autres que les idéaux de A. La notion de sous-module généralise donc la notion d'idéal, et en particulier, on peut reproduire ici presque mot à mot ce qui a été dit en **I, 2.3.1** à propos des idéaux.

Soit M un A-module. Alors $\{0\}$ est un sous-module de M, appelé *sous-module nul*, et noté 0; d'autre part M est un sous-module de M. L'intersection d'une famille quelconque de sous-modules de M est un sous-module de M. En particulier, pour toute partie X de M, il existe un plus petit sous-module de M contenant X, appelé sous-module de M engendré par X, et noté $\langle X\rangle$.

On peut décrire $\langle X\rangle$ plus précisément. On appelle *combinaison linéaire d'éléments de X (à coefficients dans A)* tout élément de M de la forme

$$\sum_{i\in F} a_i x_i\,,$$

où F est un ensemble fini, et pour $i \in F$, $a_i \in A$ et $x_i \in X$. Alors $\langle X\rangle$ n'est autre que l'ensemble des combinaisons linéaires d'éléménts de X à coefficients dans A.

Si $(M_i)_{i\in I}$ est une famille de sous-modules de M, on note $\sum\limits_{i\in I} M_i$ le sous-module de M engendré par la réunion des M_i.

Définitions. On dit que X *engendre M (comme A-module)* si $M = \langle X\rangle$. On dit que M est un *A-module de type fini* s'il est engendré par une partie finie. On dit que M est un *A-module cyclique* s'il est engendré par un élément.

1.2.3. Définition. Soient M, N deux A-modules. Une application $f : M \longrightarrow N$ est dite *A-linéaire* si elle vérifie

1) f est un morphisme de groupes de $(M,+)$ vers $(N,+)$;
2) $\forall a \in A$, $\forall x \in M$, $f(a\cdot x) = a\cdot f(x)$.

On dit alors que f est un *morphisme de A-modules de M vers N*.

1.2.4. Remarques.

1) Soient M, M' et M'' des A-modules, et $f : M \longrightarrow M'$, $g : M' \longrightarrow M''$ des applications A-linéaires; alors $g\circ f$ est une application A-linéaire de M vers M''.
L'identité d'un A-module est une application A-linéaire.
2) Si $f : M \longrightarrow M'$ est une application A-linéaire bijective, f^{-1} est A-linéaire. On dit alors que f est un *isomorphisme de A-modules.*
3) Soit M un A-module, et M' un sous-module de M. Notons i l'inclusion de M' dans M. Alors il existe sur M' une unique structure de A-module telle que i soit A-linéaire.

1.2.5. Proposition. *Soient M, M' deux A-modules, et f une application A-linéaire de M vers M'. Alors l'image de f est un sous-module de M', et le noyau de f est un sous-module de M.*

Demonstration. Puisque f est en particulier un morphisme de groupes de $(M,+)$ vers $(M',+)$, $\mathsf{Ker}\, f$ et $\mathsf{Im}\, f$ sont des sous-groupes de $(M,+)$ et $(M',+)$ respectivement. Vérifions qu'il s'agit en fait de sous-modules. Soit $x \in \mathsf{Ker}\, f$ et $a \in A$. Alors $f(ax) = af(x) = a\cdot 0 = 0$, donc $ax \in \mathsf{Ker}\, f$. De même, si $y \in \mathsf{Im}\, f$ et $a \in A$, il existe $x \in M$ tel que $y = f(x)$. On a alors $ay = f(ax) \in \mathsf{Im}\, f$. □

1.3. Exemples de A-modules

Soit A un anneau.

0) Le module nul.

Tout idéal de A est un A-module; c'est en particulier de cas de 0, qu'on appelle le *A-module nul.* Il verifie deux propriétés universelles. Pour tout A-module M, il existe une unique application A-linéaire de M dans 0, et il existe aussi une unique application A-linéaire de 0 dans M. (Ces applications sont notées 0 si nécéssaire, mais leur unicité permet souvent de se dispenser de les noter.)

1) Changement d'anneau.

Soit B un anneau muni d'un morphisme d'anneaux $\eta : A \longrightarrow B$; autrement dit, une A-algèbre. Soit M un B-module. La structure de B-module sur M correspond à la donnée d'un morphisme d'anneaux ρ de B vers l'anneau des endomorphismes de groupe $(M,+)$. Le morphisme d'anneaux $\rho \circ \eta$ fait donc de M un A-module.
Ainsi, tout B-module M peut être vu comme un A-module. Concrètement, cela revient à munir M de la multiplication externe $A \times M \longrightarrow M$, $(a,x) \mapsto \eta(a)\cdot x$.
En particulier, B est un A-module, ainsi que tout idéal de B.

2) Les modules A^I et $A^{(I)}$.

Soit I un ensemble. On a vu en **I, 1.5. 2),** que A^I est une A-algèbre, dont $A^{(I)}$ est un idéal. Ainsi A^I et $A^{(I)}$ sont des A-modules.
Pour $i \in I$, soit e_i l'élément de $A^{(I)}$ défini par $(e_i)_j = 1$ si $i = j$, 0 sinon. Alors tout élément $a = (a_i)_{i\in I}$ s'écrit

$$a = \sum_{i\in I} a_i \cdot e_i\,,$$

cette somme ayant un sens car elle ne comporte qu'un nombre fini de termes non nuls.
Ainsi, $A^{(I)}$ est engendré par les e_i pour i décrivant I.
La famille $(e_i)_{i\in I}$ est appelée la *base canonique de $A^{(I)}$*.

1.3.1. Proposition. *Soit I un ensemble. Le A-module $A^{(I)}$, muni de sa base canonique, vérifie la propriété universelle suivante.*
Pour tout A-module M et toute famille $(x_i)_{i\in I}$ d'éléments de M indexée par I, il existe une unique application A-linéaire

$$\phi : A^{(I)} \longrightarrow M$$

vérifiant $\phi(e_i) = x_i$ pour tout $i \in I$.

Demonstration. Supposons qu'un tel ϕ existe, et soit $a = (a_i)_{i\in I}$ un élément de $A^{(I)}$. Alors

$$\phi(a) = \phi(\sum_{i\in I} a_i e_i) = \sum_{i\in I} a_i \phi(e_i) = \sum_{i\in I} a_i x_i\,,$$

donc si un tel ϕ existe, il est unique. Inversement, il est clair que cette formule définit une application A-linéaire ϕ qui convient. □

3) Produits et sommes directes

Soit A un anneau, I un ensemble, et $(M_i)_{i\in I}$ une famille de A-modules indexée par I.

Définition. L'ensemble

$$\prod_{i\in I} M_i$$

muni de la loi de composition interne $+$ et de la loi de composition externe $\cdot$ définies par :

$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I} \text{ et } a\cdot (x_i)_{i\in I} = (ax_i)_{i\in I}$$

est un A-module, appelé *module produit de la famille* $(M_i)_{i\in I}$.
Pour chaque j, la projection

$$\begin{aligned} p_j : \prod_{i\in I} M_i &\longrightarrow M_j \\ (x_i)_{i\in I} &\longmapsto x_j \end{aligned}$$

est une application A-linéaire; et le module $\prod_{i\in I} M_i$, muni des projections p_j, vérifie la propriété universelle suivante.

1.3.2. Proposition. *Soit M' un A-module, et pour tout $i\in I$, donnons-nous une application A-linéaire $f_i : M' \longrightarrow M_i$. Alors il existe une unique application A-linéaire*

$$f : M' \longrightarrow \prod_{i\in I} M_i$$

vérifiant pour tout $j\in I$: $f_j = p_j \circ f$.

Demonstration. L'application f est définie par $x \mapsto (f_i(x))_{i\in I}$. $\square$

Remarque. Le module A^I n'est autre que le produit de la famille de modules définie par $M_i = A$.

Définition. Le sous-ensemble de $\prod_{i\in I} M_i$ constitué des familles presque nulles (i. e. des familles $(x_i)_{i\in I}$ telles que $\{i\in I \mid x_i \neq 0\}$ soit fini) est un sous-module, appelé *somme directe de la famille* $(M_i)_{i\in I}$, et noté

$$\bigoplus_{i\in I} M_i .$$

Pour chaque $j\in I$, l'application

$$\iota_j : M_j \longrightarrow \bigoplus_{i\in I} M_i$$

qui associe à $x\in M_j$ la suite $(y_i)_{i\in I}$ définie par $y_j = x$ si $j = i$, 0 sinon, est A-linéaire injective. On l'appelle *j-ième injection canonique.* Le module $\bigoplus_{i\in I} M_i$, muni des applications ι_j, vérifie la propriété universelle suivante.

1.3.3. Proposition. *Soit M' un A-module, et pour tout $i \in I$, donnons-nous une application A-linéaire $f_i : M_i \longrightarrow M'$. Alors il existe une unique application A-linéaire*

$$f : \bigoplus_{i \in I} M_i \longrightarrow M'$$

vérifiant pour tout $j \in I$: $f_j = f \circ \iota_j$.

DEMONSTRATION. L'application f est définie par $(x_i)_{i\in I} \mapsto \sum_{i\in I} x_i$. □

REMARQUES.
1) Si I est un ensemble fini, on a $\bigoplus\limits_{i\in I} M_i = \prod\limits_{i\in I} M_i$.
2) Le module $A^{(I)}$ n'est autre que la somme directe de la famille de modules définie par $M_i = A$.

1.3.4. Proposition. *Soit M un A-module, I un ensemble, et $(M_i)_{i\in I}$ une famille de sous-modules de M. Les deux assertions suivantes sont équivalentes.*
1) Le morphisme canonique

$$f : \bigoplus_{i \in I} M_i \longrightarrow M$$

est un isomorphisme;
2) On a

$$M = \sum_{i\in I} M_i$$

et pour tout $j \in I$,

$$M_j \cap \sum_{i\in I, i\neq j} M_i = 0\,.$$

DEMONSTRATION. Dans l'assertion 2), la première propriété est la traduction de la surjectivité de f, et la seconde, de son injectivité. □
Lorsque les conditions de la proposition **1.3.4.** sont satisfaites, on dit que M *est somme directe de ses sous-modules M_i.*

Définition. Soit M un A-module, M' et M'' deux sous-modules de M. On dit que M'' est un *supplémentaire de M' dans M* si M est la somme directe de M' et M''.

1.4. Modules quotients

1.4.1. Proposition-définition *Soit M un A-module, et M' un sous-groupe de $(M, +)$. Les deux conditions suivantes sont équivalentes :*

(i) M' est un sous-module de M;

(ii) il existe sur le groupe quotient M/M' une structure de A-module telle que la surjection canonique $\pi : M \longrightarrow M/M'$ soit A-linéaire.

En outre, si une telle structure de A-module existe sur M/M', elle est unique. Muni de cette structure, M/M' est appelé module quotient de M par M'.

DEMONSTRATION. On considère sur M la *congruence modulo* M', relation d'équivalence définie par :

$$x \equiv y \ \ (M') \Longleftrightarrow y - x \in M' .$$

L'ensemble quotient M/M' est l'ensemble des classes d'équivalence pour cette relation; et la surjection canonique $\pi : M \longrightarrow M/M'$ associe à $x \in M$ sa classe d'équivalence $\overline{x}$, qui n'est autre que $x + M'$. Il existe sur M/M' une unique loi de composition interne $+$ telle que $(M/M', +)$ soit un groupe commutatif, et π un morphisme de groupes. On a $\mathsf{Ker}(\pi) = M'$.
Suppons qu'il existe sur M/M' une multiplication $\cdot$ telle que $(M/M', +, \cdot)$ soit A-module, et π une application A-linéaire. Alors pour tout $x \in M$ et tout $a \in A$, $a \cdot \pi(x) = \pi(ax)$; comme π est surjectif, on voit qu'il y a unicité d'une telle multiplication externe. En outre, $M' = \mathsf{Ker}(\pi)$ est un sous-module de M.
Réciproquement supposons que M' soit un sous-module de M. Pour $\xi \in M/M'$, choisissons $x \in M$ tels que $\pi(x) = \xi$. Etant donné $a \in A$, l'élément $\pi(ax)$ ne dépend pas du choix de x. En effet, si $x' \equiv x \ (M')$, alors $ax' - ax = a(x' - x) \in M'$, donc $ax' \equiv ax \ (M')$. On peut donc poser $a \cdot \xi = \pi(ax)$, définissant ainsi une loi de composition externe $\cdot$: $A \times M/M' \longrightarrow M/M'$. Il est alors facile de vérifier que $(M/M', +, \cdot)$ est un A-module, et que π est A-linéaire. □

Les propositions qui suivent sont le pendant exact des propositions 1.3.2, 1.3.3 et 1.3.4 du chapitre I.

1.4.2 Proposition. (Factorisation d'un morphisme de modules)
Soit $f : M \to N$ un morphisme de A-modules, et $p : M \to M''$ un morphisme de A-modules surjectif. Les deux conditions suivantes sont équivalentes :

(i) $\mathsf{Ker}\, p \subset \mathsf{Ker}\, f$;

(ii) il existe un morphisme de A-modules $g : M'' \to N$ tel que $g \circ p = f$.

En outre si un tel g existe, il est unique; on a alors $\mathsf{Im}\, g = \mathsf{Im}\, f$, et $\mathsf{Ker}\, g = p(\mathsf{Ker}\, f)$.

DEMONSTRATION. Notons $M' = \mathsf{Ker}\, p$. Supposons qu'il existe une application $g : M'' \to N$ telle que $g \circ p = f$. Alors g est un morphisme de A-modules d'image $\mathsf{Im}\, f$, le noyau de f contient M', et le noyau de g est l'image par p de celui de f. En effet, soient $a, b \in M''$, $\lambda \in A$, et soient $x, y \in M$ tels que $p(x) = a$ et $p(y) = b$ (leur existence résulte de la surjectivité de p). Alors $g(a + \lambda b) = g(p(x) + \lambda p(y)) = g(p(x + \lambda y)) = f(x + \lambda y) = f(x) + \lambda f(y) = g(p(x)) + \lambda g(p(y)) = g(a) + \lambda g(b)$. Ainsi, g est A-linéaire. Il est clair que l'image de g est celle de f; si $x \in M'$, on a $f(x) = g(p(x)) = g(0) = 0$, donc $M' \subset \mathsf{Ker}\, f$; enfin pour $a = p(x)$, on a $g(a) = 0 \Longleftrightarrow f(x) = 0$ donc $\mathsf{Ker}\, g$ est l'image par p de $\mathsf{Ker}\, f$.
Pour achever la démonstration, il ne reste donc plus qu'a montrer que si $\mathsf{Ker}\, p \subset \mathsf{Ker}\, f$, il existe une application unique $g : M'' \longrightarrow N$ telle que $g = f \circ p$. L'unicité de g résulte de la surjectivité de p : si $a = p(x)$, on doit avoir $g(a) = f(x)$. D'autre part, la valeur de $f(x)$ ne dépend pas du choix de l'antécedent x de a; en effet, si x' était un autre antécédent, on aurait $x' - x \in \mathsf{Ker}\, p \subset \mathsf{Ker}\, f$, donc $f(x') = f(x)$. D'où l'existence de g. □

1.4.3. Proposition. (Propriété universelle du quotient)
Soit M un A-module, M' un sous-module de M, et $\pi : M \longrightarrow M/M'$ la surjection canonique. Soit N un autre A-module.
Se donner un morphisme de A-modules $g : M/M' \to N$ équivaut à se donner un morphisme de A-modules $f : M \to N$ tel que $M' \subset \mathsf{Ker}\, f$.
Plus précisément, étant donné un morphisme de A-modules $f : M \to N$ tel que $M' \subset \mathsf{Ker}\, f$, il existe un unique morphisme de A-modules $\widetilde{f} : M/M' \to N$ tel que $\widetilde{f} \circ \pi = f$. On dit que $\widetilde{f}$ s'obtient à partir de f par passage au quotient.
On a alors $\mathsf{Im}\, \widetilde{f} = \mathsf{Im}\, f$, et $\mathsf{Ker}\, \widetilde{f} = \pi(\mathsf{Ker}\, f)$.

Demonstration. Résulte immédiatement de la proposition précédente, appliquée à $M'' = A/I$ et $p = \pi$. □

1.4.4. Proposition. (Factorisation canonique d'un morphisme de modules)
Soit $f : M \longrightarrow N$ un morphisme de A-modules. Il existe un unique isomorphisme de A-modules $\widetilde{f} : M/\mathsf{Ker}\, f \longrightarrow \mathsf{Im}\, f$ rendant commutatif le diagramme suivant :

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, "\pi"'] & N \\
M/\mathsf{Ker}\, f \arrow[r, "\widetilde{f}"'] & \mathsf{Im}\, f \arrow[u, "\text{incl.}"']
\end{tikzcd}.$$

Demonstration.
Appliquons **1.4.3** au morphisme f et au sous-module $M' = \mathsf{Ker}\, f$ de M. Il existe un morphisme de A-modules unique $g : M/M' \longrightarrow N$ vérifiant : $\forall x \in M$, $g(\pi(x)) = f(x)$. En outre g a pour image $\mathsf{Im}\, f$, et pour noyau $\pi(\mathsf{Ker}\, f) = 0$. Soit $\widetilde{f} : M/\mathsf{Ker}\, f \longrightarrow \mathsf{Im}\, f$ l'application $a \mapsto g(a)$; c'est l'unique morphisme rendant commutatif le diagramme de l'énoncé, et c'est un isomorphisme d'après ce qui précède. □

1.5. Suites exactes

Soit A un anneau, M', M et M'' des A-modules, $f : M' \longrightarrow M$ et $g : M \longrightarrow M''$ deux applications A-linéaires.

1.5.1. Définition. On dit que

$$M'' \xrightarrow{f} M \xrightarrow{g} M''$$

est une *suite exacte de A-modules* si $\mathsf{Ker}\, g = \mathsf{Im}\, f$.

Plus généralement, donnons-nous un intervalle I de $\mathbb{Z}$, et pour chaque $i \in I$, soit M_i un A-module. Pour chaque $i \in I$ tel que $i + 1 \in I$, soit $f_i : M_i \longrightarrow M_{i+1}$ une application A-linéaire.

1.5.2. Définition. On dit que

$$\cdots \longrightarrow M_{j-1} \xrightarrow{f_{j-1}} M_j \xrightarrow{f_j} M_{j+1} \longrightarrow \cdots$$

est une *suite exacte de A-modules* si pour tout $i \in I$ tel que $i+1 \in I$ et $i-1 \in I$, on a $\mathsf{Ker}\, f_i = \mathsf{Im}\, f_{i-1}$.

1.5.3. EXEMPLES.

1) Soit $f : M_1 \longrightarrow M_2$ une application A-linéaire. Alors

$$M_1 \xrightarrow{f} M_2 \longrightarrow 0$$

est une suite exacte si et seulement si f est surjective;

$$0 \longrightarrow M_1 \xrightarrow{f} M_2$$

est une suite exacte si et seulement si f est injective; et

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \longrightarrow 0$$

est une suite exacte si et seulement si f est un isomorphisme.

2) Soient $f : M' \longrightarrow M$ et $g : M \longrightarrow M''$ deux applications A-linéaires. Alors

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

est une suite exacte si et seulement si f est injective, g est surjective, et $\mathsf{Ker}\, g = \mathsf{Im}\, f$. Les suites exactes de ce type sont appelées *suite exacte courte*, et jouent un rôle particulièrement important.

3) Soient M_1 et M_2 deux A-modules; soit $\iota_1 : M_1 \longrightarrow M_1 \oplus M_2$ l'inclusion canonique, et $p_2 : M_1 \oplus M_2 \longrightarrow M_2$ la surjection canonique. Alors

$$0 \longrightarrow M_1 \xrightarrow{\iota_1} M_1 \oplus M_2 \xrightarrow{s_2} M_2 \longrightarrow 0$$

est une suite exacte courte.

4) Pour toute application A-linéaire $f : M_1 \longrightarrow M_2$, on peut former deux suites exactes courtes :

$$0 \longrightarrow \mathsf{Ker}\, f \longrightarrow M_1 \longrightarrow \mathsf{Im}\, f \longrightarrow 0 \text{ et } 0 \longrightarrow M_1/\,\mathsf{Ker}\, f \longrightarrow M_2 \longrightarrow M_2/\,\mathsf{Im}\, f \longrightarrow 0\,.$$

2. Modules de type fini

2.1. Propriétés générales

Soit A un anneau. Rappelons qu'un A-module M est dit *de type fini* s'il est engendré par un nombre fini d'éléments.

2.1.1. Remarque. Soit M un A-module. Alors M est de type fini si et seulement s'il existe un entier n et une application A-linéaire surjective $\sigma : A^n \longrightarrow M$.
En effet, soient $x_1, \dots x_n$ des éléments de M, et soit σ l'unique application A-linéaire de A^n dans M qui envoie e_i (le i-ième élément de la base canonique) sur x_i. L'image de σ est le sous-module de M engendré par les x_i. Ainsi σ est surjective si et seulement si les éléments $x_1, \dots, x_n$ engendrent M.

