Algèbre de base

À Rennes, année 2016

Tobias Schmidt

Table des matières

Ce document est issu d'une prise de note par Gwendal Soisnard pendant le cours d'algèbre de base enseigné par Tobias Schmidt à l'université de Rennes 1 durant l'année 2016.

✧ **Référence :**

- N. Bourbaki, *Algèbre*
- Michael Artin, *Algebra*
- Serge Lang, *Algebra*
- N. Jacobson, *Basic Algebra I*
- S. Bosch, *Algebra*

Partie I

Anneaux et modules

1. Rappels sur les groupes

Soit X un ensemble.

1.1 Relation d'équivalence

Définition 1.1.1 - Relation.
Une *relation* sur X est une partie $\mathscr{R} \subset X \times X$. On note $x \sim y$ au lieu de $(x, y) \in \mathscr{R}$.
Une relation $\mathscr{R}$ est dite :

- **Réflexive** si : $\forall x \in X : x \sim x$.
- **Transitive** si : $\forall x, y, z \in X : (x \sim y \text{ et } y \sim z) \Rightarrow x \sim z$.
- **Symétrique** si : $\forall x, y \in X : x \sim y \Rightarrow y \sim x$.
- **Antisymétrique** si : $\forall x, y \in X : (x \sim y \text{ et } y \sim x) \Rightarrow x = y$.

Définition 1.1.2 - Relations particulières.
On appelle *relation d'équivalence* toute relation réflexive, symétrique et transitive.
On appelle *relation d'ordre (partielle)* toute relation réflexive, antisymétrique et transitive.

Définition 1.1.3 - Classe d'équivalence.
Soit $\sim$ une relation d'équivalence sur X.
On appelle *classe d'équivalence* de $x \in X$ l'ensemble suivant :

$$\overline{x} := \left\{ y \in X \mid x \sim y \right\} \subset X$$

On note $X/\sim$ l'ensemble des classes d'équivalences des éléments de X.
On a la projection canonique π suivante :

$$\begin{array}{rccc} \pi : & X & \longrightarrow & X/\sim \\ & x & \longmapsto & \overline{x} \end{array}$$

Remarque. Toute relation d'équivalence définie une partition :

$$X = \bigsqcup_{\overline{x} \in X/\sim} \overline{x}$$

Réciproquement, toute partition $X = \bigsqcup_{i \in I} X_i$ induit une relation d'équivalence en définissant :

$$\forall x, y \in X : x \sim y \Leftrightarrow \exists i \in I : x, y \in X_i$$

♢

1.2 Loi de composition interne

Définition 1.2.1 - Loi de composition interne.
On appelle *loi de composition interne* sur X toute application $\bullet : X \times X \to X$.
Une loi $\bullet$ est dite :

- **Associative** si : $\forall x, y, z \in X : x \bullet (y \bullet z) = (x \bullet y) \bullet z$.
- **Admettant un neutre** si : $\exists e \in X, \forall x \in X : x \bullet e = e \bullet x = x$.

- **Commutative** si : $\forall x, y \in X : x \cdot y = y \cdot x$.

1.3 Groupe quotient

Définition 1.3.1 - Groupe.
On appelle *groupe* tout ensemble G muni d'une loi de composition interne $\cdot : G \times G \to G$ telle que :

- La loi est **associative** : $\forall x, y, z \in G : (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- La loi possède un **élément neutre** : $\exists e \in G, \forall x \in G : x \cdot e = e \cdot x = x$.
- Tout élément $x \in G$ possède **un inverse** : $\forall x \in G, \exists x' \in G : x \cdot x' = x' \cdot x = e$.

On dit que le groupe est **commutatif**, ou **abélien**, si $\forall x, y \in G : x \cdot y = y \cdot x$.

Remarque. Dans un groupe G, l'élément neutre (souvent noté 1) est unique. Pareillement, l'inverse x^{-1} de x est unique. On écrit souvent xy au lieu de $x \cdot y$. Dans le cas abélien, on utilise la notation additive : $+$ au lieu de $\cdot$, 0 au lieu de 1, $-x$ au lieu de x^{-1}. ♢

Définition 1.3.2 - Morphisme de groupes.
Soit deux groupes G et H.
On appelle *morphisme de groupes* toute application $f : G \to H$ vérifiant :

$$\forall x, y \in G : f(x \cdot y) = f(x) \cdot f(y)$$

On appelle :

- *Noyau* de f l'ensemble $\mathrm{Ker}(f) := \{x \in G \mid f(x) = 1\}$.
- *Image* de f l'ensemble $\mathrm{Im}(f) := \{y \in H \mid \exists x \in G : y = f(x)\}$.