2.1.2. Théorème. *Soit A un anneau.*
1) Soient M, M'' deux A-modules, et $f : M \longrightarrow M''$ une application A-linéaire surjective. Alors

$$M \text{ est de type fini } \Longrightarrow M'' \text{ est de type fini.}$$

2) Considérons une suite exacte de A-modules :

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0 .$$

Si M' et M'' sont de type fini, M est de type fini.
3) Soient M et M' deux A-modules, et $f : M' \longrightarrow M$ une application A-linéaire injective. Si A est noethérien, on a

$$M \text{ est de type fini } \Longrightarrow M' \text{ est de type fini.}$$

Demonstration.
1) Supposons M de type fini. Alors il existe un entier naturel n et une application A-linéaire surjective $\sigma : A^n \longrightarrow M$. L'application A-linéaire $f\circ\sigma : A^n \longrightarrow M''$ est surjective, donc M'' est de type fini.
2) L'application g est surjective, et on a $\operatorname{Ker} g = \operatorname{Im} f$. Supposons M' et M'' de type fini, et soient $\xi_1, \dots, \xi_n$ des générateurs de M'' et $y_1, \dots, y_m$ des générateurs de M'. Pour chaque $i = 1, \dots, n$, choisissons $x_i \in M$ tel que $g(x_i) = \xi_i$.
Soit $x \in M$. Alors $g(x)$ est combinaison linéaire des ξ_i, donc il existe des éléments $a_i \in A$ tels qu'on ait

$$g(x) = a_1\xi_1 + \dots + a_n\xi_n = g(a_1x_1 + \dots + a_nx_n) .$$

Soit $x' = x - a_1x_1 - \dots - a_nx_n$; on a donc $g(x) = 0$, d'où $x \in \operatorname{Ker} g = \operatorname{Im} f$; autrement dit, il existe des éléments $b_j \in A$ tels qu'on ait

$$x' = f(b_1y_1 + \dots + b_my_m) ;$$

Par conséquent

$$x = a_1x_1 + \dots + a_nx_n + b_1f(y_1) + \dots b_mf(y_m) ,$$

ce qui montre que M est engendré par les x_i $(1 \leq i \leq n)$ et les $f(y_j)$ $(1 \leq j \leq m)$.
3) Supposons A noethérien. Il s'agit de montrer que si M est un A-module de type fini, tout sous-module de M est de type fini.
On va le montrer par étapes. Tout d'abord, si $M = A$, c'est la définition même d'un anneau noethérien, puisque les sous-modules de A sont exactement les idéaux de A.
Traitons maintenant le cas $M = A^n$, en procédant par récurrence sur n. Pour $n = 0$ c'est évident, et pour $n = 1$ c'est déjà fait. Supposons $n > 1$, et considérons les deux applications A-linéaires suivantes.

$$f : A^{n-1} \longrightarrow A^n$$
$$(x_1, \ldots, x_{n-1}) \mapsto (x_1, \ldots, x_{n-1}, 0),$$

$$g : A^n \longrightarrow A$$
$$(x_1, \ldots, x_n) \mapsto x_n .$$

Il est clair que g est surjective, f injective, et $\mathsf{Ker}\, g = \mathsf{Im}\, f$; autrement dit on a une suite exacte
$$0 \longrightarrow A^{n-1} \xrightarrow{f} A^n \xrightarrow{g} A \longrightarrow 0 .$$
Soit N un sous-module de A^n, et soit $N'' = g(N)$; c'est un sous-module de A, donc un module de type fini (cas $M = A$). D'autre part, soit $N' = f^{-1}N$; c'est un sous-module de A^{n-1}, donc un module de type fini (cas $M = A^{n-1}$). Soit $f_0 : N' \longrightarrow N$ et $g_0 : N \longrightarrow N''$ les restrictions respectives de f et g. Alors g_0 est surjective par définition de N'', f_0 est injective car c'est le cas de f, et $\mathsf{Ker}\, g_0 = \mathsf{Ker}\, g \cap N = \mathsf{Im}\, f \cap N = f(N') = \mathsf{Im}\, f_0$ par définition de f_0 ; on a donc une suite exacte courte

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0 ,$$

et puisque N' et N'' sont de type fini, il en va de même de N en vertu de l'assertion 2).
Pour M quelconque, mais de type fini, il existe n et une application A-linéaire surjective σ de A^n sur M. Soit M' un sous-module de M. Alors $N = \sigma^{-1}(M')$ est un sous-module de A^n ; il est donc de type fini d'après ce qui précède. Or M' est l'image de N par σ; en vertu de l'assertion 1), M' est donc de type fini. □

2.2. Le théorème de Hilbert

2.2.1. Théorème. (Hilbert) *Soit A un anneau. Si A est noethérien, $A[X]$ est noethérien.*

Demonstration. Supposons A noethérien. Puisque $A[X]$ est une A-algèbre, on peut le voir comme un A-module. Pour tout entier naturel n, notons M_n l'ensemble des polynômes à coefficients dans A de degré $\leq n$. C'est le sous-module du A-module $A[X]$ engendré par $1, X, \ldots, X^n$; c'est donc un A-module de type fini. Notons f_n l'application A-linéaire de M_n dans A qui associe à $P = a_0 + a_1X + \cdots + a_nX^n$ le coefficient a_n.
Soit $\mathcal{I}$ un idéal de $A[X]$. Posons $\mathcal{I}_n = \mathcal{I} \cap M_n$. Puisque M_n est un A-module de type fini, $\mathcal{I}_n$ est un A-module de type fini par l'assertion 3) de **2.1.3.**

Posons d'autre part $\mathfrak{a}_n = f_n(\mathcal{I}_n)$.
Alors $\mathfrak{a}_n$ est un sous-module de A, donc un idéal de A. Par définition de $\mathfrak{a}_n$, on a pour $a \in A$:

$$a \in \mathfrak{a}_n \Longleftrightarrow \exists P \in \mathcal{I} \text{ de la forme } P = aX^n + \text{ termes de degré } < n\,.$$

La suite d'ideaux $\mathfrak{a}_n$ est croissante; en effet si $a \in \mathfrak{a}_n$, il existe $P \in \mathcal{I}$ de la forme aX^n+ termes de degré $< n$; alors $XP \in \mathcal{I}$ est de la forme $aX^{n+1}+$ termes de degré $< n+1$, donc $a \in \mathfrak{a}_{n+1}$.
Puisque A est noethérien, la suite $\mathfrak{a}_n$ est stationaire : il existe $N \in \mathbb{N}$ tel que $\forall n \geq N, \mathfrak{a}_n = \mathfrak{a}_N$. On se fixe un tel N.
Soient $Q_1, \cdots, Q_l$ des générateurs du A-module de type fini $\mathcal{I}_N$. Soit $\mathcal{I}_0$ l'idéal de $A[X]$ engendré par $Q_1, \ldots, Q_l$. Montrons que $\mathcal{I}_0 = \mathcal{I}$, ce qui achèvera la démonstration du théorème. On a $\mathcal{I}_0 \subset \mathcal{I}$. Il s'agit donc d'établir $P \in \mathcal{I} \Longrightarrow P \in \mathcal{I}_0$, ce que nous allons faire par récurrence sur $\deg P$.
Tout d'abord, il est clair que $\mathcal{I}_0$ contient $\mathcal{I}_N$, puisque $\mathcal{I}_N$ est l'ensemble des combinaisons linéaires des Q_i à coefficients dans A. Donc si $P \in \mathcal{I}$ et $\deg P \leq N$, on a $P \in \mathcal{I}_N \subset \mathcal{I}_0$.
Soit $P \in \mathcal{I}$ de degré $n > N$, et supposons que tout élément de $\mathcal{I}$ de degré $< n$ soit dans $\mathcal{I}_0$. Alors P s'écrit aX^n+ termes de degré $< n$; et $a \in \mathfrak{a}_n = \mathfrak{a}_N$. Ainsi il existe $P_0 \in \mathcal{I}_N$ tel que $P_0 = aX^N+$ termes de degré $< N$. Soit $Q = P - X^{n-N}P_0$; on a $\deg Q < n$, et $Q \in \mathcal{I}$, donc $Q \in \mathcal{I}_0$ par hypothèse de récurrence. Comme d'autre part $P_0 \in \mathcal{I}_N \subset \mathcal{I}_0$, on a $P = Q + X^{n-N}P_0 \in \mathcal{I}_0$, ce qui achève la démonstration. □

Remarque. On a vu en **I, 4.2.3** qu'il en résulte que si A est noethérien, $A[X_1, \ldots, X_n]$ est noethérien pour tout n.

2.3. Algèbres de type fini

Soit A un anneau, et B une A-algèbre, c'est-à-dire un anneau muni d'un morphisme d'anneaux $\eta : A \longrightarrow B$.

2.3.1. Définitions. Soit X une partie de B. On dit que X *engendre* B *comme* A*-algèbre* si le sous-anneau de B engendré par $\eta(A) \cup X$ est B lui-même. On dit que B est une A*-algèbre de type fini* si B est engendré comme A-algèbre par une partie finie.

2.3.2. Remarques.
1) Soient $x_1, \ldots x_n$ des éléments de B. Soit Φ le morphisme de A-algèbres

$$A[X_1, \ldots, X_n] \longrightarrow B$$

défini par $X_i \mapsto x_i$ pour $i = 1, \ldots, n$. L'image de Φ est le sous-anneau de B engendré par $\eta(A) \cup \{x_1, \ldots, x_n\}$.
Ainsi, B est engendré par $\{x_1, \ldots, x_n\}$ comme A-algèbre si et seulement si Φ est surjectif. Autrement dit, pour toute A-algèbre de type fini B, il existe un entier naturel n et un idéal I de $A[X_1, \ldots, X_n]$ tel que B soit isomorphe à $A[X_1, \ldots, X_n]/I$.
2) Il faut prendre garde au fait suivant. Si B est une A-algèbre, B est naturellement muni d'une structure de A-module. Si B est de type fini comme A-module, c'est une A-algèbre de type fini, *mais la réciproque est fausse.*
Par exemple, $\mathbb{Q}[X]$ est une $\mathbb{Q}$-algèbre de type fini, puisqu'elle est engendrée par X, mais c'est un $\mathbb{Q}$-espace vectoriel de dimension infinie (dénombrable).

2.3.3. Proposition. *Soit A un anneau noethérien. Si B est une A-algèbre de type fini, B est un anneau noethérien.*

DEMONSTRATION.
D'après **I 4.2.3,** $A[X_1, \ldots X_n]$ est noethérien. En vertu de la remarque **2.3.2** 1), on est ramené à la proposition suivante.

2.3.4. Proposition. *Si A est un anneau noethérien et I un idéal de A, A/I est noethérien.*

Cette proposition sera un cas particulier du lemme suivant.

2.3.5. Lemme. *Soit $f : A \longrightarrow B$ un morphisme d'anneaux. On fait l'hypothèse que l'application qui à un idéal J de B associe l'idéal $f^{-1}J$ de A est injective. Alors si A est noethérien, il en va de même de B.*

Le lemme est immédiat, et s'applique pour démontrer **2.3.4.** □ □

2.3.6. EXERCICE
1) Soit A un anneau et S une partie multiplicative de A. En utilisant le lemme 2.3.5, montrer que si A est noethérien, il en va de même de $S^{-1}A$.
2) Montrer que $\mathbb{Q}$ n'est pas une $\mathbb{Z}$-algèbre de type fini. [Ceci illustre le fait que $S^{-1}A$ n'est en général pas une A-algèbre de type fini.]

3. Modules libres et modules de torsion

3.1. Modules libres

Soit A un anneau et M un A-module. Soit I un ensemble, et $(x_i)_{i \in I}$ une famille d'éléments de M indexée par I. Soit ϕ l'unique application A-linéaire de $A^{(I)}$ vers M telle que $\phi(e_i) = x_i$ pour $i \in I$ (où e_i désigne le i-ième vecteur de la base canonique).

3.1.1. Définitions. On dit que la famille $(x_i)_{i \in I}$ est *libre* (*) (resp. *génératrice*, resp. *une base de M*) si l'application ϕ est injective (resp. surjective, resp. bijective).

3.1.2. REMARQUES.
1) La famille $(x_i)_{i \in I}$ est génératrice si et seulement si l'ensemble $\{x_i \mid i \in I\}$ est une partie génératrice de M. Ainsi, tout A-module M admet une famille génératrice : par exemple, la famille $(x)_{x \in M}$.
2) On sait que si K est un corps, tout K-espace vectoriel admet une base; mais si A est un anneau non nul qui n'est pas un corps, nous verrons qu'il existe des A-modules n'admettant pas de base.

3.1.3. Définition. Un A-module M est dit *libre* s'il admet une base; cela revient à dire qu'il existe un ensemble I tel que M soit isomorphe au A-module $A^{(I)}$.

(*) On dit aussi que les x_i sont *linéairement indépendants sur A.*

Exemples.
1) Pour tout ensemble I, $A^{(I)}$ est un module libre, admettant pour base la base canonique.
2) $A[X_1, \dots, X_n]$ est un A-module libre admettant pour base la famille des monômes unitaires.

3.1.4. Proposition-définition *Soit A un anneau non nul.*
Si L est un A-module libre, toutes les bases de L ont même cardinal. Le cardinal d'une base de L est appelé rang de L, *et noté* $\operatorname{rg} L$.

Pour démontrer la proposition, nous aurons besoins de quelques préliminaires.

3.1.5. Définition. Soit A un anneau, et M un A-module. On appelle *annulateur de M* l'ensemble

$$\operatorname{ann} M = \{a \in A \mid \forall x \in M, ax = 0\}.$$

3.1.6. Remarques.
1) Soit ρ le morphisme d'anneau de A dans l'anneau des endomorphismes du groupe $(M, +)$ définissant la structure de A-module sur M. C'est l'application qui à $a \in A$ associe l'endomorphisme $\rho(a) : M \longrightarrow M$, $x \mapsto ax$.
Alors $\operatorname{ann} M$ n'est autre que le noyau de ρ. C'est donc un idéal de A.
2) Soit I un idéal de A contenu dans $\operatorname{ann} M$. Le morphisme ρ définit par passage au quotient un morphisme d'anneaux de A/I dans l'anneau des endomorphismes du groupe $(M, +)$.
Autrement dit, M est naturellement muni d'une structure de A/I-module; c'est l'unique structure de A/I-module sur le groupe abélien $(M, +)$ telle que pour $a \in A$ et $x \in M$, on ait $\overline{a} \cdot x = ax$, où $\overline{a}$ désigne la classe de a modulo I.
3) Pour tout A-module M et tout idéal $I \subset A$, l'annulateur de M/IM contient I; la remarque 2) s'applique donc, et M/IM est donc naturellement muni d'une structure de A/I-module.

Demonstration de **3.1.4.**
Soit L un A-module libre; supposons que L admette une base indexée par l'ensemble I. On a donc un isomorphisme A-linéaire $L \xrightarrow{\sim} A^I$. Soit $\mathfrak{m}$ un idéal maximal de A, et K le corps $A/\mathfrak{m}$.
D'après les remarques **3.1.6,** $E = L/\mathfrak{m}L$ est un K-espace vectoriel. On va montrer que E a pour dimension le cardinal de I, ce qui aura pour conséquence que ce dernier est indépendant du choix de la base.
On a un isomorphisme K-linéaire $E \xrightarrow{\sim} A^{(I)}/\mathfrak{m}A^{(I)}$. D'autre part, l'application A-linéaire

$$\begin{aligned} A^{(I)} &\longrightarrow K^{(I)} \\ (a_i)_{i \in I} &\longmapsto (\overline{a_i})_{i \in I}, \end{aligned}$$

est surjective, de noyau $\mathfrak{m}A^{(I)}$. On en déduit, par passage au quotient, un isomorphisme

$$A^{(I)}/\mathfrak{m}A^{(I)} \xrightarrow{\sim} K^{(I)}$$

qui est K-linéaire, donc la dimension de E est bien $\# I$. $\square$

3.2. Torsion

Soit A un anneau intègre.

3.2.1. Définitions. Soit M un A-module, et x un élément de M. On dit que x est un *élément de torsion de* M s'il existe un élément non nul a de A, tel qu'on ait $ax = 0$.
On dit que M est un *module de torsion* si tout élément de M est de torsion. On dit que M est *sans torsion* si le seul élément de torsion de M est 0.

REMARQUES.
1) Un module libre est toujours sans torsion.
2) Si $\mathsf{ann}\, M \neq 0$, M est un module de torsion.
Inversement, si M est un module de torsion de type fini, $\mathsf{ann}\, M \neq 0$. En effet, soient $x_1, \ldots, x_n$ des générateurs de M. Alors il existe $a \in A$ non nul tel que $ax_i = 0$ pour tout i, et un tel a est dans l'annulateur de M.
3) Si I est un idéal de A, l'annulateur de A/I est I. En particulier si $I \neq 0$, A/I est un module de torsion.
Si A n'est pas un corps, il existe donc un module de torsion non nul; un tel module n'est pas libre.

EXERCICE Montrer que $\mathbb{Q}/\mathbb{Z}$ est un $\mathbb{Z}$-module de torsion dont l'annulateur est $\{0\}$.

3.2.2. Proposition. *Soit M un A-module. L'ensemble des éléments de torsion de M est un sous-module de M, noté M_{tors}.*

DEMONSTRATION. Soient x, $y \in M$ deux éléments de torsion. Il existe a, $b \in A$, non nuls, tels que $ax = by = 0$. Alors ab est non nul, car A est intègre; et $ab(x+y) = bax + aby = 0$; d'autre part pour tout $\lambda \in A$, $a\lambda x = \lambda a x = 0$, donc $x + y$ et λx sont des éléments de torsion. □

REMARQUE. Pour tout A-module M, on a donc une suite exacte courte de A-modules :

$$0 \longrightarrow M_{\mathsf{tors}} \longrightarrow M \xrightarrow{\pi} M/M_{\mathsf{tors}} \longrightarrow 0\,;$$

de plus, le module M/M_{tors} est sans torsion.
En effet, soit ξ un élément de torsion de M/M_{tors}, et $x \in M$ tel que $\xi = \pi(x)$. Soit $a \in A$ non nul tel que $a\xi = 0$, donc $ax \in M_{\mathsf{tors}}$; il existe $b \in A$ non nul tel que $b \cdot ax = 0$, d'où $x \in M_{\mathsf{tors}}$, et $\xi = 0$.

3.2.3. Théorème. *Soit A un anneau intègre, L un A-module libre de rang fini n, et L' un sous-module libre de L.*
1) On a $\mathsf{rg}\, L' \leq n$.
2) Il existe un sous-module libre L'' de L vérifiant $L' \cap L'' = 0$ et $\mathsf{rg}\, L' + \mathsf{rg}\, L'' = n$.
3) On a $\mathsf{rg}\, L' = n$ si et seulement si L/L' est un A-module de torsion.

Pour démontrer ce théorème, nous aurons besoin de la notion de modules de fractions.

3.3. Modules de fractions

Soit A un anneau, et $S \subset A$ une partie multiplicative de A. Nous avons construit en **I, 2.5** une A-algèbre $S^{-1}A$. Tout $S^{-1}A$-module est naturellement muni d'une structure de A-module : c'est ce que nous avons vu en **1.3.**, exemple **1)** (changement d'anneau).
Etant donné un A-module M, on se propose de construire un $S^{-1}A$-module, noté $S^{-1}M$, de la manière suivante.
On munit l'ensemble $S \times M$ de la relation $\mathcal{R}$ définie par

$$(s,x)\,\mathcal{R}\,(s',x') \Longleftrightarrow \exists \sigma \in S \text{ tel que } \sigma s' x = \sigma s x' .$$

On vérifie que $\mathcal{R}$ est une relation d'équivalence; on note $S^{-1}M$ le quotient de $S \times M$ par la relation $\mathcal{R}$, et x/s la classe d'un élément (s,x) de $S \times M$. On observe que si (s,x) et (s',x') sont deux éléments de $S \times M$, la classe $(s'x + sx')/(ss')$ ne dépend que des classes x/s et x'/s'. Ainsi, on définit une loi de composition interne $+$ sur $S^{-1}M$. De plus si (σ, a) est un élément de $S \times A$ et (s,x) un élément de $S \times M$, la classe $ax/\sigma s$ ne dépend que des classes a/σ et x/s, ce qui définit une loi de composition externe $\cdot : S^{-1}A \times S^{-1}M \longrightarrow S^{-1}M$.
On vérifie aisément que les lois $+$ et $\cdot$ ainsi définies font de $S^{-1}M$ un $S^{-1}A$-module.
En outre, l'application

$$\begin{aligned} \eta_M : M &\longrightarrow S^{-1}M \\ x &\mapsto x/1 \end{aligned}$$

est A-linéaire.

3.3.1. Définition. Le $S^{-1}A$-module $S^{-1}M$ est appelé *module des fractions de M à dénominateur dans S.*

3.3.2. Proposition. (Propriété universelle des modules de fractions)
Soit M un A-module, et N un $S^{-1}A$-module. Pour toute application A-linéaire $f : M \longrightarrow N$, il existe une unique application $S^{-1}A$-linéaire $\widetilde{f} : S^{-1}M \longrightarrow N$ telle qu'on ait $f = \widetilde{f} \circ \eta_M$.

Demonstration.
Soit $\widetilde{f}$ une telle application. Pour $x/s \in S^{-1}M$, on a $\widetilde{f}(x/s) = \widetilde{f}(1/s \cdot x/1) = 1/s \cdot \widetilde{f} \circ \eta_M(x) = 1/s \cdot f(x)$, d'où l'unicité d'un tel $\widetilde{f}$. On vérifie aisément que l'application $\widetilde{f} : S^{-1}M \longrightarrow N$, $x/s \mapsto 1/s \cdot f(x)$ est bien définie et convient. $\square$

3.3.3. Remarques.
1) Soient M' et M deux A-modules, et $f : M' \longrightarrow M$ une application A-linéaire. Appliquant **3.3.2** à l'application A-linéaire $\eta_M \circ f : M' \longrightarrow S^{-1}M$, on voit qu'il existe une unique application $S^{-1}A$-linéaire de $S^{-1}M'$ vers $S^{-1}M$, notée $S^{-1}f$ qui rende commutatif le diagramme :

$$\begin{tikzcd} M' \arrow[r, "f"] \arrow[d, "\eta_{M'}"'] & M \arrow[d, "\eta_M"] \\ S^{-1}M' \arrow[r, "S^{-1}f"'] & S^{-1}M \end{tikzcd}$$

2) Si $f : M' \longrightarrow M$ et $g : M \longrightarrow M''$ sont deux applications A-linéaires, on a $S^{-1}g \circ S^{-1}f \circ \eta_{M'} = \eta_{M''} \circ g \circ f$, donc

$$S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f)\,.$$

De même pour tout A-module M, l'application $S^{-1}\,1_M$ n'est autre que $1_{S^{-1}M}$.

3.3.4. Proposition. *Soit A un anneau, et $S \subset A$ une partie multiplicative.*
1) Soit $(M_i)_{i\in I}$ une famille de A-modules. On a un isomorphisme de $S^{-1}A$-modules

$$\bigoplus_{i\in I} S^{-1}M_i \xrightarrow{\sim} S^{-1}(\bigoplus_{i\in I} M_i)\,.$$

2) Soit

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

une suite exacte de A-modules. Alors

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

est une suite exacte de $S^{-1}A$-modules.

Demonstration.
1) Pour tout $j \in I$, l'inclusion

$$a_j : M_j \longrightarrow \bigoplus_{i\in I} M_i$$

induit une application $S^{-1}A$-linéaire

$$S^{-1}a_j : S^{-1}M_i \longrightarrow S^{-1}(\bigoplus_{i\in I} M_i)$$

en vertu de la remarque **3.3.3.** 1), d'où par la propriété universelle de la somme directe, une application $S^{-1}A$-linéaire

$$\Phi : \bigoplus_{i\in I} S^{-1}M_i \longrightarrow S^{-1}(\bigoplus_{i\in I} M_i)\,.$$

D'autre part, l'application A-linéaire

$$\bigoplus_{i\in I} M_i \longrightarrow \bigoplus_{i\in I} S^{-1}M_i$$
$$(a_i)_{i\in I} \mapsto (\eta_{M_i}(a_i))_{i\in I}$$

induit par **3.3.2.** une application $S^{-1}A$-linéaire

$$\Psi : S^{-1}(\bigoplus_{i\in I} M_i) \longrightarrow \bigoplus_{i\in I} S^{-1}M_i\,;$$

on constate que Φ et Ψ sont inverses l'une de l'autre.
2) Considérons le diagramme commutatif

$$\begin{tikzcd}
M' \arrow[r, "f"] \arrow[d, "\eta_{M'}"'] & M \arrow[r, "g"] \arrow[d, "\eta_M"'] & M'' \arrow[d, "\eta_{M''}"'] \\
S^{-1}M' \arrow[r, "S^{-1}f"'] & S^{-1}M \arrow[r, "S^{-1}g"'] & S^{-1}M''
\end{tikzcd}$$

On a par hypothèse $\mathsf{Ker}\, g = \mathsf{Im}\, f$. En particuler, $g \circ f = 0$, donc $S^{-1}g \circ S^{-1}f = 0$ en vertu de la remarque **3.3.3.** 2). Montrons $\mathsf{Im}(S^{-1}f) \subset \mathsf{Ker}(S^{-1}g)$. Soit $x/s \in S^{-1}M$ tel que $(S^{-1}g)(x/s) = 0$. On a donc $1/s \cdot (g(x)/1) = 0$, donc $g(x)/1 = 0$. Autrement dit, il existe $\sigma \in S$ tel que $\sigma g(x) = 0$. Ainsi, $\sigma x \in \mathsf{Ker}\, g = \mathsf{Im}\, f$. Il existe donc $x' \in M'$ tel que $f(x') = \sigma x$. On a alors $(S^{-1}f)(x'/s\sigma) = 1/s\, 1/\sigma\, f(x')/1 = 1/s\, 1/\sigma\, \sigma x/1 = x/s$, d'où la seconde assertion de la propostion. □

3.3.5. Corollaire. *Si L est un A-module libre, $S^{-1}L$ est un $S^{-1}A$-module libre de même rang.* □

DEMONSTRATION DE **3.2.3.**
Puisque A est un anneau intègre, $S = A - \{0\}$ en est une partie multiplicative. Posons $F = \mathsf{Frac}\, A = S^{-1}A$.
A tout A-module M, on peut associer le F-espace vectoriel $S^{-1}M$, qu'on notera M_0.

3.3.6. Lemme. *On a l'équivalence : M est un A-module de torsion $\iff M_0 = 0$.*

DEMONSTRATION.
Pour $x \in M$, $\eta_M(x) = x/1$ est nul si et seulement s'il existe $a \in A - \{0\}$ tel que $ax = 0$. Autrement dit, le noyau de η_M est l'ensemble des éléments de torsion de M.
En particulier, si $M_0 = 0$, le module M est de torsion. Inversement si M est de torsion, $\eta_M = 0$. Tout élément de M_0 est de la forme $x/s = 1/s\, \eta_M(x)$, donc nul. □

Soit $L' \subset L$ un sous-module libre, et soit $Q = L/L'$. On a la suite exacte courte de A-modules
$$0 \longrightarrow L' \xrightarrow{f} L \xrightarrow{g} Q \longrightarrow 0,$$
d'où, d'après la seconde assertion de **4.3.4**, une suite exacte courte de F-espaces vectoriels
$$0 \longrightarrow L'_0 \xrightarrow{f_0} L_0 \xrightarrow{g_0} Q_0 \longrightarrow 0.$$

Or L_0 est un F-espace vectoriel de dimension n (**3.3.5.**).
Puisque $f_0 : L'_0 \longrightarrow L_0$ est F-linéaire injective, L'_0 est de dimension $\leq n$; autrement dit $\mathsf{rg}\, L' \leq n$ (**3.3.5.**), d'où l'assertion 1). On a $\mathsf{rg}\, L' = n \iff L'_0$ et L_0 ont même dimension (finie) $n \iff f_0$ est surjective $\iff g_0$ est nulle $\iff Q_0 = 0 \iff Q$ est un module de torsion (en vertu du lemme **3.3.6**), d'où l'assertion 3).
Reste à démontrer l'assertion 2) du théorème. Cela se ramène au lemme suivant.

3.3.7. Lemme. *Si L est un A-module libre de rang n, toute famille libre de L peut être complétée en une famille libre à n éléments.*

DEMONSTRATION. Puisque L est sans torsion, l'application $\eta_L : L \longrightarrow L_0$ est injective; on peut donc identifier tout élément x de L à son image par η_L.
Soit $(e_1, \ldots, e_m)$ une famille d'éléments de L. Cette famille est libre sur A si et seulement si, en tant que famille d'éléments de L_0, elle est libre sur F.
En effet, toute relation de liaison entre les e_i à coefficients dans A peut être vue comme une relation de liaison à coefficients dans F. Inversement, supposons donnée une relation de liaison $a_1/s_1\, e_1 + \cdots + a_m/s_m\, e_m$, avec $a_i \in A$ et $s_i \in S$. Multipliant cette relation par $s_1 \ldots s_m$, il vient une relation de liaison entre les e_i, à coefficients dans A.
Supposons la famille $(e_1, \ldots, e_m)$ libre sur A. C'est donc une famille libre du F-espace vectoriel L_0, qui est de dimension n. On peut donc la compléter en une base $(e_1, \ldots, e_m, g_1, \ldots, g_{n-m})$ de L_0. Chacun des g_i est de la forme f_i/s_i, avec $f_i \in L$ et $s_i \in S$. La famille $(e_1, \ldots, e_m, f_1, \ldots, f_{n-m})$ est encore une base du F-espace vectoriel L_0, donc une famille libre du A-module L. $\square$

Le lemme permet de conclure comme suit. Soit $(e_1, \ldots, e_m)$ une base de L'; on la complète en une famille libre $(e_1, \ldots, e_m, f_1, \ldots, f_{n-m})$ de L; il suffit alors de prendre pour L'' le sous-module de L engendré par $(f_1, \ldots, f_{n-m})$.
D'où le théorème **3.2.3.** $\square$

3.4. Suites exactes courtes scindables

3.4.1. Proposition. *Considérons une suite exacte courte de A-modules*

$$(\mathcal{E}) \qquad 0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0 .$$

Les conditions suivantes sont équivalentes :
1) Il existe une application A-linéaire $\tau : M'' \longrightarrow M$ telle que $g\tau = 1_{M''}$.
2) Il existe une application A-linéaire $\sigma : M \longrightarrow M'$ telle que $\sigma f = 1_{M'}$.
3) Il existe un couple (σ, τ) d'applications A-linéaires,

$$\sigma : M \longrightarrow M', \quad \tau : M'' \longrightarrow M ,$$

vérifiant :

$$\sigma f = 1_{M'}, \quad g\tau = 1_{M''}, \ \text{et} \ f\sigma + \tau g = 1_M .$$

De plus, si (σ, τ) est un couple vérifiant 3), l'application

$$\begin{aligned} \Psi : M &\longrightarrow M' \oplus M'' \\ x &\mapsto \sigma(x) + g(x) \end{aligned}$$

est un isomorphisme de A-modules.

DEMONSTRATION.
Il est clair que 3) $\Longrightarrow$ 1) et 2). Montrons 1) $\Longrightarrow$ 3).
On va montrer un peu plus : étant donné τ vérifiant 1), il existe σ unique tel que (σ, τ) vérifie 3).
En effet, on doit avoir $f\sigma = 1_M - \tau g$. Puisque f est injective, cette condition détermine σ de façon unique. D'autre part, on a $g(1_M - \tau g) = g - g\tau g = g - g = 0$, donc l'image de $1_M - \tau g$ est contenue dans $\mathsf{Ker}\, g = \mathsf{Im}\, f$. Il existe donc $\sigma : M \longrightarrow M'$ A-linéaire tel que $f\sigma = 1_M - \tau g$.
Reste à vérifier qu'on a $\sigma f = 1'_M$. Puisque f est injective, il suffit de montrer $f\sigma f = f$. Or $f\sigma f = (1_M - \tau g)f = f - \tau g f = f$ puisque $gf = 0$.
De même, on montre 2) $\Longrightarrow$ 3); plus précisément, on montre que si σ vérifie 2), il existe τ unique tel que (σ, τ) vérifie 3).
Montrons que si (σ, τ) vérifie 4), Φ est un isomorphisme. Soit

$$\begin{aligned} \Psi : M' \oplus M'' &\longrightarrow M \\ x' + x'' &\mapsto f(x') + \tau(x'') . \end{aligned}$$

Montrons que Φ et Ψ sont inverses l'une de l'autre.
On a $\Psi \circ \Phi(x) = f\sigma(x) + \tau g(x) = x$, donc $\Psi \circ \Phi = 1_M$. Pour conclure, il suffit donc de montrer que Ψ est injective.
Supposons $\Psi(x' + x'') = 0$, avec $x' \in M'$ et $x'' \in M''$. Alors $f(x') + \tau(x'') = 0$, donc $g(f(x') + \tau(x')) = 0 = g\tau(x') = x'$. Donc $x' = 0$, et $\tau(x'') = 0$, donc $g\tau(x'') = 0 = x''$; d'où $x'' = 0$, et Ψ est injective. $\square$

3.4.2. Définitions. Un couple (σ, τ) vérifiant la conditon 3) est un *scindage* de la suite exacte $(\mathcal{E})$.
La suite exacte $(\mathcal{E})$ est dite *scindable* si elle admet un scindage. On a alors $M \simeq M' \oplus M''$.

EXEMPLES.
1) Si M_1 et M_2 sont deux A-modules, la suite exacte

$$0 \longrightarrow M_1 \longrightarrow M_1 \oplus M_2 \longrightarrow M_2 \longrightarrow 0$$

de l'exemple **1.5.3** 3) est scindable.
En fait, toute suite exacte courte scindable est essentiellement de ce type. Plus précisément, si

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{s} M'' \longrightarrow 0$$

est une suite exacte courte scindable, $i(M')$ admet un supplémentaire N dans M, et $s_{|N}$ est un isomorphisme de N sur M''.
2) La suite exacte de $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2\times} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

n'est pas scindable, car la seule application $\mathbb{Z}$-linéaire $\mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}$ est 0.

3.4.3. Proposition. *Considérons une suite exacte de A-modules*

$$(\mathcal{E}) \qquad 0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0\,.$$

Si M'' est un module libre, $(\mathcal{E})$ est scindable.

Demonstration.
Soit $(e_i)_{i\in I}$ une base de M'', et pour tout i, choisissons $x_i \in M$ tel que $g(x_i) = e_i$. Soit $\tau : M'' \longrightarrow M$ l'unique application A-linéaire vérifiant $\tau(e_i) = x_i$ pour tout i. Alors $g\tau(e_i) = e_i$, donc $g\tau = 1_{M''}$, ce qui montre que la suite exacte est scindable. □

4. Classification des modules de type fini sur un anneau principal

Soit A un anneau principal. On se propose dans cette section de décrire complètement la structure des modules de type fini sur A.

4.1. Où l'on rend aux modules libres ce qui est aux modules libres...

4.1.1. Théorème. *Soit A un anneau principal, et L un A-module libre de rang fini. Alors tout sous-module de L est libre.*

Remarque. Soit A un anneau intègre. Tout sous-module libre de A est de rang ≤ 1, donc engendré par un élément. Si A n'est pas principal, le A-module libre A admet donc un sous-module qui n'est pas libre.

Demonstration. On procède par récurrence sur $n = \operatorname{rg} L$. On peut donc supposer $L = A^n$. Pour $n = 1$, $L = A$; un sous-module de A est un idéal, donc de la forme (f) avec $f \in A$.
Si $f = 0$, $(f) = 0$ est libre de rang 0. Sinon, f est une base de (f), qui est donc libre de rang 1.
Supposons $n > 1$, et montrons comment l'on passe de $n-1$ à n. Considérons la suite exacte

$$0 \longrightarrow A^{n-1} \xrightarrow{f} A^n \xrightarrow{g} A \longrightarrow 0$$

déjà rencontrée au cours de la démonstration du théorème **2.1.3.**
Soit M un sous-module de A^n. Posons $M' = f^{-1}(M)$ et $M'' = g(M)$. On a vu qu'on a alors une suite exacte courte :

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0\,;$$

le module M' est un sous-module de A^{n-1}; il est donc libre par hypothèse de récurrence. De même M'' est un sous-module de A, donc il est libre (cas $n = 1$).
La suite exacte $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ est donc scindable en vertu de **3.4.3,** d'où un isomorphisme $M \xrightarrow{\sim} M' \oplus M''$. Puisque M' et M'' sont libres, il en va de même de M. □

4.1.2. Théorème. *Soit A un anneau principal. Tout A-module de type fini sans torsion est libre.*

DEMONSTRATION. Soit M un A-module de type fini sans torsion, et Γ une partie génératrice finie de M. Soit Λ une partie libre maximale de Γ, et L le sous-module libre de M engendré par Λ. Pour tout $x \in \Gamma \backslash \Lambda$, $\Lambda \cup \{x\}$ n'est pas libre, donc il existe $a_x \in A$ non nul tel que $a_x \cdot x \in L$. Soit a le produit des a_x pour x décrivant $\Gamma \backslash \Lambda$. Alors $a \neq 0$ et pour tout $x \in M$, $ax \in L$.
L'application A-linéaire

$$\begin{aligned} M &\longrightarrow L \\ x &\longrightarrow ax \end{aligned}$$

est injective, car M est sans torsion, donc M est isomorphe à un sous-module de L, qui est libre de rang fini. En vertu de **4.1.1,** M est donc libre. $\square$

REMARQUE. Ceci n'est plus vrai si on ne suppose pas M de type fini. Par exemple, $\mathbb{Q}$ est un $\mathbb{Z}$-module sans torsion, mais il n'est pas libre. En effet, deux rationnels ne sont jamais linéairement indépendants sur $\mathbb{Z}$.

4.1.3. Théorème. *Soit M un A-module de type fini.*
1) Il existe un sous-module libre $L \subset M$ et un sous-module de torsion $T \subset M$ tel qu'on ait $M = T \oplus L$.
2) De plus, pour toute décomposition de ce type, on a $T = M_{\mathsf{tors}}$, et L est isomorphe à M/M_{tors}.

DEMONSTRATION.
1) Le module M/M_{tors} est de type fini, sans torsion, donc libre d'après **4.1.2.** La suite exacte

$$0 \longrightarrow M_{\mathsf{tors}} \longrightarrow M \xrightarrow{\pi} M/M_{\mathsf{tors}} \longrightarrow 0$$

est donc scindable. Autrement dit, M_{tors} admet un supplémentaire L dans M ; c'est un A-module isomorphe à M/M_{tors}.
2) Supposons $M = T \oplus L$ avec L libre et T de torsion. Alors on a clairement $T = M_{\mathsf{tors}}$; et $\pi_{|L} : L \longrightarrow M/M_{\mathsf{tors}}$ est un isomorphisme. $\square$

Ainsi, l'étude des A-modules de type fini se ramène à celle des A-modules de torsion de type fini.

4.2. ...et à la torsion ce qui est à la torsion

4.2.1. Définition. Soit p un élément irréductible de A, M un A-module, et $x \in M$. On dit que x est *p-primaire* s'il existe $n \in \mathbb{N}$ tel que $p^n x = 0$.

4.2.2. Proposition-définition. *Soit M un A-module, et p un élément irréductible de A. Les éléments p-primaires de M constituent un sous-module de M qu'on note $M(p)$, et qu'on appelle* composante p-primaire de M.

DEMONSTRATION. Pour $n \in \mathbb{N}$, soit $N_n = \{x \in M \mid p^n x = 0\}$. Les N_n constituent une suite croissante de sous-modules de M, et $M(p) = \bigcup_{n\in\mathbb{N}} N_n$ est donc un sous-module de M. □

4.2.3. Théorème. *Soit M un A-module de torsion de type fini.*
1) Il existe des éléments irréductibles de A deux à deux non associés $p_1, \dots, p_l$ tels qu'on ait pour tout irréductible p de A :

$$M(p) \neq 0 \Longleftrightarrow p \sim p_i \text{ pour un certain } i\,.$$

2) On a

$$M = \bigoplus_{1\leq i\leq l} M(p_i)\,.$$

DEMONSTRATION.
Elle repose sur le lemme suivant.

4.2.4. Lemme. *Soit M un A-module. Pour $f \in A$ posons $E_f = \{x \in M \mid fx = 0\}$.*
(i) Soient f, $g \in A$ et $h = f \vee g$. Alors $E_h = E_f + E_g$.
(ii) Si f et g sont premiers entre eux, $E_f \cap E_g = 0$.

DEMONSTRATION. Pour $f \in A$, E_f est un sous-module de M.
(i) $(h) = (f) \subset (g)$, donc E_f, $E_g \subset E_h$. D'autre part, on a $h = af = bg$, avec a et b premiers entre eux. Il existe u, $v \in A$ tels que $ua + vb = 1$ car A est principal. Soit $x \in E_h$. Alors $x = uax + vbx$. Or, $fuax = uhx = 0$, donc $uax \in E_f$; et de même, $vbx \in E_g$. D'où $x \in E_f + E_g$.
(ii) Si f et g sont premiers entre eux, $E_f \cap E_g = 0$. En effet, il existe u, $v \in A$ tels que $uf + vg = 1$. Soit $x \in E_f \subset E_g$. Alors $x = ufx + vgx = 0$. □

Puisque M est un module de torsion de type fini, $\mathsf{ann}(M) \neq 0$. Soit a un générateur de $\mathsf{ann}(M)$. Considérons la décomposition de a en produit de facteurs irréductibles : $a \sim p_1^{\nu_1} \cdots p_l^{\nu_l}$, avec $\nu_i > 0$.
Posons $q_i = p_i^{\nu_i}$. On a $M = E_a$. Appliquant de façon itérée le lemme, il vient : $M = E_a = E_{q_1} \oplus \cdots \oplus E_{q_l}$.
Soit p un irréductible de A. Si p est premier à a, $E_{p^n} = E_{p^n} \cap E_a = 0$ d'après l'assertion (ii) du lemme; donc $M(p) = 0$.
Supposons $p \sim p_i$, et montrons qu'alors $M(p) = E_{q_i}$. Puisque E_{q_i} est p-primaire, il suffit de montrer que $M(p) \subset E_{q_i}$. Posons $q'' = \prod_{j\neq i} q_j$, $M' = E_{q_i}$, $M'' = E_{q''} = \bigoplus_{j\neq i} E_{q_j}$
Soit $x \in M(p)$. Alors s'écrit $x = x' + x''$, avec $x' \in M'$ et $x'' \in M''$. Il existe n tel que $p^n x = 0$. Ceci implique $p^n x'' = 0$, donc $x'' = 0$ car p est premier à $q'' \in \mathsf{ann}\, M''$. Ainsi $M(p) = E_{q_i}$.
De plus, $M(p) = E_{q_i}$ est non nul, car $q'' \in \mathsf{ann}\, M''$ et $q'' \notin \mathsf{ann}\, M$. Ceci achève la démonstration du théorème. □

Ainsi, l'étude des A-modules de torsion de type fini se ramène à celle des modules p-primaires de type fini.

Exercice. Montrer que si M est un A-module de torsion (non nécessairement de type fini), M est somme directe de ses composantes p-primaires pour p décrivant un système de représentants des irréductibles de A.

4.3. Structure des modules p-primaires de type fini.

4.3.1. Théorème. *Soit p un élément irréductible de A, et M un A-module p-primaire de type fini.*
1) Il existe un isomorphisme

$$M \xrightarrow{\sim} \bigoplus_{1 \leq i \leq m} A/(p^{r_i}),$$

où $r_1, \ldots, r_m$ est une suite d'entiers vérifiant $r_1 \geq r_2 \geq \cdots \geq r_m \geq 1$.
2) De plus la suite $r_1, \ldots, r_m$ est déterminée de façon unique par ces conditions.

Demonstration.
Dans le cours de la démonstration, la notion suivante nous sera utile.

Définition. Soit M un A-module, et $x \in M$. On appelle *période de x* tout générateur de l'idéal $\{a \in A \mid ax = 0\}$.

Remarque. Si x est p-primaire, il existe $r \in \mathbb{N}$ tel que p^r soit une période de x. En outre, pour tout $l \in \mathbb{N}$, $y = p^l x$ admet pour période p^{r-l} si $l \leq r$, et $y = 0$ si $l \geq r$.

1) Observons qu'un module p-primaire cyclique est un module isomorphe à $A/(p^r)$ pour un certain $r \in \mathbb{N}$. Il s'agit donc de démontrer :
si M est un A-module p-primaire engendré par n éléments, M est somme directe finie de A-modules p-primaires cycliques, ce qu'on va faire par récurrence sur n. Si $n = 1$ c'est immédiat.
Supposons M engendré par une partie finie X de cardinal $n + 1$, avec $n \geq 1$. On a $\mathsf{ann}(M) = (p^r)$ pour un certain $r \in \mathbb{N}$. Chacun des éléments de X est annulé par p^r, et il y en a au moins un ayant pour période p^r. Notons $x, x_1, \ldots, x_n$ les éléments de X, x ayant pour période (p^r). Chacun des x_i est annulé par p^r.
Soit M' le sous-module de M engendré par x, $M'' = M/M'$ et $\pi : M \longrightarrow M''$ la surjection canonique. Si $z \in M$, on note $\overline{z}$ son image par π.
Le module M'' est engendré par les n éléments $\overline{x}_1, \ldots, \overline{x}_n$. Il est annulé par p^r, donc p-primaire. Par hypothèse de récurrence, il est somme directe finie de A-modules p-primaires cycliques.
Soient $\xi_1, \ldots, \xi_m \in M''$ tels que M'' soit la somme directe de ses sous-modules cycliques $A\xi_i$. Soit p^{r_i} une période de ξ_i; on a $r \geq r_i$. Ainsi, M'' s'identifie au quotient de A^n par le sous-module $(p^{r_1}) \oplus \cdots \oplus (p^{r_n})$.
On se propose de montrer que la suite exacte courte

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0\,;$$

est scindable. Cela résultera du lemme suivant.

4.3.2. Lemme. *Pour tout $i = 1, \ldots, m$, la classe ξ_i admet un représentant z_i de période p^{r_i}.*

Montrons comment le lemme permet de conclure. Soit ϕ l'application A-linéaire $A^n \longrightarrow M$ qui envoie le i-ième vecteur de la base canonique sur z_i; le noyau de ϕ contient $(p^{r_1}) \oplus \cdots \oplus (p^{r_n})$. Par passage au quotient, on en déduit une application A-linéaire $\tau : M'' \longrightarrow M$ qui envoie ξ_i sur z_i. On a $\pi \circ \tau(\xi_i) = \xi_i$, donc $\pi \circ \tau = 1\, M''$ puisque les ξ_i engendrent M''. Autrement dit la suite exacte courte

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

est scindable; d'où un isomorphisme $M \simeq M' \oplus M''$, et M est bien somme directe finie de modules cycliques p-primaires.
D'où l'assertion 1).

DEMONSTRATION DE **4.3.2.**
Soit y_i un représentant quelconque de ξ_i, de période p^s. On a $s \geq r_i$, car $\xi_i^s = \pi({y_i}^s) = 0$. Si $s = r_i$, $z_i = y_i$ convient. Supposons donc $s > r_i$.
L'élément $p^{r_i} y_i$ est dans le noyau de π, car $p^{r_i}\xi_i = 0$. Par conséquent, $p^{r_i} y_i = fx$, avec $f \in A - \{0\}$. L'élément f s'écrit $f = cp^t$, avec $c \in A - (p)$ et $t \in \mathbb{N}$.
Or $p^{r_i} y_i$ a pour période p^{s-r_i}, et fx a pour période p^{r-t}. On a donc $s = r_i + r - t$. D'autre part, $s \leq r$, donc $t \geq r_i$. Posons $z_i = y_i - cp^{t-r_i}x$. Alors $\pi(z_i) = \xi_i$, et $p^{r_i} z_i = fx - cp^t x = 0$, donc z_i convient. D'où le lemme. □

2) résultera immédiatement de l'assertion 2) du théorème suivant. □

4.4. Facteurs invariants d'un module de torsion

4.4.1. Théorème.
Soit M un A-module de torsion de type fini.
1) Il existe un isomorphisme

$$M \xrightarrow{\sim} \bigoplus_{1 \leq i \leq n} A/(a_i)$$

où $a_1, \ldots, a_n$ sont des éléments non nuls de A vérifiant $(a_1) \subset (a_2) \subset \cdots \subset (a_n)$.
2) La suite $(a_1), (a_2), \ldots, (a_n)$ est déterminée de façon unique par ces conditions.

4.4.2. Définition. Les éléments $a_1, \ldots, a_n$ sont appelés *facteurs invariants* de M.

DEMONSTRATION.
1) Le module M admet une décomposition

$$M \simeq M(p_1) \oplus M(p_2) \oplus \cdots \oplus M(p_l)\,.$$

Pour tout $j = 1, \ldots, l$, $M(p_j)$ admet une décomposition de la forme

$$M(p_j) \simeq \bigoplus_{1 \leq i < +\infty} A/(p_j^{r_{j,i}})\,,$$

où $(r_{j,i})_{1 \leq i < \infty}$ est une suite d'entiers naturels décroissante, et $r_{j,i} = 0$ pour i assez grand.

Posons $a_i = p_1^{r_{1,i}} \cdots p_l^{r_{l,i}}$ pour $1 \leq i < \infty$.
Par le lemme chinois, on a :

$$A/(a_i) \simeq \bigoplus_{j=1}^{l} A/(p_j^{r_{j,i}}),$$

donc

$$\bigoplus_{1 \leq i < \infty} A/(a_i) \simeq M.$$

D'autre part, la suite des idéaux (a_i) est croissante, et pour i assez grand, $(a_i) = A$; soit $n = \#\{i \mid (a_i) \neq A\}$.
Alors on a bien $(a_1) \subset (a_2) \subset \cdots \subset (a_n) \neq A$, et

$$M \simeq \bigoplus_{1 \leq i \leq n} A/(a_i).$$

2) Il s'agit de montrer que si

$$M \simeq \bigoplus_{1 \leq i \leq n} A/(a_i) \simeq \bigoplus_{1 \leq j \leq m} A/(b_i),$$

avec $(a_1) \subset (a_2) \subset \cdots \subset (a_n) \neq A$ et $(b_1) \subset (b_2) \subset \cdots \subset (b_m) \neq A$, alors $n = m$ et $a_i \sim b_i$ pour tout i.
Une remarque préliminaire. Soit p un irréductible de A, et soit $E = A/(q)$, avec $q \in A - \{0\}$. Si p est premier à q, $pE = A/(q)$, et $E/pE = 0$. Si par contre $p \mid q$, $pE \simeq A/(q/p)$ et $E/pE \simeq A/(p)$.
Ainsi, M/pM est un $A/(p)$-espace vectoriel de dimension le nombre de valeurs de i pour lesquelles $p \mid a_i$, et aussi le nombre de valeurs de j pour lesquelles $p \mid b_j$.
On peut choisir p de sorte qu'il divise tous les a_i; alors n est égal au nombre de valeurs de j pour lesquelles $p \mid b_j$, d'où $n \leq m$. par raison de symétrie, $n = m$. On voit que p divise aussi tous les b_i.
Reste à montrer : $a_i \sim b_i$ pour $1 \leq i \leq n$. On procède par récurrence sur le nombre de facteurs irréductibles de $a_1 \ldots a_n$. Le cas $N = 0$ correspond à $M = 0$, donc $n = 0$ et il n'y a rien à dire. Soit $N > 0$. Soit p un irréductible de A qui divise a_n, et donc aussi b_n. Soit n' (resp. m') le nombre de valeurs de i pour lesquelles p n'est pas associé à a_i (resp. à b_i). Alors

$$pM \simeq \bigoplus_{1 \leq i \leq n'} A/(a_i/p) \simeq \bigoplus_{1 \leq i \leq m'} A/(b_i/p).$$

On a donc $n' = m'$. De plus, le nombre de facteurs irréductibles de $a_1/p \cdots a_{n'}/p$ est $< N$. On en déduit donc par récurrence que pour tout $i \leq n'$, $a_i/p \sim b_i/p$. On a donc $a_i \sim b_i$ pour tout $i = 1, \ldots, n$. $\square$

4.5. Classification des sous-modules d'un module libre

4.5.1. Théorème. *Soit A un anneau principal, et L un A-module libre de rang fini n. Soit M un sous-module de L de rang r. Alors*
1) il existe une base $(e_1, \dots, e_n)$ de L, et des éléments non nuls $a_1, \dots a_r \in A$ tels que $(a_1 e_1, \dots, a_r e_r)$ soit une base de M, avec $(a_1) \subset \dots \subset (a_r)$.
2) la suite $(a_1), \dots, (a_r)$ est uniquement déterminée par ces conditions.