Nous appelons *isomorphisme* tout morphisme bijectif. Dans ce cas, l'application inverse f^{-1} est aussi un morphisme.

Remarque.

- L'image de $1 \in G$ par un morphisme de groupes $f : G \to H$ est $1 \in H$.
- L'image de $x^{-1} \in G$ par un morphisme de groupes $f : G \to H$ est $f(x)^{-1} \in H$.

♢

Définition 1.3.3 - Sous-groupe.
On appelle *sous-groupe* d'un groupe G un sous-ensemble $H \subset G$ préservant la structure de groupe :

- $\forall x, y \in H : xy \in H$.
- $\forall x \in H : x^{-1} \in H$.

En particulier, H est un groupe.

Définition 1.3.4 - Sous-groupe normal.
On appelle *sous-groupe normal* tout sous-groupe H de G vérifiant :

$$\forall x \in G, y \in H : x^{-1}yx \in H$$

On le note $H \triangleleft G$.

Exemple. Soit $f : G \to H$ un morphisme.

- L'image $\mathrm{Im}(f) \subset H$ est un sous-groupe.
- Le noyau $\mathrm{Ker}(f) \subset G$ est un sous-groupe normal.

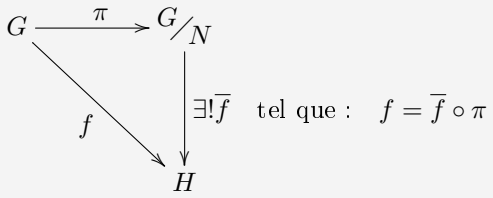
△

Théorème 1.3.5 - Propriété universelle du groupe quotient.
Soit G un groupe et N un sous-groupe normal.
On a une la relation d'équivalence $\sim$ sur G par :

$$\forall x, y \in G : x \sim y \Leftrightarrow x^{-1} \cdot y \in N$$

La classe d'équivalence $\overline{x}$ de x est $xN := \left\{xn \mid n \in N\right\} \subset G$ et on pose ${}^{G}\!/_{N} := {}^{G}\!/_{\sim}$. L'ensemble ${}^{G}\!/_{N}$ est un groupe par rapport à la loi interne $xN \cdot yN := xyN$ et la projection $\pi : G \to {}^{G}\!/_{N}, x \mapsto xN$ est un morphisme de groupes. Il satisfait la propriété universelle :

Pour tout groupe H et tout morphisme $f : G \to H$ tel que $N \subset \mathrm{Ker}(f)$, il existe un unique morphisme $\overline{f} : {}^{G}\!/_{N} \to H$ tel que le diagramme suivant commute :



Remarque. Dans le groupe ${}^{G}\!/_{N}$ on a $(xN)^{-1} = x^{-1}N$ et la classe N est l'élément neutre. En plus, on a $\mathrm{Ker}\left(\overline{f}\right) = {}^{\mathrm{Ker}(f)}\!/_{N}$ et $\mathrm{Im}\left(\overline{f}\right) = \mathrm{Im}(f)$. ♢

Démonstration. Exercice. Le morphisme $\overline{f}$ est défini par $\overline{f}(xN) := f(x)$.

Corollaire 1.3.6
Soit G et H deux groupes.
Soit $\varphi : G \to H$ un morphisme surjectif de noyau N. Alors $\overline{\varphi}$ est un isomorphisme ${}^{G}\!/_{N} \simeq H$.

Théorème 1.3.7 - Premier théorème d'isomorphisme.
Soit G un groupe, N un sous-groupe normal de G et H un sous-groupe de G.
L'ensemble $HN := \left\{hn \mid h \in H, n \in N\right\}$ est un sous-groupe de G. En plus, $N \cap H$ est un sous-groupe normal de H et N est un sous-groupe normal de HN. L'inclusion $H \to HN$ composé avec la projection canonique $HN \to {}^{HN}\!/_{N}$ induit un isomorphisme

$${}^{H}\!/_{H \cap N} \cong {}^{HN}\!/_{N}$$

Démonstration. Exercice. Le morphisme composé $H \to HN \to {}^{HN}\!/_{N}, h \mapsto hN$ est surjectif et son noyau est $N \cap H$.