DEMONSTRATION.
1) Quelques préliminaires.
Pour $x \in L$, notons $I(x)$ l'ensemble des éléments de A de la forme $\lambda(x)$, où λ décrit l'ensemble des application A-linéaires de L dans A. C'est un idéal de A. On peut le décrire de la façon suivante : soient $(\varepsilon_1, \dots, \varepsilon_n)$ une base quelconque de L, et $x_1, \dots, x_n$ les coordonnées de x dans cette base. Alors $I(x)$ est l'idéal de A engendré par les x_i; autrement dit, c'est l'idéal engendré par le PGCD des x_i.
En particulier, pour $x \in L$ et $a \in A$, on a $I(ax) = aI(x)$; et si $I(x) = (a)$, il existe $e \in L$ tel que $x = ae$.

4.5.2. Lemme. *Soit e un élément non nul de L. Les conditions suivantes sont équivalentes :*
(i) L/Ae est sans torsion;
(ii) il existe un sous-module $L'' \subset L$ tel que $L = Ae \oplus L''$;
(iii) $I(e) = A$.

DEMONSTRATION.
(i) $\Longrightarrow$ (ii) résulte de **3.4.3.** et **4.1.2.**.
(ii) $\Longrightarrow$ (iii). Supposons $L = Ae \oplus L''$. Soit $\lambda : L \longrightarrow A$ l'application définie par $\lambda(ae + x'') = a$ pour $a \in A$ et $x'' \in L''$. Alors $\lambda(e) = 1$ donc $I(e) = A$.
(iii) $\Longrightarrow$ (i). Supposons $I(e) = A$. Soit ξ un élément de torsion de L/Ae, classe de $x \in L$ modulo Ae.
Il existe $a \in A - \{0\}$ tel que $a\xi = 0$; on a donc $ax = be$ pour un certain $b \in A$. On a $(b) = bI(e) = I(be) = I(ax) = aI(x) \subset (a)$; donc $a \mid b$, de sorte que $x \in Ae$, et $\xi = 0$. □

Démontrons maintenant l'assertion 1) du théorème par récurrence sur $r = \operatorname{rg} M$. Si $r = 0$, n'importe quelle base de L fait l'affaire. Supposons $r > 0$.
Soit x_r un élément de M tel que $I(x_r)$ soit maximal dans l'ensemble des $I(x)$ pour x décrivant M. (Un tel x_r existe car A est noethérien).
Soit a_r un générateur de $I(x_r)$, et e_r l'élément de L tel que $x_r = a_r e_r$. On a $I(e_r) = A$. Soit $L' = Ae_r$. D'après le lemme, il existe un sous-module L'' de L tel que $L = L' \oplus L''$. Soit $M' = M \cap L'$ et $M'' = M \cap L''$.
On se propose de montrer :

$$M = M' \oplus M''.$$

Pour cela, observons que tout $x \in M$ s'écrit de manière unique $x' + x''$, avec $x' \in L'$ et $x'' \in L''$; il suffit alors de vérifier que $x' \in M$. Soit $a \in A$ tel que $x' = ae_r$, et c un PGCD de a_r et de a. Soient u, $v \in A$ tels que $c = ua_r + va$. Posons $y = ux_r + vx$. On a $y \in M$, et $y = ua_r e_r + vae_r + vx'' = ce_r + vx''$, donc $c \in I(y)$. Ainsi $I(x_r) = (a_r) \subset (c) \subset I(y)$.

D'après le choix de x_r, ceci entraîne $I(x_r) = I(y)$; d'où $(a_r) = (c)$, et donc $a \in (a_r)$. Ainsi, $x' \in a_r x_r \subset M'$, ce qui achève de démontrer $M = M' \oplus M''$.
Or, M'' est un sous-module de rang $r-1$ du module libre L''. Par hypothèse de récurrence, il existe une base $(e_1, \ldots, e_{r-1})$ de L'' et des éléments non nuls $a_1, \ldots, a_{r-1}$ de A tels que $(a_1e_1, \ldots, a_{r-1}e_{r-1})$ soit une base de M'', avec en outre $(a_1) \subset \cdots \subset (a_{r-1})$. Ainsi $(e_1, \ldots, e_n)$ est une base de L, et $(a_1e_1, \ldots, a_re_r)$ une base de M.
Pour conclure, il suffit donc de vérifier : $(a_{r-1}) \subset (a_r)$. Soit $x = a_1e_1 + \cdots + a_re_r \in M$. On a $I(x) = (a_1, \ldots, a_r)$ donc $(a_i) \subset I(x)$ pour $i = 1, \ldots, r$. D'après le choix de x_r, on a donc $(a_r) = I(x_r) = I(x)$, d'où $(a_{r-1}) \subset (a_r)$.
2) Soient (a_i) et (e_i) comme dans l'énoncé. Soit $Q = L/M$. On a $Q \simeq A/(a_1) \oplus \cdots A/(a_r) \oplus A^{n-r}$. Ainsi, $Q_{\mathsf{tors}} \simeq A/(a_1) \oplus A/(a_r)$, avec $(a_1) \subset \cdots \subset (a_r)$; de plus $r = n - \operatorname{rg} Q$. Soit m le nombre d'indices pour lesquels $(a_i) \neq A$. Alors $a_1, \ldots, a_m$ sont les facteurs invariants de Q_{tors}, d'où l'unicité de la suite des (a_i). $\square$

5. Eléments entiers sur un anneau.

Soit B un anneau, et A un sous-anneau de B. On peut voir B comme une A-algèbre. Si $\mathcal{X}$ est une partie de B, on notera $A[\mathcal{X}]$ le sous-anneau de B engendré par $A \cup \mathcal{X}$. Si $\mathcal{X} = \{x_1, \ldots, x_n\}$, on pose $A[x_1, \ldots, x_n] = A[\mathcal{X}]$.

5.1.1. Théorème-définition. *Soit B un anneau et A un sous-anneau de B. Soit $x \in B$. Les quatre conditions suivantes sont équivalentes :*

(i) il existe un polynôme unitaire Q à coefficients dans A tel que $Q(x) = 0$;

(ii) il existe un entier naturel n tel que $A[x]$ soit engendré comme A-module par les x^l pour $0 \leq l < n$.

(iii) $A[x]$ est un A-module de type fini;

(iv) il existe un sous-anneau de B contenant $A[x]$, et de type fini comme A-module.

On dit que x est entier sur A *si l'une de ces quatre conditions est remplie.*
On dit que B est entier sur A *si tout élément de B est entier sur A.*

Demonstration.
(i) $\Longrightarrow$ (ii) : soit $Q \in A[X]$, unitaire de degré n, tel que $Q(x) = 0$. Soit $z \in A[x]$. Alors z est de la forme $P(x)$, avec $P \in A[X]$. La division euclidienne par Q permet d'écrire P sous la forme $QT + R$, avec T, $R \in A[X]$ et $\deg R < n$,

$$x = Q(x)T(x) + R(x) = R(x) = \sum_{l=0}^{n-1} a_l x^l \,,$$

où a_l désigne le coefficient de degré l de R; ainsi, $A[x]$ est engendré comme A-module par les x^l, pour $0 \leq l < n$.
(ii) $\Longrightarrow$ (iii) de manière immédiate.
(iii) $\Longrightarrow$ (iv) car $A[x]$ convient.
(iv) $\Longrightarrow$ (i) : soit $B_0 \subset B$ un sous-anneau contenant $A[x]$, et de type fini comme A-module.

Soient $y_1, \dots, y_n$ des générateurs de B_0 comme A-module. Il existe des éléments $a_{i,j} \in A$ tels qu'on ait pour tout $i = 1, \dots, n$:

$$xy_i = \sum_{j=1}^{n} a_{i,j} y_j \, .$$

Soit M la matrice $(a_{i,j}) \in M_n(A)$, et $T \in M_n(A[x])$ la matrice $xI_n - M$, dont le coefficient i,j est $t_{i,j} = \delta_{i,j} x - a_{i,j}$.
Le déterminant de T est de la forme $x^n + a_{n-1}x^{n-1} + \cdots + a_0$, avec $a_l \in A$. Il suffit donc de montrer que $\det(T)$ est nul. Or on a pour tout $i = 1, \dots, n$:

$$\sum_{j=1}^{n} t_{i,j} y_j = 0 \, .$$

Le lemme suivant permettra donc de conclure.

Lemme. *Soit R un anneau, et M un R-module de type fini, engendré par des éléments $y_1, \cdots, y_n$. Soit $T = (t_{i,j})$ un élément de $M_n(R)$ vérifiant pour tout $i = 1, \dots, n$:*

$$\sum_{j=1}^{n} t_{i,j} y_j = 0 \, .$$

Alors $\det(T) \in \operatorname{\mathsf{ann}} M$.

DEMONSTRATION. Soit $T^* = (t^*_{i,j})$ la transposée de la comatrice de T (voir l'appendice **II, 6**). On a $\det(T) I_n = T^* T$, donc pour tout $k = 1, \dots, n$:

$$\det(T)\, y_k = \sum_{1 \le j \le n} \det(T)\, \delta_{k,j}\, y_j = \sum_{1 \le i,j \le n} t^*_{k,i}\, t_{i,j}\, y_j = \sum_{i=1}^{n} t^*_{k,i} \sum_{j=1}^{n} t_{i,j} y_j = 0 \, ;$$

ainsi $\det(T)$ est un élément de R qui annule M. □
Il résulte du lemme que $\det(T)$ annule B_0, et donc $\det(T) = \det(T) \cdot 1 = 0$, d'où (i). □

5.1.2. REMARQUES.
1) En vertu du critère (iv), si B est de type fini comme A-module, B est entier sur A. Nous aurons bientôt un résultat plus précis.
2) Soient C un anneau, A et B des sous-anneaux de C vérifiant $A \subset B$. Soit $x \in C$. En vertu du critère (i), si x est entier sur A, il est entier sur B.

5.1.3. Proposition. *Soit B un anneau et A un sous-anneau de B. L'ensemble des éléments de B qui sont entiers sur A est un sous-anneau de B contenant A.*

DEMONSTRATION.
Elle repose sur le lemme suivant.

5.1.4. Lemme. *Soit B_0 un sous-anneau de B contenant A, et de type fini comme A-module. Soit y un élément de B entier sur B_0. Alors $B_0[y]$ est un A-module de type fini. En particulier, $B_0[y]$ est entier sur A.*

DEMONSTRATION. En vertu du critère (iii), $B_0[y]$ est engendré comme B_0-module par $1, y, \ldots, y^{n-1}$ (pour un certain $n \in \mathbb{N}$), et par hypothèse, B_0 est engendré comme A-module par des éléments $x_1, \ldots, x_m$ (pour un certain $m \in \mathbb{N}$).
Ainsi tout $z \in A_0[y]$ s'écrit $b_0 + b_1 y + \cdots + b_{n-1} y^{n-1}$, avec $b_j \in B_0$, et chaque b_j s'écrit $a_{1,j} x_1 + a_{2,j} x_2 + \cdots + a_{m,j} x_m$, avec $a_{i,j} \in A$. Donc z est combinaison linéaire à coefficients dans A des $x_i y^j$ pour $1 \leq i \leq m$ et $0 \leq j < n$, ce qui montre que $B_0[y]$ est un A-module de type fini. D'après la remarque 1), il est entier sur A. □

Soient x, $y \in B$ entiers sur A. Alors $B_0 = A[x]$ est de type fini comme A-module selon le critère (iii), et y est entier sur B_0 en vertu de la remarque 2). Il résulte du lemme que tout élément de $A[x, y] = A[x][y]$ est entier sur A; c'est en particulier le cas de $x - y$, de xy et de tout élément de A, d'où la proposition. □

5.1.5. Proposition. *Soit B un anneau et A un sous-anneau de B. Si B est de type fini comme A-algèbre, on a l'équivalence*

$$B \text{ est un } A\text{-module de type fini} \iff B \text{ est entier sur } A.$$

DEMONSTRATION. On a déjà constaté $\Longrightarrow$. Montrons la réciproque. Par hypothèse, B est de la forme $A[x_1, \ldots, x_n]$. Montrons par récurrence sur n que si B est entier sur A, B est un A-module de type fini. Si $n = 0$, c'est trivial. Pour $n > 0$, posons $B_0 = A[x_1, \ldots, x_{n-1}]$. Par hypotèse de récurrence B_0 est de type fini comme A-module; de plus x_n est entier sur A, donc sur B_0. Il résulte donc du lemme **5.1.4** que $B = B_0[x_n]$ est de type fini comme A-module. □

5.1.6. Théorème.
1) Soient C un anneau, A et B des sous-anneaux de C vérifiant $A \subset B$. On a l'équivalence :

$$C \text{ est entier sur } A \iff C \text{ est entier sur } B \text{ et } B \text{ est entier sur } A.$$

2) Soient D un anneau, A, B et C des sous-anneaux de D. On suppose $A \subset B$ et $A \subset C$. Rappelons qu'on note $B[C]$ le sous-anneau de D engendré par B et C. Alors si B est entier sur A, $B[C]$ est entier sur C.

DEMONSTRATION.
Assertion 1). L'implication $\Longrightarrow$ est claire. La réciproque résultera immédiatement du lemme suivant.

5.1.7. Lemme. *Supposons B entier sur A. Soit $x \in C$. Si x est entier sur B, x est entier sur A.*

DEMONSTRATION. Si x est entier sur B, on a $x^n + b_{n-1} x^{n-1} + \cdots + b_0 = 0$, avec $b_i \in B$. Posons $B_0 = A[b_0, \cdots, b_{n-1}]$. Alors x est entier sur B_0. De plus B_0 est entier sur A; c'est donc un A-module de type fini en vertu de **5.1.5.** Appliquant le lemme **4.1.4** à l'élément x, on voit que ce dernier est entier sur A. □

Assertion 2). Supposons B entier sur A. Alors tout élément de B est entier sur C. Les éléments de D qui sont entiers sur C constituent un sous-anneau de D qui contient C et B, donc aussi le sous-anneau de D engendré par B et C, à savoir $B[C]$. □

5.2. Anneaux intégralement clos

5.2.1. Définition. Soit A un anneau intègre. On dit que A est *intégralement clos* si les éléments de $\mathsf{Frac}\,A$ entiers sur A sont les éléments de A.

5.2.2. Proposition. *Si A est factoriel, A est intégralement clos.*

DEMONSTRATION. Tout $x \in \mathsf{Frac}\,A$ s'écrit $x = p/q$, avec $p,\ q \in A$ premiers entre eux, et $q \neq 0$. Supposons $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, avec $a_l \in A$. Multipliant ceci par q^n, il vient

$$p^n = -a_1p^{n-1}q - a_2p^{n-2}q^2 - \cdots - a_nq^n\,,$$

donc q divise p^n; or q est premier à p^n, donc $q \in A^*$ et par conséquent $x \in A$. □

Cependant, un anneau intègre peut être intégralement clos sans être pour autant factoriel.

6. Appendice : Déterminants

Soit R un anneau, et $n \in \mathbb{N}$. Notons E le R-module libre R^n, et pour $1 \le i \le n$, soit e_i le i-ième vecteur de la base canonique de E. Une matrice $n \times n$ peut être considérée comme la suite de ses vecteurs-colonnes $C_1, \ldots, C_n$. Ainsi, $M_n(R)$ s'identifie à E^n.
Soit $\mathcal{D}_n$ l'ensemble des applications $\delta : E^n \longrightarrow A$ vérifiant :
1) δ est R-linéaire en chaque variable;
2) $\delta(C_1, \ldots, C_n)$ est nul s'il existe $1 \le i < j \le n$ tels que $C_i = C_j$.
Il est clair que l'ensemble $\mathcal{D}_n$ est un sous-module du R-module des applications de $M_n(R)$ dans R, et qu'il contient $\det$.

Théorème. *Pour tout $\delta \in \mathcal{D}_n$, on a*

$$\delta = \delta(1_n) \cdot \det\ .$$

DEMONSTRATION. Soit $\delta \in \mathcal{D}_n$. Soit σ une application de $\{1, \ldots, n\}$ dans lui-même. Soit T_σ la matrice dont le coefficient $i,\ j$ est 1 si $i = \sigma(j)$, et 0 sinon.
On observe que $\delta(T_\sigma)$ est nul si σ n'est pas injective. Si $\sigma \in \mathfrak{S}_n$, T_σ s'obtient à partir de 1_n en effectuant la permutation σ sur les colonnes de 1_n. On a donc $\delta(T_\sigma) = \varepsilon(\sigma)\delta(1_n)$.
Soit $A = (a_{i,j}) \in M_n(A)$. Si C_j désigne le j-ième vecteur-colonne de A, on a

$$C_j = \sum_{i=1}^{n} a_{i,j}e_i\,.$$

On a donc

$$\begin{aligned}\delta(A) &= \sum_{\sigma \in \{1,\ldots,n\}^{\{1,\ldots,n\}}} a_{\sigma(1),1} \cdots a_{\sigma(n),n}\delta(T_\sigma)\\ &= \delta(1_n) \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)a_{\sigma(1),1} \cdots a_{\sigma(n),n} = \delta(1_n)\det(A)\,.\ \square\end{aligned}$$

Corollaire. *Pour* $A,\ B \in M_n(R)$, *on a* $\det(AB) = \det A \det B$.

DEMONSTRATION.
L'application $\delta_A : E^n \longrightarrow R$ définie par $(C_1, \ldots, C_n) \mapsto \det(AC_1, \ldots, AC_n)$, est un élément de $\mathcal{D}_n$; on a donc $\delta_A = \delta_A(1_n) \cdot \det$. D'autre part, on a pour $B \in M_n(R) \simeq E^n$, $\delta_A(B) = \det(AB)$; en particulier $\delta_A(1_n) = \det A$, d'où $\det(AB) = \det A \det B$. □

Définition. Soit $A = (a_{i,j}) \in M_n(R)$. Pour $1 \leq i, j \leq n$, on note $A_{i,j}$ l'élément de $M_{n-1}(R)$ obtenu à partir de A en supprimant la i-ième ligne et la j-ième colonne. On appelle *comatrice de* A l'élément de $M_n(A)$ dont le coefficient i, j est $(-1)^{i+j} \det(A_{i,j})$. On note A^* la transposée de la comatrice de A.

Proposition. *On a* $AA^* = A^*A = \det A\, I_n$.

DEMONSTRATION.
Soit $a^*_{i,j}$ le coefficient i, j de A^*.
Soient $C_1, \ldots, C_n$ les vecteurs colonnes de A. Pour $j \in [n]$ et $C \in A^n$, posons

$$A_j(C) = (C_1, \ldots, C_{j-1}, C, C_{j+1}, \ldots, C_n).$$

On a $\det A_j(e_i) = (-1)^{i+j} \det A_{i,j} = a^*_{j,i}$.
Par ailleurs, la matrice $A_i(C_j)$ est égale à A si $i = j$, mais dans le cas contraire elle présente deux vecteurs colonne identiques. On a donc $\det A_i(C_j) = \delta_{i,j} \det A$. Or

$$\det A_i(C_j) = \sum_{k \in [n]} a_{k,j} \det A_i(e_k) = \sum_{i \in [n]} a^*_{i,k} a_{k,j}\,,$$

qui n'est autre que le coefficient i, j de A^*A; d'où $A^*A = \det AI_n$.
L'autre formule s'en déduit, par exemple en constatant que $({}^tA)^* = {}^t(A^*)$. □

Chapitre III : THEORIE DE GALOIS

Ce chapitre regroupe cinq sections. Dans la première sont rassemblés, à titre de référence, divers rappels sur la théorie des groupes. La seconde est consacrée aux corps commutatifs et à leurs extensions. Le théorème de Galois fait l'objet de la troisième section. La quatrième regroupe quelques exemples d'application du théorème de Galois. La cinquième section traite de la résolution des équations algébriques par radicaux.

1. Rappels sur les groupes

1.1. Groupes et morphismes de groupes

Définition. Un *groupe* est un ensemble G muni d'une loi de composition interne (qu'on notera multiplicativement) vérifiant les conditions suivantes :

— la loi de composition est associative;

— il existe un élément neutre dans G;

— tout élément g de G admet un inverse, noté g^{-1}.

Le groupe G est dit *commutatif*, ou *abélien*, si la loi de composition est commutative.

Exemples.

1) Si X est un ensemble, les bijections de X sur lui-même constituent, pour la composition des applications, un groupe appelé *groupe symétrique de* X et noté $\mathfrak{S}_X$. Pour tout entier $n > 0$, le groupe symétrique de $\{1, 2, \ldots, n\}$ est noté $\mathfrak{S}_n$.

2) Pour n entier, $n \geq 0$, $\mathbb{Z}/n\mathbb{Z}$, muni de l'addition, est un groupe commutatif.

Définition. Si G est un groupe, on appelle *sous-groupe de* G tout sous-ensemble H de G vérifiant :

— H est non vide;

— pour tous g, g' dans H, $g' g^{-1}$ est encore dans H.

Si G est un groupe, le sous-ensemble de G réduit à l'élément neutre est un sous-groupe appelé *sous-groupe trivial de* G, et qu'on notera le plus souvent 1.

Définition. Si G et G' sont deux groupes, on appelle *morphisme de groupes de* G *vers* G' toute application $f : G \longrightarrow G'$ compatible aux lois de composition internes, c'est-à-dire satisfaisant la condition $f(g\, g') = f(g) f(g')$ pour tous g, g' dans G.

Remarques.

1) La composée de deux morphismes de groupes, lorsqu'elle a un sens, est encore un morphisme de groupes. Si G est un groupe, l'identité de G est un morphisme de groupes de G dans G.

2) Si H est un sous-groupe d'un groupe G, il admet une structure de groupe unique de sorte que l'inclusion soit un morphisme de groupes de H vers G.

Définitions. Si $f : G \longrightarrow G'$ est un morphisme de groupes, l'image de f est un sous-groupe de G' qu'on note $\mathsf{Im}(f)$; de même, l'image réciproque par f de l'élément neutre de G' est un sous-groupe de G appelé *noyau de* f et noté $\mathsf{Ker}(f)$. Le morphisme f est injectif si et seulement si son noyau est le sous-groupe trivial.

1.1.1. Proposition. *Soient G, G', Γ trois groupes, et $f : G \longrightarrow G'$ et $p : G \longrightarrow \Gamma$ deux morphismes de groupes; on suppose p surjectif. On cherche un morphisme de groupes $\widetilde{f} : \Gamma \longrightarrow G'$ tel que l'on ait : $f = \widetilde{f} \circ p$.*
1) Un tel $\widetilde{f}$ existe si et seulement si $\mathsf{Ker}(p) \subset \mathsf{Ker}(f)$.
2) Quand $\widetilde{f}$ existe, il est unique. Il est surjectif si et seulement si f est surjectif, et il est injectif si et seulement si $\mathsf{Ker}(f) = \mathsf{Ker}(p)$.

DEMONSTRATION.
1) Il est clair que si $\widetilde{f}$ existe, on a $\mathsf{Ker}(p) \subset \mathsf{Ker}(f)$. Si $\mathsf{Ker}(p) \subset \mathsf{Ker}(f)$, soit $\gamma \in \Gamma$, et choisissons $g \in G$ tel que $p(g) = \gamma$. Posons $\widetilde{f}(\gamma) = f(g)$ (c'est obligatoire). Cette définition n'est pas ambigüe, car pour tout autre choix g', on aurait $p(g'g^{-1}) = p(g')p(g^{-1}) = \gamma\gamma^{-1} = e$, donc $g'g^{-1} \in \mathsf{Ker}(p) \subset \mathsf{Ker}(f)$, et $f(g') = f(g)$. On vérifie aisément que le $\widetilde{f}$ ainsi défini convient.
2) L'unicité est évidente, p étant surjectif. On a $\mathsf{Im}(f) = \mathsf{Im}(\widetilde{f})$. Enfin, $\mathsf{Ker}(\widetilde{f}) = p(\mathsf{Ker}(f))$, donc $\widetilde{f}$ est injectif si et seulement si $\mathsf{Ker}(f) = \mathsf{Ker}(p)$. □

1.2. Classes à droite et quotient à droite

Définitions. Soit G un groupe, H un sous-groupe de G, et g un élément de G. Le sous-ensemble $gH = \{gh, h \in H\}$ s'appelle la *classe à droite de g modulo H*. Les classes à droite modulo H constituent une partition de G; l'ensemble des classes à droite modulo H est appelé quotient à droite de G par H, et noté G/H ; l'application

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ g &\longmapsto gH \end{aligned}$$

est appelée *surjection canonique.*

Si G est un groupe et H un sous-groupe de G, on appelle *indice de H dans G* le cardinal du quotient G/H. On le note $[G : H]$; en particulier, l'indice du sous-groupe trivial dans G, qui n'est autre que le cardinal de G, est appelé *ordre de G*, et noté $\mathcal{O}(G)$.

1.2.1. Proposition. *Soit G un groupe et H un sous-groupe de G. Alors on a*

$$\mathcal{O}(G) = [G : H]\mathcal{O}(H).$$

DEMONSTRATION. Soit X un sous-ensemble de G tel que la restriction de la surjection canonique $\pi : G \longrightarrow G/H$ à X soit une bijection de X sur G/H : on a donc $[G : H] = \# X$ (un tel sous-ensemble de G est appelé un *système de représentants des classes à droite de G modulo H*).
Soit $f : X \times H \longrightarrow G$ l'application qui au couple $(x, h) \in X \times H$ associe l'élément xh de G. C'est une bijection. On a donc $\mathcal{O}(G) = \#(X \times H) = [G : H]\mathcal{O}(H)$. □

Remarque. Lorsque l'ordre de G est fini, on a donc $[G:H] = \mathcal{O}(G)/\mathcal{O}(H)$ pour tout sous-groupe H de G; en particulier, l'ordre de H divise l'ordre de G.

1.3. Sous-groupes distingués

Soit G un groupe, et H un sous-groupe de G. Est-il possible de munir le quotient G/H d'une structure de groupe de telle sorte que la surjection canonique $\pi : G \longrightarrow G/H$ soit un morphisme de groupes?

1.3.1. Proposition-définition *Soit G un groupe, et H un sous-groupe de G. Les conditions suivantes sont équivalentes.*

(i) Pour tous $h \in H$ et $g \in G$, $ghg^{-1} \in H$;

(ii) il existe sur G/H une structure de groupe (nécessairement unique) telle que la surjection canonique $G \longrightarrow G/H$ soit un morphisme de groupes;

(iii) il existe un groupe G' et un morphisme de groupes f de G dans G' tel que H soit le noyau de f.

Lorsque l'une de ces conditions est réalisée, on dit que H est un sous-groupe distingué de *G, ce qu'on écrit $H \triangleleft G$.*

Demonstration. (i) $\Longrightarrow$ (ii) : on définit une loi de composition interne sur G/H de la façon suivante. Soit x, x' dans G/H. On choisit g, g' dans G tels que $\pi(g) = x$ et $\pi(g') = x'$. On pose alors $xx' = \pi(gg')$. Cette définition ne dépend pas du choix de g et g', car pour un autre choix g_1, g_1', on aurait $g_1 = gh$, $g_1' = g'h'$ avec h, h' dans H, et alors $g_1g_1' = ghg'h' = gg'(g'^{-1}hg')h'$; or $g'^{-1}hg' \in H$ d'après (i), donc $\pi(g_1g_1') = \pi(gg')$. Par définition, on a $\pi(gg') = \pi(g)\pi(g')$, et comme π est surjectif, la loi de composition ainsi définie sur G/H est associative; $\pi(e)$ est élément neutre, et pour tout $g \in G$, $\pi(g^{-1})$ est inverse de $\pi(g)$, d'où (ii).
(ii) $\Longrightarrow$ (iii) : le noyau de $\pi : G \longrightarrow G/H$ est H.
(iii) $\Longrightarrow$ (i). Soit $f : G \longrightarrow G'$ un morphisme de noyau H. Soit $h \in H$ et $g \in G$. Alors $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)f(g^{-1}) = e$ donc $ghg^{-1} \in H$. □

Exemple. Soit $n \geq 2$. Il existe un morphisme surjectif unique de $\mathfrak{S}_n$ vers $\mathbb{Z}/2\mathbb{Z}$, qu'on appelle *signature* et qu'on note ε. Le noyau de ε est un sous-groupe distingué de $\mathfrak{S}_n$, d'indice 2, qu'on appele *groupe alterné d'indice* n et qu'on note $\mathfrak{A}_n$.

Définition. Soit G un groupe et H un sous-groupe de G. On appelle *normalisateur de H dans G*, et on note $N_G(H)$, l'ensemble des $g \in G$ tels que $gHg^{-1} = H$; c'est le plus grand sous-groupe de G dans lequel H soit distingué.

Nous aurons besoin de quelques propriétés des sous-groupes distingués.

1.3.2. Proposition. *Soit G un groupe, H et U deux sous-groupes de G. On suppose que U est contenu dans le normalisateur de H. Alors :*
1) $H \cap U$ est un sous-groupe distingué de U ;
2) l'ensemble $HU = UH$ est un sous-groupe de G dans lequel H est distingué;
3) on a un isomorphisme naturel

$$U/(H \cap U) \simeq UH/H \quad .$$

DEMONSTRATION.
1) est évident. Précisons que si X et Y sont des parties de G, XY désigne l'ensemble des produits xy, $x \in X$ et $y \in Y$. On a $UH \subset HU$, car $uh = (uhu^{-1})u \in HU$, et de même $HU \subset UH$, donc $HU = UH$. On a $HU \neq \emptyset$, car HU contient H et U. Enfin, si x, $y \in HU$, on a $y^{-1} \in UH$, et donc $y^{-1}x \in UHHU \subset UHU = HUU \subset HU$ donc $HU = UH$ est un sous-groupe de G; il est contenu dans $N_G(H)$, donc 2) est vérifié. Soit $f : U \longrightarrow HU/H$ le morphisme de groupes qui à $u \in U$ associe sa classe modulo H. Alors f est surjectif, de noyau $U \cap H$, d'où l'isomorphisme $U/(U \cap H) \simeq HU/H$ d'après 1.1.1. □

Soit G un groupe et H un sous-groupe distingué de G. Soit $\pi : G \longrightarrow G/H$ le morphisme canonique. Si G' est un sous-groupe de G/H, $\pi^{-1}(G')$ est un sous-groupe de G contenant H. On définit ainsi une bijection entre l'ensemble des sous-groupes de G/H et l'ensemble des sous-groupes de G contenant H. Dans cette bijection, les sous-groupes distingués se correspondent. Quand K est un sous-groupe de G contenant H, on identifiera souvent implicitement K/H au sous-groupe $\pi(K) \subset G/H$.

1.3.3. Proposition. *Soit G un groupe commutatif, et H, K deux sous-groupes distingués de G, avec $H \subset K$. Alors on a l'isomorphisme*

$$(G/H)/(K/H) \simeq G/K \quad .$$

DEMONSTRATION. Le morphisme naturel $G/H \longrightarrow G/K$ est surjectif, et a pour noyau K/H. □

1.4. Groupes résolubles

Définition. Soit G un groupe. Une *filtration distinguée de G* est une suite croissante de sous-groupes $1 = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_m = G$ telle que G_{i-1} soit distingué dans G_i pour $i = 1, \ldots m$. On écrira alors $1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_m = G$.

1.4.1. Lemme *Soit G un groupe, et H un sous-groupe de G.*
1) Soit $1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_m = G$ une filtration distinguée de G. Posons $H_i = H \cap G_i$. Alors $1 = H_0 \lhd H_1 \lhd H_2 \lhd \ldots \lhd H_m = H$ est une filtration distinguée de H, et H_i/H_{i-1} est isomorphe à un sous-groupe de G_i/G_{i-1}.
2) On suppose H distingué dans G. Soit $1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_m = G$ une filtration distinguée de G. Notons G'_i l'image de G_i dans G/H. Alors $1 = G'_0 \lhd G'_1 \lhd G'_2 \lhd \ldots \lhd G'_m = G/H$ est une filtration distinguée de G/H, et G'_i/G'_{i-1} est isomorphe à un quotient de G_i/G_{i-1}.
3) On suppose toujours H distingué dans G, et on note π le morphisme canonique $G \longrightarrow G/H$. Soit $1 = H_0 \lhd H_1 \lhd H_2 \lhd \ldots \lhd H_p = H$ une filtration distinguée de H, et $1 = G'_0 \lhd G'_1 \lhd G'_2 \lhd \ldots \lhd G'_q = G/H$ une filtration distinguée de G/H. Soit $m = p + q$; pour $i = 1, \ldots m$ on définit un sous-groupe G_i de G en posant $G_i = H_i$ si $i \leq p$ et $G_i = \pi^{-1}G'_{i-p}$ si $i \geq p$. Alors $1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_m = G$ est une filtration distinguée de G, et G_i/G_{i-1} est isomorphe à H_i/H_{i-1} pour $i = 1, \ldots p$ et à G'_{i-p}/G'_{i-p-1} pour $i = p+1, \ldots m$.

DEMONSTRATION. Ce lemme résulte directement de ce qui précède. □

Définition. Un groupe G est *résoluble* s'il admet une filtration distinguée $1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_m = G$ telle que G_i/G_{i-1} soit commutatif pour tout $i = 1, \ldots m$.

1.4.2. Proposition. *Soit G un groupe, et H un sous-groupe de G. Alors :*
(i) si G est résoluble, H l'est aussi;
(ii) si $H \lhd G$, alors G est résoluble si et seulement si H et G/H sont résolubles.

DEMONSTRATION.
(i) résulte immédiatement de l'assertion 1) du lemme, et du fait qu'un sous-groupe d'un groupe commutatif est commutatif.
(ii) G résoluble $\Longrightarrow$ G/H résoluble : ceci résulte de l'assertion 2) du lemme, et du fait qu'un quotient d'un groupe commutatif est commutatif.
H résoluble et G/H résoluble $\Longrightarrow$ G résoluble résulte immédiatement de l'assertion 3) du lemme. □

EXEMPLE. Soit $n \geq 3$, et P_n un polygone régulier à n sommets dans le plan euclidien. Les isométries de P_n constituent un groupe d'ordre $2n$, qu'on appelle *groupe diédral d'indice n* et qu'on note D_n. Le groupe diédral contient un sous-groupe distingué d'indice 2, isomorphe à $\mathbb{Z}/n\mathbb{Z}$: c'est le groupe des rotations, qui est engendré par la rotation d'un n-ième de tour. Ainsi, le groupe diédral est résoluble.

1.5. Groupes simples et théorème de Jordan-Hölder

Définition. Un groupe G est dit *simple* s'il est non trivial ($G \neq 1$) et s'il n'admet pas d'autre sous-groupe distingué que 1 et G.

EXEMPLES.
1) Les groupes simples commutatifs sont les $\mathbb{Z}/p\mathbb{Z}$, avec p premier.
2) On montre que les groupes alternés $\mathfrak{A}_n$ sont simples pour $n = 3$ et $n \geq 5$ (mais $\mathfrak{A}_4$ n'est pas simple : il admet un sous-groupe distingué d'ordre 4). En particulier, pour $n \geq 5$, $\mathfrak{A}_n$ n'est pas résoluble, et $\mathfrak{S}_n$ non plus.

1.5.1. Théorème. (de Jordan-Hölder)
Soit G un groupe fini.
(i) Il existe une filtration distinguée $1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_m = G$ de G telle que les quotients G_i/G_{i-1} soient tous simples.
(ii) Si $1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_m = G$ et $1 = \Gamma_0 \lhd \Gamma_1 \lhd \Gamma_2 \lhd \ldots \lhd \Gamma_n = G$ sont deux filtrations distinguées de G telles que les quotients G_i/G_{i-1} et Γ_j/Γ_{j-1} soient simples, alors $m = n$ et il existe une bijection σ de $\{1, \ldots m\}$ dans lui-même, telle que G_i/G_{i-1} soit isomorphe à $\Gamma_{\sigma(i)}/\Gamma_{\sigma(i)-1}$ pour tout $i = 1, \ldots m$.

Les groupes simples G_i/G_{i-1} de l'assertion (i) sont appelés *groupes simples associés à G*. L'assertion (ii) signifie que ces groupes simples sont uniquement déterminés à isomorphisme et ordre près.

DEMONSTRATION DE **1.5.1.**
Démontrons l'assertion (i) par récurrence sur l'ordre du groupe G. Si G est trivial, la filtration distinguée $1 = G_0 = G$ convient. Soit $N > 0$. Supposons l'assertion vraie pour tout groupe d'ordre $< N$ et montrons qu'elle est encore vraie pour un groupe G d'ordre N. Si G est simple, la filtration distinguée $1 = G_0 \triangleleft G_1 = G$ convient; on peut donc supposer que G n'est pas simple. Il existe alors $H \triangleleft G$, avec $1 \neq H \neq G$. L'assertion (i) est vraie pour H et pour G/H, et en appliquant l'assertion 3) du lemme 1.4.1, on voit qu'elle est encore vraie pour G.
La démonstration de l'assertion (ii), plus délicate, nécessite le lemme suivant.

1.5.2. Lemme (dit 'du papillon') *Soit G un groupe, U et V deux sous-groupes de G, H un sous-groupe distingué de U et K un sous-groupe distingué de V.*
Alors $H(U \cap K) \triangleleft H(U \cap V)$ et $(H \cap V)K \triangleleft (U \cap V)K$. En outre, les quotients $H(U \cap V)/H(U \cap K)$ et $(U \cap V)K/(H \cap V)K$ sont isomorphes.

DEMONSTRATION. On a $H \triangleleft U$, donc d'après **1.3.2,** $H(U \cap K) = (U \cap K)H$ et $H(U \cap V) = (U \cap V)H$ sont des sous-groupes de U. Montrons que $H(U \cap K)$ est distingué dans $H(U \cap V)$. Soit $x \in H(U \cap K)$ et $g \in H(U \cap V)$; il s'agit de vérifier : $gxg^{-1} \in H(U \cap K)$. Posons $g = hu$, avec $h \in H$ et $u \in U \cap V$. Alors $gxg^{-1} = h(uxu^{-1})h^{-1}$; il suffit donc de montrer $uxu^{-1} \in H(U \cap K)$. Posons $x = hk$, avec $h \in H$ et $k \in U \cap K$. Alors $uxu^{-1} = (uhu^{-1})(uku^{-1})$. Or $uhu^{-1} \in H$ car $H \triangleleft U$, et $uku^{-1} \in U \cap K$ car $K \triangleleft V$ et u, $k \in U$. D'où $H(U \cap K) \triangleleft H(U \cap V)$.
Considérons à présent le morphisme de groupes

$$\begin{aligned} f : U \cap V &\longrightarrow H(U \cap V)/H(U \cap K) \\ g &\longmapsto \text{classe de } g \quad . \end{aligned}$$

Alors f est surjectif; en effet, tout $y \in H(U \cap V)/H(U \cap K)$ est la classe d'un produit hg, avec $h \in H$ et $g \in U \cap V$; la classe de h étant triviale, $y = f(g)$. On a $\mathsf{Ker}(f) = U \cap V \cap H(U \cap K)$. Montrons à présent : $\mathsf{Ker}(f) = (H \cap V)(U \cap K)$. Notons au passage que, $H \cap V$ et $U \cap K$ étant tous deux distingués dans $U \cap V$, $(H \cap V)(U \cap K) = (U \cap K)(H \cap V)$ est un sous-groupe de $U \cap V$. On a clairement $(H \cap V)(U \cap K) \subset U \cap V \cap H(U \cap K)$. Réciproquement, soit $g \in U \cap V \cap H(U \cap K)$; alors $g = hk$, avec $h \in H$, $k \in U \cap K$, et $g \in V$ implique $h \in V$. On a donc bien $g \in (H \cap V)(U \cap K)$.
D'où, par passage au quotient, un isomorphisme

$$(U \cap V)/(H \cap V)(U \cap K) \simeq H(U \cap V)/H(U \cap K).$$

Comme (U, H) et (V, K) jouent des rôles symétriques, on a également $(H \cap V)K \triangleleft (U \cap V)K$, et un isomorphisme

$$(U \cap V)/(H \cap V)(U \cap K) \simeq (U \cap V)K/(H \cap V)K.$$

On en déduit un isomorphisme entre $H(U \cap V)/H(U \cap K)$ et $(U \cap V)K/(H \cap V)K$, d'où le lemme. □

Revenons à la démonstration de l'assertion (ii) du théorème de Jordan-Hölder. Soit $1 = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_m = G$ et $1 = \Gamma_0 \triangleleft \Gamma_1 \triangleleft \Gamma_2 \triangleleft \ldots \triangleleft \Gamma_n = G$ deux filtrations distinguées de G telles que les quotients G_i/G_{i-1} et Γ_j/Γ_{j-1} soient simples.
Formons les sous-groupes

$$\begin{aligned} G_{i,j} &= G_{i-1}(\Gamma_j \cap G_i) \qquad \text{pour } i = 1, \ldots, m \text{ et } j = 0, \ldots, n; \\ \Gamma_{i,j} &= (\Gamma_j \cap G_i)\Gamma_{j-1} \qquad \text{pour } i = 0, \ldots, m \text{ et } j = 1, \ldots, n; \end{aligned}$$

et appliquons le lemme du papillon avec $U = G_i$, $V = \Gamma_j$, $H = G_{i-1}$ et $K = \Gamma_{j-1}$. Il vient :

$$G_{i,j}/G_{i,j-1} \simeq \Gamma_{i,j}/\Gamma_{i-1,j} \quad . \tag{1}$$

D'autre part, on a pour tout $i = 1, \ldots, m$:

$$G_{i-1} = G_{i,0} \triangleleft G_{i,1} \triangleleft \ldots G_{i,n} = G_i \quad .$$

Comme G_i/G_{i-1} est simple, chacun des $G_{i,j}$ est égal soit à G_i, soit à G_{i-1}. Ainsi il existe un unique indice $j = \sigma(i) \in \{1, \ldots, n\}$ tel que le groupe $G_{i,j}/G_{i,j-1}$ soit non trivial, et il est alors isomorphe à G_i/G_{i-1}. Le même raisonnement, appliqué aux $\Gamma_{i,j}$, montre que pour $j = 1, \ldots, n$, il existe un unique indice $i = \tau(j) \in \{1, \ldots, m\}$ tel que le groupe $\Gamma_{i,j}/\Gamma_{i-1,j}$ soit non trivial, et il est alors isomorphe à Γ_j/Γ_{j-1}. D'après l'isomorphisme (1), σ et τ sont inverses l'un de l'autre, d'où l'assertion (ii) du théorème. □

1.6. Groupe agissant sur un ensemble et formule des orbites

Définition. Soit G un groupe et X un ensemble. Une *action, ou opération (à gauche) de G sur X* est la donnée d'une application

$$\begin{aligned} \rho : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

vérifiant les conditions suivantes :
— pour tous g, $g' \in G$ et $x \in X$, $(gg') \cdot x = g \cdot (g' \cdot x)$;
— pour tout $x \in X$, $e \cdot x = x$.
On écrira généralement gx pour $g \cdot x$.

Donnons-nous une action d'un groupe G sur un ensemble X. Pour $g \in G$ notons ρ_g l'application de X dans lui-même qui à x associe $\rho_g(x) = g \cdot x$. On a alors $\rho_{gg'} = \rho_g \circ \rho_{g'}$ et $\rho_e = 1_X$. Autrement dit, ρ définit un morphisme de groupes

$$G \longrightarrow \mathfrak{S}_X \quad .$$

Réciproquement, tout morphisme de groupes $\phi : G \longrightarrow \mathfrak{S}_X$ définit une action de G à gauche sur X (en posant $\rho(g, x) = \phi(g)(x)$).

Pour $x \in X$, l'ensemble $\mathsf{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}$ s'appelle le *stabilisateur de x dans G*; c'est un sous-groupe de G. L'ensemble $G \cdot x = \{g \cdot x; g \in G\}$ s'appelle *orbite de x sous l'action de G*.
Les orbites $G \cdot x$ constituent une partition de l'ensemble X. L'ensemble des orbites est appelé *quotient de X par G* et noté X/G.
On a donc la surjection canonique

$$\begin{aligned} \pi : X &\longrightarrow X/G \\ x &\longmapsto G \cdot x \end{aligned}$$

et on appelle *système de représentants des orbites de X (sous l'action de G)* tout $X' \subset X$ tel que π induise une bijection de X' sur X/G.

1.6.1. Proposition. *Soit G un groupe opérant sur un ensemble X, et $X' \in X$ un système de représentants des orbites de X. Alors on a la formule suivante, dite* formule des orbites :

$$\# X = \sum_{x \in X'} [G : \mathsf{Stab}_G(x)] \quad .$$

Demonstration. Comme les orbites constituent une partition de X, on a

$$\# X = \sum_{x \in X'} \# G \cdot x \quad .$$

L'application $\sigma_x : G \longrightarrow X$, qui à g associe $g \cdot x$, a pour image $G \cdot x$. En outre, on a $\sigma_x(g) = \sigma_x(g') \iff gx = g'x \iff g^{-1}g' \in \mathsf{Stab}_G(x) \iff g' \in g\,\mathsf{Stab}_G(x)$. D'où une bijection de $G/\mathsf{Stab}_G(x)$ vers $G \cdot x$, définie par $g\,\mathsf{Stab}_G(x) \longmapsto gx$. Le cardinal de $G \cdot x$ est donc $[G : \mathsf{Stab}_G(x)]$, d'où la formule annoncée. □

Exemple. Soit G un groupe. On fait opérer G sur lui-même (à gauche) par la formule : $g \cdot x = gxg^{-1}$. (on dit que *G opère par conjuguaison* sur lui-même). L'orbite d'un élément $x \in G$ est appelé la *classe de conjugaison de x*. Le stabilisateur de x est l'ensemble des g vérifiant $gx = xg$; on l'appelle *centralisateur de x*, et on le note $Z(x)$.
On appelle *centre de G* l'ensemble $Z(G) = \{x \in G \mid \forall g \in G, xg = gx\}$. C'est un sous-groupe commutatif distingué de G. Notons qu'on a $x \in Z(G) \iff Z(x) = G$.
Dans ce cadre, la formule des orbites prend la forme suivante.