Corollaire 1.3.8 - Deuxième théorème d'isomorphisme.
Soit G un groupe et N et M deux sous-groupes normaux de G tels que M soit inclus dans N.
Alors ${}^{N}\!/_{M}$ est un sous-groupe normal de ${}^{G}\!/_{M}$ et l'application ${}^{G}\!/_{M} \to {}^{G}\!/_{N}, gM \mapsto gN$ induit un isomorphisme

$$\left({}^{G}\!/_{M}\right)\!/\left({}^{N}\!/_{M}\right) \cong {}^{G}\!/_{N}$$

Démonstration. Exercice. L'application ${}^{G}\!/_{M} \to {}^{G}\!/_{N}, gM \mapsto gN$ est bien-défini (car $M \subset N$) et un morphisme surjectif. Son noyau est ${}^{N}\!/_{M}$.

2. Anneaux

L'objectif de ce chapitre est d'introduire la théorie fondamentale des anneaux et des modules.

2.1 Définition d'un anneau

Considérons un ensemble A muni de deux lois de composition interne :

$$\begin{array}{rccc} +: & A\times A & \longrightarrow & A \\ & (x,y) & \longmapsto & x+y \end{array} \quad \text{et} \quad \begin{array}{rccc} \cdot: & A\times A & \longrightarrow & A \\ & (x,y) & \longmapsto & x\cdot y \end{array}$$

Définition 2.1.1 - Anneau.
On appelle *anneau* tout ensemble muni de deux lois de composition $+$ et $\cdot$ telles que :

1. L'ensemble $(A,+)$ est un groupe abélien dont on note 0 l'élément neutre ;
2. La loi $\cdot$ est associative et possède un neutre 1 différent de 0 ;
3. La loi est distributive sur $+$:

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

Un anneau est dit *commutatif* si la loi $\cdot$ est commutative, c'est-à-dire si $\forall x,y : x\cdot y = y\cdot x$.

Remarque. On écrit souvent xy au lieu de $x\cdot y$.

La condition 2. implique que A n'est pas nul.

De plus, $(A,\cdot)$ n'est pas un groupe. En effet 0 n'a pas d'inverse :

$$\forall x\in A : 0\cdot x = (1-1)\cdot x = 1\cdot x - 1\cdot x = x - x = 0 \neq 1$$

♢

Exemple. Donnons des exemples d'anneaux :

- Un corps, en particulier les corps classiques $\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (avec p premier).
- Les anneaux de matrices sur un corps.
- L'anneau des polynômes à coefficients dans un corps.
- L'anneau des entiers $\mathbb{Z}$ et l'anneau des entiers de Gauss $\mathbb{Z}[i]\subset\mathbb{C}$.

△

2.2 Morphisme d'anneaux, sous-anneau et centre

Définition 2.2.1 - Morphisme d'anneaux.
Soit $(A,+,\cdot)$ et $(B,+,\cdot)$ deux anneaux.
On appelle *morphisme d'anneaux* toute application $f : A\to B$ telle que :

- L'application f est un morphisme de groupes de $(A,+)$ dans $(B,+)$:

$$\forall a,b\in A : f(a+b) = f(a) + f(b)$$

- L'application f préserve $\cdot$:

$$\forall x,y\in A : f(x\cdot y) = f(x)\cdot f(y)$$

- On a

$$f(1_A) = 1_B$$

On appelle *isomorphisme* tout morphisme bijectif. Dans ce cas l'application inverse est aussi un morphisme.

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

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \longrightarrow & A \\ & n & \longmapsto & n \cdot 1_A := 1_A + \cdots + 1_A \end{array}$$

(n-fois) si $n > 0$ et $\varphi(n) := -\varphi(-n)$ si $n < 0$. △

Définition 2.2.2 - Sous-anneau.
Soit $(A, +, \cdot)$ un anneau.
On appelle *sous-anneau* tout sous-groupe A' de $(A, +)$ qui contient 1 et qui est stable par la multiplication :

$$\forall x, y \in A' : x \cdot y \in A'$$

En particulier, A' est un anneau.

Exemple. Soit $(A_i)_{i \in I}$ est une famille de sous-anneaux de A. Alors $\bigcap_{i \in I} A_i \subset A$ est un sous-anneau.

Si $f : A \to B$ est un morphisme d'anneaux alors $\mathrm{Im}(f) \subset B$ est un sous-anneau. △

Définition 2.2.3 - Centre d'un anneau.
Soit A un anneau. On appelle *centre* de A l'ensemble

$$\mathcal{Z} = \Big\{ a \in A \mid ab = ba, \forall b \in A \Big\}$$

Tout élément de $\mathcal{Z}$ est dit *central*. Le centre $\mathcal{Z}$ est un sous-anneau commutatif de A.

Exemple. Soit K un corps et A l'anneau de matrices carrés de taille n sur K. Le centre $\mathcal{Z}$ de A sont les matrices diagonaux $diag(a, ..., a)$ avec $a \in K$. En particulier, $K \simeq \mathcal{Z}, a \mapsto diag(a, ..., a)$. △

Hypothèse :
Dans la suite du cours, tous les anneaux sont supposés commutatifs, sauf les anneaux de matrices.

2.3 Premières propriétés

Soit A un anneau (commutatif). On classifie quelques éléments de A :

Définition 2.3.1 - Inversible, régulier, corps, anneau intègre.
Soit $(A, +, \cdot)$ un anneau.

- On dit que $x \in A$ est *inversible* s'il existe $y \in A$ tel que $xy = yx = 1$.
- On dit que $x \in A$ est *régulier* ou *non diviseur de zéro* $xy = 0 \Rightarrow y = 0$.

Un anneau A tel que tout élément non nul est inversible est appelé *corps*.
Un anneau A tel que tout élément non nul est régulier est dit *intègre*.

Remarque. L'ensemble des inversibles de A forme un groupe multiplicatif, noté $(A^\times, \cdot)$. Inversible implique régulier. ♢

Exemples d'anneaux intègres.

1. Tout corps est intègre.
2. Un sous-anneau d'un anneau intègre est intègre.
3. Les anneaux $\mathbb{Z}$ et $\mathbb{Z}[i] \subset \mathbb{C}$ sont intègres.
4. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.
5. L'anneau des polynômes à coefficients dans un corps est intègre.

△

2.4 Anneau des polynômes

Définition 2.4.1 - Anneau des polynômes.
Soit A un anneau.
Nous notons $A[X]$ *l'anneau des polynômes* à coefficients dans A :

$$A[X] = \left\{ \sum_n a_n X^n \mid a_n \in A \text{ et } a_n \text{ presque tous nuls} \right\}$$

(ici, $X^0 := 1$) et l'addition et la multiplication sont données par les formules usuelles

$$\sum_n a_n X^n + \sum_n b_n X^n = \sum_n (a_n + b_n) X^n \quad \text{et} \quad \left(\sum_n a_n X^n\right)\left(\sum_n b_n X^n\right) = \sum_n \left(\sum_{i+j=n} a_i b_j\right) X^n$$

Remarque. L'anneau des coefficients A est un sous-anneau de $A[X]$ par identification via l'injection :

$$\begin{array}{rccc} \iota : & A & \longrightarrow & A[X] \\ & a & \longmapsto & aX^0 \end{array}$$

♢

L'anneau $A[X]$ a une importante propriété universelle :

Théorème 2.4.2 - Propriété universelle de l'anneau des polynômes.
Soit $f : A \to B$ un morphisme d'anneaux et soit $\alpha \in B$.
Alors il existe un unique morphisme :

$$\begin{array}{rccc} f_\alpha : & A[X] & \longrightarrow & B \end{array}$$

avec les propriétés $f_\alpha(a) = f(a) \quad \forall a \in A$ et $f_\alpha(X) = \alpha$.

Démonstration.
Unicité : Si f_α est un tel morphisme, on a :

$$f_\alpha\left(\sum_n a_n X^n\right) = \sum_n f_\alpha\left(a_n X^n\right) = \sum_n f_\alpha(a_n) f_\alpha(X)^n = \sum_n f(a_n)\alpha^n$$

Donc f_α est uniquement déterminé par ces propriétés.