1.6.2. Proposition. *Soit G un groupe, et S' un système de représentants des classes de conjuguaison. On pose $S = S' \backslash Z(G)$. Alors on a la formule suivante, dite* formule des classes :

$$\mathcal{O}(G) = \mathcal{O}(Z(G)) + \sum_{g \in S} [G : Z(g)] \quad . \square$$

Plus généralement, on peut faire opérer G sur l'ensemble des parties de G par conjugaison : $g \cdot X = gXg^{-1}$ pour $g \in G$ et $X \in \mathcal{P}(X)$. Il est à noter que si H est un sous-groupe de G, $g \cdot H$ est encore un sous-groupe de G. En outre, le stabilisateur de H est exactement le normalisateur de H dans G.

1.7. Théorème de Sylow.

Dans ce paragraphe, p désigne un nombre premier.

Définitions. Un *p-groupe* est un groupe fini dont l'ordre est une puissance de p.
Soit G un groupe fini. Un *p-sous-groupe de G* est un sous-groupe de G qui est un p-groupe. Un *p-sous-groupe de Sylow de G*, ou plus simplement, un *p-Sylow de G*, est un sous-groupe de G dont l'ordre est la plus grande puissance de p qui divise l'ordre de G.

On a le théorème suivant.

1.7.1. Théorème. (Sylow) *Soit G un groupe fini, et p un nombre premier.*
1) Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow.
2) Les p-sous-groupes de Sylow sont conjugués; autrement dit, si P et P' sont deux p-sous-groupes de Sylow, il existe $g \in G$ tel que $P' = gPg^{-1}$.
3) Le nombre de p-sous-groupes de Sylow de G est congru à 1 modulo p.

DEMONSTRATION. On aura besoin des lemmes suivants.

1.7.2. Lemme. *Soit G un groupe abélien d'ordre divisible par p. Alors G contient un sous-groupe d'ordre p.*

DEMONSTRATION. On peut considérer G comme un $\mathbb{Z}$-module. Soit $G(p)$ la composante p-primaire de G, qui est non triviale par hypothèse. Soit x un élément non nul de $G(p)$. Il est d'ordre p^a pour un certain $a > 0$, et $y = p^{a-1}x$ est donc d'ordre p. Le sous-groupe de G engendré par y est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. $\square$

1.7.3. Lemme. *Soit G un p-groupe opérant sur un ensemble fini X. Alors le nombre d'orbites réduites à un point est congru au cardinal de X modulo p.*

DEMONSTRATION. Le cardinal d'une orbite est une puissance de p; le cardinal de X, qui est la somme des cardinaux des orbites, est donc congru modulo p au nombre d'orbites de cardinal 1. $\square$

A présent, revenons au théorème de Sylow. Soit $\mathcal{P}$ l'ensemble des p-Sylow de G.

Commençons par démontrer que $\mathcal{P}$ est non vide. On procède par récurrence sur l'ordre de G, et, l'assertion étant évidente si $\mathcal{O}(G)$ est premier à p, on peut supposer que p divise $\mathcal{O}(G)$.
Si $H \subset G$ est un sous-groupe d'indice premier à p, alors tout p-Sylow de H est un p-Sylow de G, de sorte que si $H \neq G$, on peut conclure par l'hypothèse de récurrence.
On peut donc supposer que G n'admet pas d'autre sous-groupe d'indice premier à p que lui-même. D'après la formule des classes

$$\mathcal{O}(G) = \mathcal{O}(Z(G)) + \sum_{g \in S} [G : Z(g)] \quad ,$$

l'ordre de $Z(G)$ est divisible par p. Par le lemme **1.7.2,** on en déduit l'existence d'un sous-groupe $H \subset Z(G)$ d'ordre p. Le sous-groupe H est distingué dans G, car contenu dans le centre.

Soit $G' = G/H$, et $\pi : G \longrightarrow G'$ le morphisme canonique. Alors G' admet un p-Sylow P'. Posons $P = \pi^{-1}(P')$. On a $\mathcal{O}(P) = \mathcal{O}(H)\mathcal{O}(P') = p\mathcal{O}(P')$, et, puisque $\mathcal{O}(G) = \mathcal{O}(H)\mathcal{O}(G') = p\mathcal{O}(G')$, P est un p-Sylow de G. On a donc $\mathcal{P} \neq \emptyset$.

Le groupe G agit sur $\mathcal{P}$ par conjugaison, autrement dit par $g \cdot P = gPg^{-1}$. Soit H un p-sous-groupe de G, et P un p-Sylow de G. Nous allons montrer qu'il existe $g \in G$ tel que $H \subset g \cdot P$, ce qui entraînera les assertions 1) et 2) du théorème.
Pour cela, soit $\mathcal{P}_0$ l'orbite de P dans $\mathcal{P}$ sous l'action de G. On a $P \subset Stab^G(P)$, donc $\# \mathcal{P}_0 = (G : Stab^G(P))$ est premier à p. Faisons agir H sur $\mathcal{P}_0$ par conjuguaison : $h \cdot P' = hP'h^{-1}$. D'après le lemme **1.7.3,** il y a au moins une orbite réduite à un point. Il existe donc $P' \in \mathcal{P}_0$ tel que $Stab^H(P') = H$, autrement dit, H est contenu dans le normalisateur de P'. Montrons que P' contient H. L'ensemble HP' est un sous-groupe de G, dans lequel P' est distingué. On a $HP'/H \simeq P'/(H \cap P')$ donc HP'/H est un p-groupe, ainsi que HP' lui-même. Comme HP' contient le p-Sylow P', on a $HP' = P'$ et donc $H \subset P'$. On a donc montré les assertions 1) et 2). En particulier, on a $\mathcal{P}_0 = \mathcal{P}$ (assertion 2)).

Montrons l'assertion 3). Soit P un p-Sylow. Soit $P' \in \mathcal{P}$, et supposons que l'orbite de P' sous l'action de P soit réduite à $\{P'\}$. En appliquant le raisonnement précédent à $H = P$, on obtient $P \subset P'$, donc $P = P'$. Ainsi, $\mathcal{P}$ contient une et une seule orbite de cardinal 1 sous P, et $\# \mathcal{P}$ est congru à 1 modulo p par le lemme **1.7.3.** $\square$

2. Corps et extensions

2.1. Rappels sur les corps

Un *corps* est un anneau unitaire non réduit à zéro où tout élément non nul est inversible. Un *sous-corps* d'un corps K est un sous-anneau unitaire K' de K tel que l'inverse de tout élément non nul de K' soit encore dans K'.

Si K et L sont deux corps, un *morphisme de corps de K vers L* est un morphisme d'anneaux de K vers L. Un tel morphisme est toujours injectif, car l'image d'un élément inversible de K est un élément inversible de L.

Soit K un corps. L'intersection d'une famille quelconque de sous-corps de K est encore un sous-corps de K. Pour toute partie $A \subset K$, il existe donc un plus petit sous-corps de K contenant A, qu'on appelle le *sous-corps de K engendré par A*.

Quel est le plus petit sous-corps de K?
Soit ϕ l'unique morphisme d'anneaux unitaires de $\mathbb{Z}$ vers K. Le noyau de ϕ est un idéal de $\mathbb{Z}$; il est donc de la forme $p\mathbb{Z}$, avec $p \in N$. Le nombre p est appelé la *caractéristique de K*, et noté $\mathsf{car}(K)$. Le morphisme ϕ induit un morphisme injectif d'anneaux de $\mathbb{Z}/p\mathbb{Z}$ vers K; comme K est intègre, $\mathbb{Z}/p\mathbb{Z}$ l'est aussi, et donc p est soit premier, soit nul. Dans le premier cas, l'image de ϕ est le plus petit sous-corps de K; ce sous-corps est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Dans le second cas, on peut identifier $\mathbb{Z}$ à son image par ϕ dans K. Le plus petit sous-corps de K s'identifie alors à $\mathbb{Q}$.

2.2. Extensions

Définition. Soit K un corps commutatif. Une *extension de K* est la donnée d'un corps commutatif L et d'un morphisme de corps $j : K \longrightarrow L$.

EXEMPLE. Si L est un corps commutatif et K un sous-corps de L, l'inclusion de K dans L est une extension de K qu'on notera $(L : K)$. Toute extension est essentiellement de ce type.

Définition. Soit K un corps commutatif, et soit $j : K \longrightarrow L$ et $j' : K \longrightarrow L'$ deux extensions de K. Un *morphisme d'extensions de $j : K \longrightarrow L$ vers $j' : K \longrightarrow L'$* est un morphisme de corps $\sigma : L \longrightarrow L'$ vérifiant : $\sigma \circ j = j'$. Si en outre σ est surjectif (donc bijectif) on dit que c'est un *isomorphisme d'extensions*. Un isomorphisme d'extensions de $j : K \longrightarrow L$ dans elle-même est appelé un *automorphisme de $j : K \longrightarrow L$*.

2.2.1. Proposition. *Soit K un corps commutatif et $j : K \longrightarrow L$ une extension de K. Alors il existe un corps commutatif L_0 contenant K comme sous-corps, de sorte que l'extension $j : K \longrightarrow L$ soit isomorphe à l'extension $(L_0 : K)$.*

DEMONSTRATION. On peut trouver un ensemble X, disjoint de K, et de même cardinal que $\Lambda = L \backslash j(K)$. Posons $L_0 = K \cup X$. Il existe une bijection σ_0 de X sur Λ, qu'on prolonge en une bijection σ de L_0 sur L de sorte que σ coïncide avec j sur K. On définit une addition et une multiplication dans L_0 de sorte que σ soit un isomorphisme. Pour ces lois de composition, L_0 est un corps, et l'inclusion de K dans L_0 est un morphisme de corps, donc K est un sous-corps de L_0. En outre, σ est un isomorphisme d'extensions de $(L_0 : K)$ vers $j : K \longrightarrow L$. $\square$

REMARQUE IMPORTANTE
Chaque fois qu'on aura à travailler sur une extension $K \longrightarrow L$, on pourra toujours supposer que K est un sous-corps de L, quitte à remplacer l'extension considérée par une extension qui lui est isomorphe. On formulera donc souvent des résultats ou des définitions pour des extensions de la forme $(L : K)$, où K est un sous-corps de L, pour les appliquer ensuite à des extensions quelconques.
Il faut absolument prendre garde au fait suivant. Quand il existe un morphisme de corps $K \longrightarrow L$, il en existe en général plusieurs.
Cependant, lorsqu'on parlera d'une extension $K \longrightarrow L$, et que le contexte exclura toute ambigüité quant au morphisme de K dans L considéré, on notera souvent $(L : K)$ une telle extension, le morphisme étant implicite.

Définition. Soit K un corps commutatif, et $(L : K)$ une extension de K. Les automorphismes de l'extension $(L : K)$ constituent (pour la composition des applications) un groupe qu'on appelle le *groupe de Galois* de l'extension $(L : K)$, et qu'on note $\mathsf{Gal}(L : K)$.

Le groupe de Galois d'une extension est l'objet central de la théorie de Galois. Le but de cette dernière est d'établir un dictionnaire permettant de traduire les propriétés d'une extension $(L : K)$ en termes de propriétés de son groupe de Galois (et réciproquement). Cependant le dictionnaire en question n'est valable que pour des extensions d'un type bien particulier : les extensions galoisiennes. Il nous reste donc à introduire quelques notions sur les extensions avant de pouvoir formuler le théorème principal.

Étant donnée une extension $j : K \longrightarrow L$, la multiplication externe $K \times L \longrightarrow L$, $(x, y) \longmapsto j(x)y$, fait de L un K-espace vectoriel.

Définitions. Soit K un corps commutatif, et $(L : K)$ une extension de K. La dimension de L en tant que K-espace vectoriel est appelée *degré de l'extension*. Le degré de l'extension $(L : K)$ est noté $[L : K]$. Une extension est dite *finie* quand elle est de degré fini.

2.2.2. Proposition. *Soit $K \subset E \subset L$ trois corps commutatifs emboîtés. Alors on a :*

$$[L : K] = [L : E][E : K] \quad .$$

DEMONSTRATION. Soit $(x_i)_{i \in I}$ une base de E comme K-espace vectoriel, et $(y_j)_{j \in J}$ une base de L en tant que E-espace vectoriel, de sorte que $[E : K] = \# I$ et $[L : E] = \# J$. Alors les $x_i y_j$ constituent, pour (i, j) décrivant $I \times J$, une base de L sur K. On a donc bien $[L : K] = \mathsf{dim}_K\, L = \# I \,\# J = [E : K][L : E]$. □

Définitions. Soit K un corps commutatif, $(L : K)$ une extension de K, et A une partie de L. Alors on note $K[A]$ (resp. $K(A)$) le plus petit sous-anneau (resp. sous-corps) de L contenant K et A. On dit que *l'extension* $(L : K)$ *est engendrée par* A, ou que L est engendré par A sur K, lorsque $L = K(A)$. L'extension $(L : K)$ est dite *de type fini* si elle est engendrée par une partie finie.

2.3. Eléments algébriques et transcendants

Soit K un corps commutatif, et $(L : K)$ une extension de K. Soit x un élément de L. Si P est un polynôme à coefficients dans K, posons $ev_x(P) = P(x)$; cela définit un morphisme d'anneaux $ev_x : K[X] \longrightarrow L$, le *morphisme d'évaluation en* x, dont l'image est $K[x]$.
On dit que x est une *racine de* P *(dans* L*)* si $P(x) = 0$.
L'anneau $A = K[X]$ est principal. Soit $I = \mathsf{Ker}(ev_x)$; ev_x induit un morphisme injectif de A/I dans L, donc A/I est intègre; autrement dit, I est un idéal premier. On doit donc distinguer deux cas.
1) Si I est nul, il n'est pas maximal; ev_x est injectif, et $K[x]$ n'est pas un corps.
2) Si I est non nul, il est maximal. Alors $K[x]$ est un corps. En outre, I est engendré par un polynôme unitaire P, de degré d. Soit $K[X]_d$ le K-espace vectoriel des polynômes de degré $< d$. On a alors

$$K[X] = K[X]_d \oplus I$$

(c'est la division euclidienne par P), donc $K[x] \simeq A/I$ est de dimension d sur K. Tous ces faits sont résumés dans la proposition suivante.

2.3.1. Proposition. *Les conditions suivantes sont équivalentes :*

(i) le morphisme ev_x *n'est pas injectif; autrement dit, il existe un polynôme non nul* P *à coefficients dans* K *tel que* x *soit une racine de* P*;*

(ii) la dimension de $K[x]$ *sur* K *est finie;*

(iii) le corps $K(x)$ *est égal à* $K[x]$. $\square$

Définitions. Si l'une de ces trois conditions est vérifiée, l'élément x est dit *algébrique sur* K. Le générateur unitaire du noyau de ev_x est alors appelé *polynôme minimal de* x *sur* K et noté $P_{x,K}$; c'est un polynôme irréductible sur K. Le degré de ce polynôme, qui est aussi le degré de l'extension $(K(x) : K)$, est appelé *degré de* x *sur* K. Dans le cas contraire, on dit que l'élément x est *transcendant sur* K. Le corps $K(x)$ est alors isomorphe au corps des fractions rationnelles $K(X)$.
L'extension $(L : K)$ est dite *algébrique* si tous les éléments de L sont algébriques sur K. Une extension finie est algébrique, en vertu du point (ii) de la proposition **2.3.1.** Une extension de la forme $K(x)$ est finie si et seulement si x est algébrique sur K. Il en résulte par **2.2.2.** qu'une extension algébrique de type fini est finie.

2.3.2. Proposition. *Soit* K *un corps commutatif et* $(L : K)$ *une extension de* K*. Soit* E *l'ensemble des éléments de* L *qui sont algébriques sur* K*. Alors* E *est un sous-corps de* L *qui contient* K*.*

Demonstration. L'ensemble E est non vide car il contient K. Soit $x,\ y \in E$. Soit $F = K(x, y) = K(x)(y)$. Comme x est algébrique sur K, l'extension $(K(x) : K)$ est finie. De même, y est algébrique sur K, et a fortiori sur $K(x)$, donc l'extension $(K(x, y) : K(x))$ est elle aussi finie. On a $[K(x, y) : K] = [K(x, y) : K(x)][K(x) : K]$ donc l'extension $[K(x, y) : K]$ est finie. On a donc $K(x, y) \subset E$. En particulier, $x - y \in E$ et pour $y \neq 0$, $xy^{-1} \in E$, donc E est un sous-corps de L. $\square$

Comme on l'a vu, un polynôme minimal est toujours irréductible. Inversement, étant donné un polynôme P, irréductible, unitaire, à coefficients dans K, on peut construire le corps

$$K_P = K[X]/(P) \quad .$$

Le morphisme canonique $K[X] \longrightarrow K_P$ induit un morphisme de corps $j : K \longrightarrow K_P$; on considère donc K_P comme une extension de K. Soit $x_P \in K_P$ l'image de X par le morphisme canonique; c'est une racine de P dans K_P, et $K_P = K(x_P)$. On a donc construit une extension de K où P admet une racine x_P. Cette construction est universelle au sens suivant.

2.3.3. Proposition. *Soit K un corps commutatif, et P un polynome irréductible à coefficients dans K. Soit K_P l'extension de K, et x_P la racine de P définies ci-dessus. Alors pour toute extension $(L : K)$, et toute racine x de P dans L, il existe un morphisme d'extensions unique de $(K_P : K)$ vers $(L : K)$ qui envoie x_P sur x.*

DEMONSTRATION. Le morphisme d'évaluation $K[X] \longrightarrow L$ qui envoie X sur x s'annule en P, donc définit par passage au quotient l'unique morphisme d'extensions de K_P vers L qui envoie x_P sur x. □

Cependant, l'extension K_P présente un grave défaut que nous allons bientôt mettre en évidence...

2.4. Corps de décomposition et extensions normales.

Soit K un corps commutatif, et Q un polynôme unitaire de degré d à coefficients dans K. Soit $(L : K)$ une extension de K. On dit que Q est *scindé dans* $(L : K)$, ou plus simplement *scindé dans* L, si Q est un produit de polynômes de degré 1 dans $L[X]$; autrement dit, s'il existe $x_1, x_2, \ldots, x_d$ dans L tels que

$$Q(X) = (X - x_1)(X - x_2)\ldots(X - x_d) \quad .$$

Les x_i sont alors les racines de Q dans L.

Définition. Une extension $(L : K)$ est un *corps de décomposition de Q sur K* si les deux conditions suivantes sont remplies :

— le polynôme Q est scindé dans L;

— les racines de Q dans L engendrent L sur K, autrement dit $L = K(x_1, x_2, \ldots, x_d)$.

2.4.1. Théorème. *Tout polynôme unitaire à coefficients dans un corps commutatif K admet un corps de décomposition sur K.*

DEMONSTRATION. Soit $Q \in K[X]$ de degré $d > 0$. On procède par récurrence sur d; si $d = 1$, K convient. Si $d > 1$, soit P un facteur irréductible de Q. On a vu ci-dessus qu'il existe une extension de K de la forme $K(x)$, avec $P(x) = 0$. Le polynôme Q admet la racine x dans $K(x)$, donc il s'écrit $Q = (X - x)R$ dans $K(x)[X]$, avec $\mathsf{deg}(R) < d$. Soit $(L : K(x))$ un corps de décomposition de R sur $K(x)$, dont l'existence est assurée par l'hypothèse de récurrence. Alors, R est scindé dans L, et Q aussi. Les racines de Q dans L sont celles de P, et x. Or, les racines de P engendrent L sur $K(x)$, donc les racines de Q engendrent L sur K, et $(L : K)$ est un corps de décomposition de Q sur K. □

REMARQUE. Si $(L : K)$ est un corps de décomposition de P sur K, et si E est un corps intermédiaire entre K et L, alors $(L : E)$ est un corps de décomposition de P sur E.

2.4.2. Théorème. *Soit K un corps commutatif, Q un polynôme unitaire à coefficients dans K, $(L:K)$ une extension engendrée par des racines de Q, et $(L':K)$ une extension où Q est scindé. Alors il existe un morphisme d'extensions (non nécéssairement unique!) de $(L:K)$ vers $(L':K)$.*

Demonstration. On procède par récurrence sur $d = [L:K]$. Si $d = 1$, $L = K$ et l'inclusion de K dans L' convient.
Plaçons-nous dans le cas $d > 1$. Alors, il existe une racine x de Q dans L de degré $\delta > 1$ sur K. Soit P le polynôme minimal de x sur K. Alors P est scindé dans L' car il divise Q. Soit y une racine de P dans L'. Soit $K' = K(x)$. D'après la proposition **2.3.3,** il existe un (unique) morphisme d'extensions σ_0 de $(K':K)$ vers $(L':K)$ envoyant x sur y.
D'après la proposition **2.2.1,** on peut, quitte à remplacer l'extension $\sigma_0 : K' \longrightarrow L'$ par une extension isomorphe, supposer que K' est un sous-corps de L' et que σ_0 est l'inclusion. L'extension $(L:K')$ est engendrée par les racines de Q, et Q est scindé dans L'. On a $[L:K'] = d/\delta < d$, donc l'hypothèse de récurrence peut s'appliquer à cette situation. On en déduit l'existence d'un morphisme d'extensions de $(L:K')$ vers $(L':K')$, qui est a fortiori un morphisme d'extensions de $(L:K)$ vers $(L':K)$. □

Remarque. Ce résultat sera bientôt précisé (*cf.* **2.6.3.**)

2.4.3. Corollaire. *Soit Q un polynôme unitaire à coefficients dans un corps commutatif K. Alors le corps de décomposition de Q sur K est unique à isomorphisme d'extensions près.*

Demonstration. Soit $j : K \longrightarrow L$ et $j' : K \longrightarrow L'$ deux corps de décomposition de Q sur K; d'après le théorème **2.4.2,** il existe un morphisme d'extensions σ de $j : K \longrightarrow L$ vers $j' : K \longrightarrow L'$. Soit $x_1, \dots, x_d$ les racines de Q dans L, de sorte que Q s'écrit $(X - x_1)\dots(X - x_d)$ dans $L[X]$. Alors on a $Q = (X - \sigma(x_1))\dots(X - \sigma(x_d))$ dans $L'[X]$, donc les racines de Q dans L', qui engendrent L' sur K, sont les images des racines de Q dans L. Ainsi σ est surjectif; c'est donc un isomorphisme. □

Définition. Soit K un corps commutatif. Une extension algébrique $(L:K)$ est dite *normale* si tout polynôme irréductible dans $K[X]$ qui admet une racine dans L est scindé dans L.

2.4.4. Théorème. *Soit K un corps commutatif et $(L:K)$ une extension. Les deux conditions suivantes sont équivalentes.*

(i) $(L:K)$ est normale et finie;

(ii) $(L:K)$ est le corps de décomposition d'un polynôme unitaire à coefficients dans K.

Demonstration.
(i) $\Longrightarrow$ (ii). Soit $(L:K)$ une extension normale finie. Soient $x_1, x_2, \dots, x_n$ des éléments de L tels que $L = K(x_1, x_2, \dots, x_n)$ (par exemple, on peut prendre les éléments d'une base de L sur K), et soit P_i le polynôme minimal de x_i sur K pour $i = 1, 2, \dots, n$. Soit $Q = P_1 P_2 \dots P_n$. Alors Q est scindé dans L car chacun des P_i y a une racine. Comme L est engendré sur K par les x_i, qui sont des racines de Q, L est un corps de décomposition de Q sur K.

(ii) $\Longrightarrow$ (i). Soit Q un polynôme unitaire dans $K[X]$ et $(L:K)$ son corps de décomposition. C'est une extension algébrique de type fini, donc finie. Reste à montrer qu'elle est normale. Soit P un polynôme irréductible unitaire dans $K[X]$ et supposons que P admet une racine x_1 dans L. Soit $(L':L)$ un corps de décomposition de P sur L, et x_2 une racine de P dans L'. Il s'agit de montrer que $x_2 \in L$. Comme on a $L = L(x_1)$, il suffit de vérifier : $[L(x_1):K] = [L(x_2):K]$
Or, $(L(x_i):K(x_i))$ est un corps de décomposition de Q sur $K(x_i)$ pour $i = 1,\ 2$. Il y a un isomorphisme σ unique de $(K(x_1):K)$ sur $(K(x_2):K)$, qui envoie x_1 sur x_2 (proposition 2.3.3.). Notons j_i l'inclusion de $K(x_i)$ dans $L(x_i)$; alors $j_1 : K(x_1) \longrightarrow L(x_1)$ et $j_2\sigma : K(x_1) \longrightarrow L(x_2)$ sont deux corps de décomposition de Q sur $K(x_1)$; ils sont isomorphes, et en particulier, $[L(x_1):K] = [L(x_2):K]$. □

Remarque. Si $(L:K)$ est une extension normale finie, et si E est un corps intermédiaire entre K et L, alors $(L:E)$ est encore une extension normale (pourquoi?), mais en général, $(E:K)$ n'en est pas une; nous l'allons voir à l'instant.