Existence : On définit une application $f_\alpha : A[X] \to B$ par :

$$\forall P \in A[X] : f_\alpha(P) = \sum_n f(a_n)\alpha^n$$

Alors $f_\alpha(X) = \alpha$ et $\forall a \in A : f_\alpha(a) = a$. Vérifions que f_α est un morphisme d'anneaux :

- Préserve l'unité : $f_\alpha(1) = f(1) = 1$.
- Préserve $+$:

$$\begin{aligned} f_\alpha(P+Q) = f_\alpha\left(\sum_n (a_n + b_n) X^n\right) &= \sum_n f(a_n + b_n)\alpha^n \\ &= \sum_n f(a_n) X^n + \sum_n f(b_n)\alpha^n = f_\alpha(P) + f_\alpha(Q) \end{aligned}$$

• Préserve • :

$$\begin{aligned} f_\alpha(PQ) = f_\alpha\left(\sum_n c_n X^n\right) &= \sum_n f_\alpha\left(\sum_{i+j=n} a_i b_j\right)\alpha^n \\ &= \sum_n \sum_{i+j=n} f(a_i) f\big(b_j\big)\alpha^n \\ &= \left(\sum_n f(a_n)\alpha^n\right)\left(\sum_n f(b_n)\alpha^n\right) = f_\alpha(P) f_\alpha(Q) \end{aligned}$$

Ce qui conclut.

Définition 2.4.3 - Évaluation.
Soit A un anneau et $P = \sum_n a_n X^n$ un polynôme de $A[X]$ et $\alpha \in A$.
On appelle *la valeur* de P en α l'élément

$$P(\alpha) := \sum_n a_n \alpha^n \in A$$

Remarque. L'application $A[X] \to A, P \mapsto P(\alpha)$ est le morphisme d'anneaux obtenu par la propriété universelle de $A[X]$ dans le cas $B = A$ et $f = \mathrm{id}$. ♢

Définition 2.4.4 - Coefficient dominant et degré.
Soit A un anneau et P un polynôme nonnul de $A[X]$:

$$P = \sum_{n=0}^{d} a_n X^n \text{ avec } a_d \neq 0$$

On appelle *coefficient dominant* l'élément a_d et *degré* de P l'entier d. On écrit $\deg(P) = d$.
Pour le polynôme nul, on pose $\deg(0) := -\infty$.

Proposition 2.4.5 - Degré d'un produit.
Soit A un anneau. Nous avons alors :

$$\forall f, g \in A[X] : \deg(fg) \leqslant \deg(f) + \deg(g)$$

De plus, si $f \neq 0$ et son coefficient dominant est régulier alors :

$$\forall g \in A[X] : \deg(fg) = \deg(f) + \deg(g)$$

Théorème 2.4.6 - Division euclidiénne dans $A[X]$.
Soit $f, g \in A[X]$ tel que le coefficient dominant de g est inversible. Alors

$$\exists!(q, r) \in A[X]^2 : f = qg + r \text{ avec } \deg(r) < \deg(g)$$

Démonstration.
Unicité : Si $\tilde{q}, \tilde{r}$ vérifient aussi la conclusion alors :

$$qg + r = f = \tilde{q}g + \tilde{r} \text{ d'où } (q - \tilde{q})g = \tilde{r} - r$$

Ainsi $\deg\big((q - \tilde{q})g\big) = \deg(q - \tilde{q}) + \deg(g) = \deg(\tilde{r} - r) < \deg(g)$ (par la proposition precedente).
Donc $q = \tilde{q}$ puis $r = \tilde{r}$.

Existence : On peut supposer $f \neq 0$.
Notons aX^m et bX^n les monômes dominants de f et g. Procédons par récurrence sur m.

- Si $m < n$, on prend $q = 0$ et $r = f$.
- Si $m \geqslant n$, on observe que :

$$gb^{-1}aX^{m-n} = bX^n b^{-1}aX^{m-n} + \ldots = aX^m + \ldots$$

Ainsi $\deg\left(f - gb^{-1}aX^{m-n}\right) < m$ donc par hypothèse de récurrence :

$$f - gb^{-1}aX^{m-n} = \tilde{q}g + r \text{ avec } \deg(r) < \deg(g)$$

On prend $q = \tilde{q} + b^{-1}aX^{m-n}$ et on vérifie que $f = qg + r$.

Définition 2.4.7 - Zéro.
Soit A un anneau et P un polynôme de $A[X]$. Soit $\alpha \in A$.
Si $P(\alpha) = 0$, on dit que α est un *zéro* de P et on peut écrire par division euclidienne :

$$P = (X - \alpha)Q \text{ avec un facteur } Q \in A[X] \text{ qui est uniquement déterminé par} f.$$

Proposition 2.4.8 - Intégrité de $A[X]$.
Soit A un anneau. L'anneau $A[X]$ est intègre si et seulement si A est intègre.