Exemple. Soit $K = \mathbb{Q}$. Soit Q le polynôme $X^3 - 2$ dans $\mathbb{Q}[X]$. Il est irréductible, et admet dans $\mathbb{R}$ la racine $\sqrt[3]{2}$. Le corps $\mathbb{Q}[\sqrt[3]{2}]$ est une extension de degré 3 de $\mathbb{Q}$ qui n'est pas normale, car Q admet dans $\mathbb{C}$ deux autres racines, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$, qui ne sont pas réelles. Le corps de décomposition de Q sur $\mathbb{Q}$ est $\mathbb{Q}[\sqrt[3]{2}, j]$, qui est de degré 6 sur $\mathbb{Q}$.
On voit sur cet exemple que les extensions finies de la forme $(K(x):K)$ ne sont en général pas normales. Cependant toute extension finie se plonge dans une extension normale.

2.5. Clôture normale

Définition. Soit K un corps commutatif, et $(E:K)$ une extension finie de K. Une *clôture normale de* $(E:K)$ est une extension $(L:E)$ vérifiant
(i) l'extension $(L:K)$ est normale;
(ii) l'extension $(L:E)$ est minimale pour la propriété (i).

2.5.1. Proposition. *Toute extension finie $(E:K)$ admet une clôture normale, qui est unique à isomorphisme près.*

Demonstration. Soit $x_1, \dots x_n$ une base de E sur K. Soit P_i le polynôme minimal de x_i sur K, et $Q = P_1P_2\dots P_n$.
Soit $(L:E)$ une extension de E. Supposons l'extension $(L:K)$ normale. Le sous-corps L' de L engendré sur K par les racines de Q est une extension normale de K qui contient E, et qui est minimale pour cette propriété.
Ainsi, $(L:E)$ est une clôture normale de $(E:K) \iff L = L' \iff (L:E)$ est un corps de décomposition de Q sur E.
D'où l'existence d'une clôture normale, et son unicité à isomorphisme près. □

2.6. Extensions séparables

Définitions. Soit K un corps commutatif, et P un polynôme irréductible dans $K[X]$. On dit que P est *séparable (sur K)* s'il n'admet pas de racines multiples dans son corps de décomposition. Dans le cas contraire, on dit que P est *inséparable (sur K).*

2.6.1. Proposition. *Soit P un polynôme irréductible dans $K[X]$. Si $\mathsf{car}(K)=0$, P est toujours séparable. Si par contre $\mathsf{car}(K)$ est un premier p, alors P est inséparable si et seulement si $P\in K[X^p]$.*

DEMONSTRATION. Tout d'abord, un lemme.

2.6.2. Lemme. *Soit $P\in K[X]$. Les deux conditions suivantes sont équivalentes.*
(i) P et $\frac{d}{dX}P$ sont premiers entre eux dans $K[X]$;
(ii) P n'admet pas de racine multiple dans son corps de décomposition.

DEMONSTRATION. Soit P et Q deux éléments de $K[X]$ et $(L:K)$ une extension de K. Alors la division euclidienne de Q par P est la même dans $K[X]$ et dans $L[X]$; en particulier, le reste est le même. Ainsi, l'algorithme d'Euclide appliqué à la recherche du pgcd de P et de Q donne le même résultat dans $K[X]$ et dans $L[X]$. Il résulte de ces remarques que P et Q sont premiers entre eux dans $K[X]$ si et seulement s'ils le sont dans $L[X]$.
La condition (i) équivaut donc à : P et $\frac{d}{dX}P$ sont premiers entre eux dans $L[X]$. Lorsque L est le corps de décomposition de P, cette condition équivaut à dire que P (qui est scindé dans L) n'admet pas de racines multiples dans L. □

Soit P un polynôme irréductible inséparable. Alors P n'est pas premier à $\frac{d}{dX}P$; or, on a $\mathsf{deg}(\frac{d}{dX}P)<\mathsf{deg}(P)$; il faut donc $\frac{d}{dX}P=0$. Si $P=\sum_{i=0}^{n}a_nX^n$, alors $\frac{d}{dX}P=\sum_{i=1}^{n}na_{n-1}X^n$ n'est nul que si P est constant (ce qui est exclu), ou si la caractéristique est un premier p, et que le coefficient a_n est nul pour n non congru à zéro modulo p, ce qui revient à dire $P\in K[X^p]$. Dans ce dernier cas, P est effectivement inséparable. □

Définitions. Soit K un corps commutatif, et $(L:K)$ une extension algébrique de K. Un élément x de L est dit *séparable sur K* si son polynôme minimal $P_{x,K}$ est séparable sur K (autrement dit, si $\frac{d}{dX}P_{x,K}\neq 0$). L'extension $(L:K)$ est *séparable* si tous les éléments de L sont séparables sur K. C'est toujours le cas si $\mathsf{car}(K)=0$.

2.6.3. Proposition. *Soit $(E:K)$ une extension finie de degré d et $(L:K)$ une extension quelconque.*
Notons δ le nombre de morphismes d'extensions de $(E:K)$ vers $(L:K)$. Alors
1) $\delta\leq d$;
2) Soient $(x_1,\dots x_r)$ des générateurs de E sur K. Si $(L:K)$ est (algébrique) normale et s'il existe au moins un morphisme de (E,K) dans $(L:K)$, les conditions suivantes sont équivalentes :
(i) $\delta=d$;
(ii) chacun des x_i est séparable sur K;
(iii) l'extension $(E:K)$ est séparable.

DEMONSTRATION.
1) Sur le modèle de la démonstration de **2.4.2,** on procède par récurrence sur d, le cas $d=1$ étant évident. Soit donc $d>1$. On peut trouver un corps E_0, intermédiaire entre K et E, de sorte que E soit de la forme $E_0(x)$ et que $(E_0:K)<d$. Par hypothèse de récurrence, le nombre des morphismes d'extensions de $(E_0:K)$ dans $(L:K)$ est au plus $[E_0:K]$. Soit σ_0 l'un d'entre eux et voyons L comme une extension de E_0 via σ_0. Se

donner un morphisme $\sigma : E_0(x) \to L$ qui prolonge σ_0 équivaut à se donner dans L une racine de l'image de P_{x,E_0}.
Puisque $\mathsf{deg}(P_{x,E_0}) = [E : E_0]$, il y a donc au plus $[E : E_0]$ manières d'étendre σ_0 à L. En fin de compte, il a au plus $[E : E_0][E_0 : K] = [E : K]$ morphismes d'extensions de $(E : K)$ vers $(L : K)$.
Revoyons maintenant plus en détail ce raisonnement sous les hypothèses de 2).
Soit $E_i = K[x_1, \ldots, x_i]$, de sorte que $K = E_0 \subset E_1 \subset \cdots \subset E_r = E$ et $E_i = E_{i-1}[x]$. Soit P_i le polynôme minimal de x_i sur E_{i-1}.
Donnons-nous un morphisme σ_0 de (E_{i-1}, K) dans $(L : K)$. Le nombre de prolongements de σ_0 à E_i est exactement le nombre de racines de P_i dans L.
On a donc $d = \delta$ si et seulement si, pour tout i et pour tout σ_0, le nombre de racines de P_i dans L est égal à son degré, autrement dit P_i est séparable et scindé dans L.
Or P_i est nécessairement scindé dans L; en effet il divise $P_{x_i,K}$ qui est scindé dans L car $(L : K)$ est normale et $(E : K)$ s'y plonge.
Si pour tout i, $P_{x_i,K}$ est séparable, P_i est séparable donc on a bien $d = \delta$. Ainsi, (ii) $\Longrightarrow$ (i).
Supposons $d = \delta$. Alors $P_1 = P_{x_1,K}$ est séparable, donc x_1 est séparable sur K; mais tout élément de E peut jouer le rôle de x_1, donc $(E : K)$ est séparable. D'où (i) $\Longrightarrow$ (iii).
Enfin, (iii) $\Longrightarrow$ (ii) est évident. □

2.6.4. Corollaire. *Une extension finie $(E : K)$ est séparable si et seulement si elle est engendrée par des éléments séparables.*

DEMONSTRATION. Soit $(L : K)$ une extension normale où $(E : K)$ se plonge (par exemple, sa clôture normale). L'assertion 2) de la proposition s'applique donc. Par (ii) $\Longrightarrow$ (i), il y a exactement $[E : K]$ plongements de $(E : K)$ dans $(L : K)$. Par (i) $\Longrightarrow$ (iii), $(E : K)$ est séparable. □

3. Théorème de Galois

3.1. Énoncé du théorème de Galois

Soit K un corps commutatif, et $(L : K)$ une extension de K. Soit $\mathsf{Gal}(L : K)$ le groupe de Galois de cette extension.
On considère

$\mathcal{G}$ l'ensemble des sous-groupes de $\mathsf{Gal}(L : K)$

$\mathcal{K}$ l'ensemble des corps intermédiaires entre K et L.

Pour tout sous-groupe H de $\mathsf{Gal}(L : K)$, on peut former l'ensemble

$$L^H = \{x \in L \mid \forall h \in H, h(x) = x\} \quad .$$

C'est un sous-corps de L qui contient K.
De même, si E est un corps intermédiaire entre K et L, on peut former le sous-groupe de G

$$G_E = \{g \in G \mid \forall x \in E, g(x) = x\} \quad .$$

qui n'est autre que $\mathsf{Gal}(L : E)$.
D'où deux applications décroissantes $\dagger : \mathcal{G} \longrightarrow \mathcal{K}$ et $\star : \mathcal{K} \longrightarrow \mathcal{G}$ définies respectivement par $H \longmapsto H^\dagger = L^H$ et $E \longmapsto E^\star = G_E$.
On se propose de comparer $\mathcal{G}$ et $\mathcal{K}$ au moyen de ces deux applications.
Il est clair qu'on a $E \subset (E^\star)^\dagger$ pour tout $E \in \mathcal{K}$ et $H \subset (H^\dagger)^\star$ pour tout $H \in \mathcal{G}$.

Pour pouvoir en dire plus, nous aurons besoin de la notion suivante.

Définition. Une extension $(L : K)$ est dite *galoisienne* si elle est à la fois normale et séparable.

Remarques. En fait, nous nous intéresserons aux extensions galoisiennes finies. Une extension $(L : K)$ est galoisienne finie si et seulement si c'est le corps de décomposition sur K d'un polynôme P dans $K[X]$ tel que P et $\frac{d}{dX}P$ soient premiers entre eux. (La partie "si" utilise la proposition 2.5.3.)
Si $(L : K)$ est une extension galoisienne finie, et si E est un corps intermédiaire, l'extension $(L : E)$ est encore galoisienne; par contre, l'extension $(E : K)$ est séparable, mais en général elle n'est pas normale.

3.1.1. Théorème. (Galois) *Soit $(L : K)$ une extension galoisienne finie. Alors*
(1) le groupe de Galois $G = \mathsf{Gal}(L : K)$ est d'ordre $[L : K]$;
(2) les applications $\dagger : \mathcal{G} \longrightarrow \mathcal{K}$ et $\star : \mathcal{K} \longrightarrow \mathcal{G}$ définies ci-dessus sont inverses l'une de l'autre;
(3) si E est un corps intermédiaire entre K et L, alors on a $[L : E] = \mathcal{O}(E^\star)$ et $[E : K] = [G : E^\star]$;
(4) en outre, $(E : K)$ est une extension normale si et seulement si $E^\star$ est distingué dans G;
(5) si tel est le cas, on a un isomorphisme $\mathsf{Gal}(E : K) \simeq G/E^\star$.

La démonstration de ce théorème va se dérouler en plusieurs étapes.

3.2. Comparaison entre l'ordre des groupes et le degré des extensions

C'est l'essentiel du travail. Nous en avons déjà fait la moitié :

3.2.1. Proposition. *L'ordre du groupe de Galois d'une extension finie est au plus égal au degré de cette extension, avec égalité lorsque l'extension est galoisienne finie.*

DEMONSTRATION. C'est un cas particulier de **2.6.3.** Soit $(E:K)$ une extension finie de degré d. Son groupe de Galois coïncide avec l'ensemble des morphismes d'extensions de $(E:K)$ dans $(E:K)$. Notant δ son ordre, on a $\delta \leq d$. Par ailleurs $\delta \geq 1$. Si $(E:K)$ est normale et séparable, on a $\delta = d$. □

3.2.2. Corollaire. *Les assertions (1) et (3) du théorème de Galois sont vraies.*

DEMONSTRATION. La proposition contient l'assertion (1). Si $E \in \mathcal{K}$, $(L:E)$ est normale et séparable donc galoisienne. Puisque tout automorphisme de L fixant les éléments de E fixe aussi ceux de K, $\mathsf{Gal}(L:E)$ n'est autre que $E^\star$. L'assertion (1) donne ici $[L:E] = \mathcal{O}(E^\star)$. Puisque $[L:E][E:K] = [L:K]$ et $\mathcal{O}(E^\star)[G:E^\star] = \mathcal{O}(G)$, on a $[E:K] = [G:E^\star]$. □

Reste l'autre moitié, qui, on le verra, repose sur des idées différentes.

3.2.3. Théorème. *Soit L un corps commutatif, et G un sous-groupe fini du groupe $\mathsf{Aut}(L)$ des automorphismes de L. Soit $K = L^G$. Alors l'extension $(L:K)$ est galoisienne, de degré $\mathcal{O}(G)$.*

DEMONSTRATION.
Commençons par la partie facile : $(L:K)$ est galoisienne. En effet, soit x un élément de L; il s'agit de vérifier que $P_{x,K}$ est séparable et scindé dans K. Soient $x_1, \dots x_n$ les points distincts de l'orbite de x sous l'action de G; ce sont des racines de $P_{x,K}$. Soit $P = (X - x_1)\dots(X - x_n)$; c'est un polynôme unitaire à coefficients dans L, et invariant sous l'action de G, donc à coefficients dans K; il est séparable et scindé dans L; d'autre part P s'annule en x et divise $P_{x,K}$, donc $P = P_{x,K}$.

A présent, la partie difficile, qui relève de l'algèbre linéaire. Soit $[L:K] = m$ et $\mathcal{O}(G) = n$.

1) Montrons $m \geq n$. On utilise le lemme suivant.

3.2.4. Lemme. (Dedekind) *Soient K et L deux corps commutatifs. Les morphismes de corps $K \xrightarrow{\sigma} L$ constituent une famille libre dans le L-espace vectoriel des applications de K dans L.*

DEMONSTRATION. Soit une relation de liaison sur L

$$\sum_{i=1}^{n} x_i \sigma_i = 0\,,$$

où les x_i sont dans L et les σ_i sont des morphismes de corps distincts de K dans L. On suppose n minimal. Toutes les relations de liaison sur L entre les σ_i sont donc proportionnelles à celle-ci.

On a $\forall x \in K, \quad \sum_{i=1}^n x_i\sigma_i(x) = 0$. Pour $y \in K$ non nul, on a $\sum_{i=1}^n x_i\sigma_i(yx) = 0$ donc $\sum_{i=1}^n x_i\sigma_i(y)\sigma_i(x) = 0$. Autrement dit, on a : $\sum_{i=1}^n x_i\sigma_i(y)\sigma_i = 0$. Cette relation de liaison entre les σ_i est proportionnelle à $\sum_{i=1}^n x_i\sigma_i = 0$, donc $\sigma_1(y) = \sigma_2(y) = \ldots \sigma_n(y)$, et les σ_i sont tous égaux. On a donc $n = 1$, ce qui est absurde, car un morphisme de corps n'est jamais nul. □

Soit $(x_1, \ldots, x_m)$ une base de L sur K. D'après le lemme de Dedekind, les vecteurs $(g(x_1), \ldots, g(x_m)) \in L^m$ sont indépendants (sur L) pour $g \in G$, donc l'ordre de G est au plus m.

2) Montrons $m \leq n$. On suppose le contraire : $m > n$. Soit $x_1, x_2, \ldots, x_{n+1} \in L$ linéairement indépendants sur K. La matrice $(g(x_i))_{g\in G, 1\leq i\leq n+1}$ comporte n lignes et $n+1$ colonnes; ces dernières sont donc liées sur L. Il existe donc $y_1, \cdots y_{n+1} \in L$ tels qu'on ait

$$\forall g \in G, \qquad \sum_{i=1}^{n+1} g(x_i)y_i = 0 \quad .$$

On peut réordonner les indices de sorte que les y_i non nuls soient les r premiers; on a donc une relation de la forme :

$$\forall g \in G, \qquad g(x_1)y_1 + \cdots + g(x_r)y_r = 0 \quad .$$

où les y_i sont non nuls. On suppose r minimal.
Soit $\gamma \in G$; on a alors

$$\gamma(g(x_1)y_1) + \cdots + \gamma(g(x_r)y_r) = 0\,,$$

d'où

$$(\gamma g)(x_1)\gamma(y_1) + \cdots + (\gamma g)(x_r)\gamma(y_r) = 0\,.$$

Or, quand g décrit G, γg décrit aussi G. On a donc

$$\forall g \in G, \qquad g(x_1)\gamma(y_1) + \cdots + g(x_r)\gamma(y_r) = 0 \quad .$$

Comme on a choisi r minimal, on a $\gamma(y_1)/y_1 = \cdots = \gamma(y_r)/y_r$. Cela se traduit par : $\gamma(y_i/y_1) = y_i/y_1$ pour tout $\gamma \in G$, donc $z_i = y_i/y_1 \in K$.
Divisons la relation $g(x_1)y_1 + \cdots + g(x_r)y_r = 0$ par y_1 et posons $g = 1_L$. Il vient $x_1z_1 + \cdots + x_rz_r = 0$, et les x_i sont liés sur K, ce qui contredit leur choix. □

3.2.5. Corollaire. *L'assertion (2) du théorème de Galois est vraie.*

Demonstration. Soit $(L : K)$ une extension galoisienne finie de degré n, et G son groupe de Galois. Alors $L^G = K$. En effet G est un sous-groupe de $\mathsf{Aut}(L)$ d'ordre n. Soit $K_0 = L^G$; on a $K \subset K_0 \subset L$ et $[L : K_0] = n = [L : K]$ (par 3.2.3), donc $K = K_0$.
Soit maintenant E un corps intermédiaire. Appliquant ce qui précède à l'extension $(L : E)$, qui est galoisienne finie de groupe de Galois $E^\star$, on a donc $E^{\star\dagger} = E$.
Soit à présent H un sous-groupe de G, et notons $H_0 = H^{\dagger\star}$. On a par construction $H \subset H_0$. D'autre part, $H_0{}^\dagger = H^{\dagger\star\dagger} = H^\dagger$ d'après ce qu'on vient de voir. Par (3.2.3), $\mathcal{O}(H) = [L : H^\dagger]$ et $[L : H^\dagger] = [L : H_0{}^\dagger] = \mathcal{O}(H_0)$ (toujours par 3.2.3). On a donc $\mathcal{O}(H) = \mathcal{O}(H_0)$, et puisque $H \subset H_0$, $H = H_0$. □

3.3. Fin de la démonstration du théorème de Galois

Soit $(L : K)$ une extension. Le groupe de galois $G = \mathsf{Gal}(L : K)$ opère à gauche sur l'ensemble $\mathcal{K}$ des corps intermédiaires par $\sigma \cdot E = \sigma(E)$.
Un corps intermédiaire E est dit *invariant par* G si pour tout σ dans G, $\sigma(E) = E$.
Or, pour $E \in \mathcal{K}$ et $\sigma \in \mathsf{Gal}(L : K)$, on a

$$\sigma(E)^{\star} = \sigma E^{\star} \sigma^{-1} \quad .$$

En effet, soit $g \in G$. Alors on a : $g \in \sigma(E)^{\star} \iff \forall x \in E, g\sigma(x) = \sigma(x) \iff \forall x \in E, \sigma^{-1} g \sigma(x) = x \iff \sigma^{-1} g \sigma \in E^{\star}$.
On voit donc que $E^{\star}$ est distingué dans G si et seulement si E est invariant par $\mathsf{Gal}(L : K)$.
L'assertion (4) du théorème de Galois résulte donc de la proposition suivante.

3.3.1. Proposition. *Soit $(L : K)$ une extension normale finie, de groupe de Galois G, et E un corps intermédiaire entre K et L. Alors l'extension $(E : K)$ est normale si et seulement si E est invariant par G.*

Demonstration. Supposons l'extension $(E : K)$ normale. C'est le corps de décomposition sur K d'un polynôme unitaire $Q \in K[X]$. Ainsi, E est engendré sur K par les racines de Q dans L. Un automorphisme $\sigma \in \mathsf{Gal}(L : K)$ permute les racines de Q dans L, et donc envoie E sur lui-même.
Pour montrer la réciproque, nous aurons besoin du lemme suivant.

3.3.2. Lemme. *Soient $(L : K)$ une extension normale finie et x et y deux éléments de L ayant même polynôme minimal sur K. Alors il existe σ dans $\mathsf{Gal}(L : K)$ tel que $\sigma(x) = y$.*

Demonstration. L'extension $(L : K)$ est le corps de décomposition d'un polynôme $Q \in P[X]$. Il existe un morphisme d'extensions (unique) σ_0 de $(K(x) : K)$ dans L qui envoie x sur y (2.3.3). Les extensions $(L : K(x))$ et $\sigma_0 : K(x) \longrightarrow L$ sont deux corps de décomposition de Q sur $K(x)$; elles sont donc isomorphes. D'où l'existence d'un automorphisme σ de L qui prolonge σ_0. □

Fin de la démonstration de la proposition 3.3.1. Soit $E \in K$ invariant par G.
Soit $P \in K[X]$ un polynôme irréductible unitaire admettant une racine x dans E. Alors P est scindé dans L, car $(L : K)$ est normal. Si y est une racine de P dans L, il existe $\sigma \in G$ tel que $\sigma(x) = y$ et puisque E est invariant, $y \in E$. Ainsi, P est scindé dans E, ce qui montre que $(E : K)$ est normale. □

Reste l'assertion (5) du théorème de Galois. Soit E un corps intermédiaire tel que l'extension $(E : K)$ soit normale, donc donc galoisienne. Par l'assertion (1) du théorème, $\mathcal{O}(\mathsf{Gal}(E : K)) = [E : K]$. D'autre part E est invariant sous l'action de $\mathsf{Gal}(L : K)$, donc tout automorphisme de $(L : K)$ induit par restriction un automorphisme de $(E : K)$; d'où un morphisme de groupes :

$$\mathsf{Gal}(L : K) \longrightarrow \mathsf{Gal}(E : K) .$$

Ce morphisme a pour noyau $E^{\star} = \mathsf{Gal}(L : E)$, et induit donc par passage au quotient un morphisme de groupes injectif $\psi : \mathsf{Gal}(L : K)/\mathsf{Gal}(L : E) \hookrightarrow \mathsf{Gal}(E : K)$. Comme $[\mathsf{Gal}(L : K) : \mathsf{Gal}(L : E)] = [E : K]$ (assertion (3) du théorème) $= \mathcal{O}(\mathsf{Gal}(E : K)$, ψ est un isomorphisme, ce qui achève la démonstration de l'assertion (5) et donc du théorème de Galois. □

4. Quelques exemples

4.1.

Soit $K = \mathbb{Q}$. Soit Q le polynôme $X^4 - 2$; il est irréductible dans $\mathbb{Q}[X]$. Soit $\xi = \sqrt[4]{2}$. Alors Q admet les racines ξ, $i\xi$, $-\xi$ et $-i\xi$ dans $\mathbb{C}$. Le corps de décomposition de Q est donc $L = \mathbb{Q}(\xi, i)$. On a $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$, et $L = \mathbb{Q}(\xi)(i) = \mathbb{Q}(\xi) \oplus i\mathbb{Q}(\xi)$, donc $[L : \mathbb{Q}] = 8$. Soit $G = \mathsf{Gal}(L : \mathbb{Q})$. C'est un groupe à huit éléments. Il existe τ unique dans G vérifiant : $\tau(\xi) = \xi$ et $\tau(i) = -i$; c'est la restriction à L de la conjuguaison complexe. D'autre part il existe σ unique dans G vérifiant $\sigma(\xi) = i\xi$ et $\sigma(i) = i$. (En effet, $L = \mathbb{Q}(i)(\xi)$ est une extension de degré 4 de $\mathbb{Q}(i)$; $i\xi$ est une racine de $P_{\xi,\mathbb{Q}(i)} = X^4 - 2$, et σ est l'unique automorphisme de $(L : \mathbb{Q}(i))$ qui envoie ξ sur $i\xi$.)
Ces éléments vérifient :

$$\sigma^4 = e, \qquad \tau^2 = e, \qquad \tau\sigma = \sigma^3\tau \quad .$$

On a $G = \{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$. C'est le *groupe diédral d'ordre 8*, qu'on note D_4 (c'est le groupe des isométries d'un carré).
Les sous-groupes de G sont les suivants.

Sous-groupes d'ordre 8 :
$G = \mathsf{D}_4$.

Sous-groupes d'ordre 4 :
$S = \{e, \sigma, \sigma^2, \sigma^2\}$,
$T = \{e, \sigma^2, \tau, \sigma^2\tau\}$,
$U = \{e, \sigma^2, \sigma\tau, \sigma^2\tau\}$.
Ce sont des sous-groupes distingués de G; S est isomorphe à $\mathbb{Z}/4\mathbb{Z}$; U et T sont isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Sous-groupes d'ordre 2 :
$A = \{e, \sigma^2\}$,
$B = \{e, \tau\}$,
$C = \{e, \sigma\tau\}$,
$D = \{e, \sigma^2\tau\}$,
$E = \{e, \sigma^3\tau\}$,
Seul A est distingué dans G; tous sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$.

Et le sous-groupe trivial 1.

On en déduit par un calcul les sous-corps de L :
$G^\dagger = \mathbb{Q}$,
$S^\dagger = \mathbb{Q}(i)$,
$T^\dagger = \mathbb{Q}(\sqrt{2})$,
$U^\dagger = \mathbb{Q}(i\sqrt{2})$,
$A^\dagger = \mathbb{Q}(i, \sqrt{2})$,
$B^\dagger = \mathbb{Q}(\xi)$,
$C^\dagger = \mathbb{Q}((1+i)\xi)$,
$D^\dagger = \mathbb{Q}(i\xi)$,

$E^{\dagger} = \mathbb{Q}((1-i)\xi)$,
$1^{\dagger} = L$.

4.2. Corps finis.

Soit E un corps commutatif fini,(*) de cardinal q. La caractéristique de E est un nombre premier p (en effet, un corps de caractéristique zéro est infini, car son plus petit sous-corps est isomorphe à $\mathbb{Q}$). Par conséquent le plus petit sous-corps de E est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On note encore $\mathbb{F}_p$ ce sous-corps. Soit n le degré de l'extension $(E : \mathbb{F}_p)$; alors $q = p^n$. L'ordre du groupe des éléments inversibles de E est $q-1$; on a donc $x^{q-1} - 1 = 0$ pour tout $x \in E$ non nul; on en déduit : $\forall x \in E, x^q - x = 0$.
Il en résulte que l'extension $(E : \mathbb{F}_p)$ est un corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$; en effet ce polynôme de degré q admet pour racines tous les éléments de E, qui sont au nombre de q.

Par ailleurs, si E est un corps commutatif de caractéristique p, l'application

$$\begin{aligned} F : E &\longrightarrow E \\ x &\mapsto x^p \end{aligned}$$

est un morphisme de corps appelé *morphisme de Frobénius*. Pour m entier ≥ 1, F^m est encore un morphisme de corps. Il en résulte que l'ensemble des points fixes de F^m est un sous-corps de E; c'est aussi l'ensemble des racines du polynôme $X^{p^m} - X$ dans E, donc il est de cardinal au plus p^m.

Soit p un npmbre premier, n un entier ≥ 1, et $q = p^n$. Notons $\mathbb{F}_q$ le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$. Soit R l'ensemble des racines de $X^q - X$ dans $\mathbb{F}_q$: ces racines sont simples, car la dérivée de $X^q - X$ dans $\mathbb{F}_p[X]$ vaut -1; par conséquent, R a pour cardinal q. Par définition, R engendre l'extension $(\mathbb{F}_q : \mathbb{F}_p)$, et comme R est un sous-corps de $\mathbb{F}_q$ contenant $\mathbb{F}_p$, on a $R = \mathbb{F}_q$. Ainsi, $\mathbb{F}_q$ est un corps de cardinal q. La proposition suivante résume ces informations.

4.2.1. Proposition. *Le cardinal d'un corps (commutatif) fini est toujours de la forme $q = p^n$, où p est un nombre premier et n un entier ≥ 1.*
Pour un tel nombre q, il existe un corps (commutatif) de cardinal q; en outre un tel corps est unique à isomorphisme près. Ce corps, noté $\mathbb{F}_q$, est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. □

Soit G le groupe des automorphismes de $\mathbb{F}_q$. C'est un groupe fini, puisque c'est un sous-groupe du groupe des permutations de $\mathbb{F}_q$. Le morphisme de Frobénius $F : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ est injectif, donc bijectif; c'est donc un élément de G. Soit m un entier ≥ 1. Le morphisme F^m a au plus p^m points fixes, donc F^m n'est pas l'identité de $\mathbb{F}_q$ si $1 \leq m < n$; par conséquent, le sous-groupe de G engendré par F est d'ordre au moins n. Soit $K = \mathbb{F}_q^G$ le corps des points fixes de $\mathbb{F}_q$ sous l'action de G. On sait que l'extension $(\mathbb{F}_q : K)$ est galoisienne, de degré $\mathcal{O}(G) \geq n$. D'autre part, $\mathbb{F}_p \subset K$, et $[\mathbb{F}_q : \mathbb{F}_p] = n$; donc $K = \mathbb{F}_p$, et $\mathcal{O}(G) = n$. D'où la proposition suivante.

(*) En fait, tout corps fini est commutatif : c'est le théorème de Wedderburn.

4.2.2. Proposition. *L'extension* $(\mathbb{F}_q : \mathbb{F}_p)$ *est galoisienne, et son groupe de Galois est un groupe cyclique d'ordre* n *engendré par le morphisme de Frobénius.* $\square$

Pour chaque entier naturel d divisant n, il y a exactement *un* sous-groupe d'ordre n/d dans $\mathbb{Z}/n\mathbb{Z}$: c'est le sous-groupe engendré par la classe de d. Appliquant le théorème de Galois à cette situation, on obtient le corollaire suivant.

4.2.3. Corollaire. *Pour chaque entier naturel* d *divisant* n, *il existe un et un seul sous-corps de cardinal* p^d *dans* $\mathbb{F}_q$ *; c'est l'ensemble des points fixes de* F^d. *Notons-le* $\mathbb{F}_{p^d}$. *L'extension* $[\mathbb{F}_q : \mathbb{F}_{p^d}]$ *est galoisienne, et son groupe de Galois est cyclique d'ordre* n/d, *engendré par* F^d. $\square$

4.3. Corps cyclotomiques

Définition. Soit n un entier ≥ 1. On appelle *n-ième corps cyclotomique* le sous-corps de $\mathbb{C}$ engendré par les racines n-ièmes de l'unité.

Soit $n \geq 1$. L'ensemble μ_n des racines n-ièmes complexes de l'unité est un sous-groupe de $\mathbb{C}^*$, cyclique d'ordre n. Les générateurs de μ_n sont ses éléments d'ordre n, les racines n-ièmes primitives; on note Π_n l'ensemble de ces racines, et $\phi(n) = \# \Pi_n$. On définit le n-ième polynôme cyclotomique Φ_n par la formule :

$$\Phi_n = \prod_{\xi \in \Pi_n} (X - \xi).$$

C'est un polynôme unitaire de degré $\phi(n)$. On a alors :

$$X^n - 1 = \prod_{\omega \in \mu_n} (X - \omega) = \prod_{d|n} \Phi_d$$

car μ_n est la réunion disjointe des Π_d pour d entier naturel divisant n. De cette formule se déduit par récurrence sur n que les coefficients de Φ_n sont entiers.

4.3.1. Proposition. *Soit* $\xi \in \Pi_n$. *Le* n*-ième corps cyclotomique est le corps* $\mathbb{Q}(\xi)$. *En outre le polynôme minimal de* ξ *sur* $\mathbb{Q}$ *est* Φ_n. *L'extension* $(\mathbb{Q}(\xi) : \mathbb{Q})$ *est galoisienne, de degré* $\phi(n)$, *et son groupe de Galois est isomorphe à* $(\mathbb{Z}/n\mathbb{Z})^*$.

Demonstration. En tant que corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$, le n-ième corps cyclotomique est une extension normale de $\mathbb{Q}$, donc galoisienne, puisqu'en caractéristique zéro toute extension est séparable. L'élément ξ engendre le groupe μ_n, donc il engendre le n-ième corps cyclotomique sur $\mathbb{Q}$.

4.3.2. Lemme. *Le polynôme* Φ_n *est irréductible sur* $\mathbb{Q}$.

DEMONSTRATION. Soit P un facteur irréductible unitaire de Φ_n. On a $\Phi_n = PQ$, et, en vertu du lemme de Gauss, P et Q sont à coefficients entiers. Soit ζ une racine de P, et p un nombre premier ne divisant pas n. Alors $\zeta^p \in \Pi_n$. On se propose de montrer que ζ^p est encore une racine de P.
Supposons $P(\zeta^p) \neq 0$. On a $\zeta^p \in \Pi_n$, donc $Q(\zeta^p) = 0$; autrement dit, ζ est une racine de $Q(X^p)$. Il en résulte que P divise $Q(X^p)$ dans $\mathbb{Z}[X]$. Considérons le morphisme d'anneaux

$$\begin{gathered}\mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X] \\ R = \sum a_k X^k \mapsto \overline{R} = \sum \overline{a_k} X^k .\end{gathered}$$

Alors $\overline{P}$ divise $\overline{Q}(X^p)$; or, on a $\overline{Q}(X^p) = \overline{Q}^p$; ainsi, $\overline{P}$ divise $\overline{Q}^p$.
Soit E un corps de décomposition du polynôme $X^n - \overline{1}$ sur $\mathbb{F}_p$. Alors $\overline{P}$ et $\overline{Q}$ ont une racine commune dans E, et $\overline{PQ} = \overline{\Phi}_n$ a une racine multiple. Par ailleurs le polynôme $X^n - \overline{1}$ n'a que des racines simples dans E, sa dérivée ayant pour seule racine 0, et $\overline{\Phi}_n$ le divise, donc ne peut avoir de racine multiple, d'où contradiction.
On a donc montré que pour ζ racine de P et p premier ne divisant pas n, ζ^p est encore une racine de P. On en déduit immédiatement que ζ^m est une racine de P pour tout entier m premier à n; or, les ζ^m décrivent Π_n lorsque m décrit l'ensemble des entiers premiers à n; les éléments de Π_n sont donc tous racines de P, d'où $\Phi_n = P$ est irréductible. □

Comme $\Phi_n(\xi) = 0$, Φ_n est le polynôme minimal de ξ sur $\mathbb{Q}$. Soit $G = \mathsf{Aut}(\mathbb{Q}(\xi))$; c'est le groupe de Galois de $(\mathbb{Q}(\xi) : \mathbb{Q})$, car tout $\sigma \in G$ induit l'identité sur $\mathbb{Q}$. Pour $\alpha \in \mathbb{Z}/n\mathbb{Z}$ et $\omega \in \mu_n$, posons $\omega^\alpha = \omega^a$, où $a \in \mathbb{Z}$ est un représentant de α. Lorsque α décrit $(\mathbb{Z}/n\mathbb{Z})^*$, ξ^α décrit Π_n, ensemble des racines de Φ_n. Pour un tel α, il existe donc un unique $\sigma_\alpha \in G$ vérifiant $\sigma_\alpha(\xi) = \xi^\alpha$, et tout élément de G est de cette forme. Pour tout $\omega \in \mu_n$, on a $\sigma_\alpha(\omega) = \omega^\alpha$. L'application

$$\begin{gathered}\mathbb{Z}/n\mathbb{Z} \longrightarrow G \\ \alpha \mapsto \sigma_\alpha\end{gathered}$$

est donc un isomorphisme de groupes. □

5. Résolution par radicaux

5.1. Extensions radicales

Etant donné un polynôme $P \in \mathbb{Q}[X]$, on aimerait savoir si chaque racine de P peut être exprimée au moyen d'une formule ne faisant intervenir que des nombres rationnels, les opérations arithmétiques usuelles ($+$,$-$, $\times$, $/$) et l'extraction d'une racine n-ième.
Pour formuler ce problème de façon précise, on est amené a poser les définitions suivantes. Nous nous placerons en caractéristique 0 pour simplifier l'exposé.

Définition. Soit K un corps commutatif, $\mathsf{car}(K) = 0$. Une extension finie $(E : K)$ est dite *radicale* s'il existe des éléments $x_1, \ldots, x_n$ dans E tels que, si l'on pose $E_i = K(x_1, \ldots, x_i)$ (donc $E_0 = K$), on ait : $E_n = E$, et pour tout $i = 1, \ldots, n$, il existe un entier $d_i > 0$ tel que ${x_i}^{d_i} \in E_{i-1}$.
(On résumera cela en disant que E s'obtient à partir de K par l'adjonction successive des racines $x_1, \ldots, x_n$.)

Définition. Un polynôme P à coefficients dans K (avec $\mathsf{car}(K) = 0$) est dit *résoluble par radicaux (sur K)* s'il est scindé dans une extension radicale finie de K.

5.2. Rapport entre extensions radicales et groupes résolubles

5.2.1. Théorème. *Soit K un corps commutatif de caractéristique nulle. Alors*
1) la clôture normale d'une extension finie radicale de K est une extension radicale de K ;
2) soit $(L : K)$ une extension de K et E un corps intermédiaire entre K et L. Si l'extension $(L : K)$ est radicale, le groupe de Galois de l'extension $(E : K)$ est résoluble.

Demonstration.
Assertion 1).
Si $(L : K)$ est une extension, et si E, F sont deux corps intermédiaires, on note EF le sous-corps de L engendré par E et F. Si $(E : K)$ et $(F : K)$ sont des extensions radicales, alors $(EF : K)$ est encore une extension radicale. En effet, si E s'obtient à partir de K par l'adjonction successive des racines $x_1, \ldots, x_m$, et si F s'obtient à partir de K par l'adjonction successive des racines $y_1, \ldots, y_n$, alors EF s'obtient à partir de K par l'adjonction successive des racines $x_1, \ldots, x_m, y_1, \ldots, y_n$.

Lemme. *Soit $(E : K)$ une extension finie, et $(L : E)$ une clôture normale de $(E : K)$. Alors le corps L est engendré par les $\sigma(E)$, pour σ décrivant $\mathsf{Gal}(L : K)$.*

Demonstration. Soit L' le sous-corps de L engendré par les $\sigma(E)$, pour σ décrivant $\mathsf{Gal}(L : K)$. Il contient E, et il est invariant sous l'action de $\mathsf{Gal}(L : K)$, donc l'extension $(L' : K)$ est normale (3.3.1). La propriété de minimalité de la clôture normale entraîne : $L' = L$. $\square$
La clôture normale $(L : K)$ de $(E : K)$ est donc engendrée par les $\sigma(E)$ pour $\sigma \in \mathsf{Gal}(L : K)$. Si $(E : K)$ est radicale, chacun des $(\sigma(E) : K)$ l'est encore, ainsi que $(L : K)$.

Assertion 2).
La démonstration en est plus longue. Tout d'abord, quelques réductions.
Soit K_0 le corps des points fixes de E sous l'action de $\mathsf{Gal}(E:K)$; on a donc $K \subset K_0$. Si $(L:K)$ est radicale, $(L:K_0)$ l'est à plus forte raison. En outre $(E:K_0)$ est galoisienne (3.2.3.), et $\mathsf{Gal}(E:K) = \mathsf{Gal}(E:K_0)$. On peut donc supposer $(E:K)$ galoisienne.
D'après 1), on peut remplacer $(L:K)$ par sa clôture normale, et ainsi supposer $(L:K)$ galoisienne. Alors $\mathsf{Gal}(E:K)$ est un quotient de $\mathsf{Gal}(L:K)$; comme tout quotient d'un groupe résoluble est encore résoluble, on peut supposer $E = L$.
On se ramène ainsi à démontrer que le groupe de Galois d'une extension galoisienne finie radicale est résoluble.
On commence par traiter deux cas particuliers importants, qui font l'objet des deux lemmes suivants.

5.2.2. Lemme. *Soit K un corps commutatif de caractéristique nulle. Soit p un nombre premier, et $(L:K)$ le corps de décomposition de $X^p - 1$ sur K. Alors $\mathsf{Gal}(L:K)$ est abélien.*

Demonstration. Les racines p-ièmes de 1 dans L constituent un groupe Γ d'ordre p. Soit ω un générateur de ce groupe. Soit $G = \mathsf{Gal}(L:K)$. Tout $\sigma \in G$ est déterminé par $\sigma(\omega)$, qui est un élément de Γ, donc de la forme ω^m. Soit $\sigma' \in G$; alors $\sigma'(\omega)$ s'écrit ω^n, et on a $\sigma\sigma'(\omega) = \omega^{nm} = \sigma'\sigma(\omega)$, donc $\sigma\sigma' = \sigma'\sigma$. $\square$

5.2.3. Lemme. *Soit p un nombre premier, et K un corps commutatif de caractéristique nulle dans lequel $X^p - 1$ est scindé. Soit a un élément de K, et $(L:K)$ le corps de décomposition de $X^p - a$ sur K. Alors $\mathsf{Gal}(L:K)$ est abélien.*

Demonstration. Soit α une racine p-ième de a, Γ le groupe des racines p-ièmes de 1 dans L, et ω un générateur de Γ. Les racines p-ièmes de a sont les $\alpha\omega^k$, et on peut répéter la démonstration du lemme précédent. $\square$

Fin de la démonstration de l'assertion 2) du théorème.
Soit $(L:K)$ une extension galoisienne finie radicale. On obtient L à partir de K par l'adjonction successive de racines $x_1, \ldots, x_n$. Notons $L_i = K(x_1, \ldots, x_i)$. Pour tout $i = 1, \ldots, n$, il existe un entier $p_i > 0$ tel que ${x_i}^{p_i} \in L_{i-1}$. On peut supposer les p_i premiers, quitte à rajouter des étapes.
Soit p un nombre premier, $(L':L)$ un corps de décomposition de $X^p - 1$ sur L, et K' le sous-corps de L' engendré sur K par les racines de $X^p - 1$. L'extension $(L':K)$ est normale, donc galoisienne, et $(K':K)$ est un corps de décomposition de $X^p - 1$ sur K. On a $L' = K'(x_1, \ldots, x_n)$, donc $(L':K')$ est radicale et galoisienne. Dans ce cadre, montrons que si $\mathsf{Gal}(L':K')$ est résoluble, $\mathsf{Gal}(L:K)$ l'est aussi.
Supposons $\mathsf{Gal}(L':K')$ résoluble. Alors $\mathsf{Gal}(K':K) \simeq \mathsf{Gal}(L':K)/\mathsf{Gal}(L':K')$ par le théorème de Galois. D'après le lemme 5.2.2, $\mathsf{Gal}(K':K)$ est commutatif, donc résoluble. Ainsi, $\mathsf{Gal}(L':K)$ est résoluble (1.4.2). Le groupe $\mathsf{Gal}(L:K)$ est un quotient de $\mathsf{Gal}(L':K)$; donc il est résoluble.
En vertu de ce qui précède, on peut supposer que les polynômes $X^{p_i} - 1$ sont tous scindés dans K. On procède maintenant par récurrence sur n. Si $n = 0$, $L = K$ et le groupe de Galois est trivial. Pour $n > 0$, l'extension $(K(x_1):K)$ est normale, car c'est un corps de

décomposition pour $X^{p_1} - x_1^{p_1}$ sur K. On a donc un isomorphisme : $\mathsf{Gal}(K(x_1) : K) \simeq \mathsf{Gal}(L : K)/\mathsf{Gal}(L : K(x_1))$. L'hypothèse de récurrence assure que $\mathsf{Gal}(L : K(x_1))$ est résoluble, et le lemme 5.2.3, que $\mathsf{Gal}(K(x_1) : K)$ est commutatif; donc $\mathsf{Gal}(L : K)$ est résoluble par 1.4.2. □

5.3. Un exemple d'équation de degré 5 non résoluble par radicaux

5.3.1. Proposition. *Le polynôme $X^5 - 6X + 3$ n'est pas résoluble par radicaux sur $\mathbb{Q}$.*

DEMONSTRATION. Par le critère d'Eisenstein, le polynôme $P = X^5 - 6X + 3$ est irréductible dans $\mathbb{Q}[X]$. D'autre part, une étude de fonction montre que P admet exactement trois racines réelles.

5.3.2. Lemme. *Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible sur $\mathbb{Q}$ de degré premier impair p admettant exactement $p-2$ racines réelles. Alors le groupe de Galois de P (c'est-à-dire celui du corps de décomposition de P sur $\mathbb{Q}$) est isomorphe au groupe symétrique $\mathfrak{S}_p$.*

DEMONSTRATION. Soit L le corps de décomposition de P sur $\mathbb{Q}$, et G le groupe de Galois de L sur $\mathbb{Q}$. Ce groupe permute les racines de P. Si l'on numérote celles-ci de 1 à p, G apparaît comme un sous-groupe de $\mathfrak{S}_p$. Soit $\tau \in G$ la conjuguaison complexe.
Le polynôme P a exactement deux racines de partie imaginaire non nulle, et ces racines sont conjuguées, donc τ est la transposition de ces deux racines. D'autre part, soit ξ une racine de P. Alors L contient $\mathbb{Q}(\xi)$, qui est de degré p sur $\mathbb{Q}$, donc p divise $[L : \mathbb{Q}] = \mathcal{O}(G)$. D'autre part, $\mathcal{O}(G)$ divise $\mathcal{O}(\mathfrak{S}_p) = p!$ Ainsi, G contient un élément d'ordre p. En tant que permutation, cet élément est un cycle de longueur p.
Ainsi, G s'identifie à un sous-groupe de $\mathfrak{S}_p$ qui contient une transposition τ et un p-cycle σ. Nons allons voir qu'un tel sous-groupe est égal à $\mathfrak{S}_p$. Quitte à renuméroter les éléments, on peut supposer que τ est la transposition $(1,2)$. Il existe k tel que $\sigma^k(1) = 2$, donc quitte à remplacer σ par σ^k, on peut supposer $\sigma(1) = 2$; renumérotant $3, \dots p$, on se ramène au cas où $\tau = (1,2)$ et $\sigma = (1, 2, \dots, p)$, et ces deux éléments engendrent $\mathfrak{S}_p$. □

Ainsi, le groupe de Galois de $X^5 - 6X + 3$ sur $\mathbb{Q}$ est $\mathfrak{S}_5$, qui n'est pas résoluble, donc P n'est pas résoluble par radicaux. □

Lors de la révision de ce texte, j'ai corrigé un certain nombre de coquilles et simplifié plusieurs démonstrations. Il reste certainement beaucoup d'erreurs et de maladresses.

Toute critique, toute suggestion et tout commentaire seront les bienvenus!

Alain Bruguières
Département de Mathématiques
C. C. 051
Université Montpellier II
Place Eugène Bataillon
34 095 MONTPELLIER CEDEX 5
e-mail : bruguier@math.univ-montp2.fr