Démonstration. En effet, si $A[X]$ est intègre, ses sous-anneaux sont intègres donc A est intègre.
Réciproquement, si A est intègre, soit deux polynômes P et Q nonnuls de degré n_0 et m_0. Alors :

$$\left(\sum_{n=0}^{n_0} a_n X^n\right)\left(\sum_{m=0}^{m_0} b_m X^m\right) = 0 \Rightarrow a_{n_0}b_{m_0} = 0 \Rightarrow a_{n_0} = 0 \text{ ou } b_{m_0} = 0$$

Ce qui contredit que $\deg(P) = n_0$ et $\deg(Q) = m_0$.

2.5 Corps des fractions

Soit A un anneau intègre.
Nous définissons la relation d'équivalence $\sim$ sur l'ensemble $A \times A \setminus \{0\}$ par :

$$(f, g) \sim \left(\tilde{f}, \tilde{g}\right) \text{ si et seulement si } f\tilde{g} = \tilde{f}g \text{ dans } A.$$

Proposition 2.5.1 - Corps des fractions.
Soit A un anneau intègre.
L'ensemble $\mathrm{Frac}(A)$ des classes d'équivalence de $\sim$ est un corps, muni des lois suivantes :

$$\frac{f}{g} + \frac{\tilde{f}}{\tilde{g}} \overset{\text{def}}{=} \frac{f\tilde{g} + \tilde{f}g}{g\tilde{g}} \quad \text{et} \quad \frac{f}{g} \times \frac{\tilde{f}}{\tilde{g}} \overset{\text{def}}{=} \frac{f\tilde{f}}{g\tilde{g}}$$

Remarque.

- L'élément neutre additif est $\dfrac{0}{1}$, l'élément neutre multiplicatif est $\dfrac{1}{1}$.
- Si $\dfrac{f}{g} \neq 0$ alors $f \neq 0$ et ainsi nous pouvons calculer son inverse $\left(\dfrac{f}{g}\right)^{-1} = \dfrac{g}{f}$.
- Le corps $\mathrm{Frac}(A)$ est appelé *le corps des fractions* de A. On a un morphisme d'anneaux injectif :

$$\begin{array}{rccc} \iota : & A & \longrightarrow & \mathrm{Frac}(A) \\ & a & \longmapsto & \dfrac{a}{1} \end{array}$$

- Si A est déjà un corps, alors ce morphisme est bijectif car :

$$\frac{f}{g} = \frac{fg^{-1}}{1}$$

♢

Exemple de corps des fractions.

- Le corps des fractions des entiers sont les rationnels : $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.
- Si K est un corps, $\mathrm{Frac}\big(K[X]\big) = K(X)$, le corps des fonctions rationnelles sur K.

△

2.6 Produits d'anneaux

Théorème 2.6.1 - Propriété universelle du produit d'anneaux.

Soit $(A_i)_{i\in I}$ une famille d'anneaux.
Le *produit direct* $A = \prod_{i\in I} A_i$ est, comme ensemble, le produit cartésien des A_i. C'est un anneau muni de l'addition et de la multiplication coordonnée par coordonnée. De plus, pour $j \in I$, les projections $\pi_j : \prod_i A_i \to A_j$ sont des morphismes d'anneaux vérifiant la propriété universelle :

Pour tout anneau B et toute famille de morphisme $f_j : B \to A_j$, il existe un unique morphisme $f : B \to \prod_i A_i$ avec tel que le diagramme commute :

$$\begin{array}{ccc} A = \prod_i A_i & \xleftarrow{\exists! f} & B \\ & \searrow^{\pi_j} & \downarrow f_j \\ & & A_j \end{array} \quad \text{tel que :} \quad f_j = \pi_j \circ f$$

Démonstration. On définit $\forall j \in I \forall b \in B : f(b)_j = f_j(b)$.

Cela donne une application $f : B \to \prod_i A_i$ qui rend le diagramme commutatif.
De plus, c'est la seule qui satisfait la condition $f_j = \pi_j \circ f$. Montrons que f est un morphisme :

- Préserve l'unité : $\forall j \in I : f(1_B)_j = f_j(1_B) = 1_{A_j} = (1_A)_j$ d'où $f(1_B) = 1_A$
- Préserve $+$:

$$\forall j \in I : f(a+b)_j = f_j(a+b) = f_j(a) + f_j(b) = f(a)_j + f(b)_j \text{ d'où } f(a+b) = f(a) + f(b)$$

- Préserve $\times$:

$$\forall j \in I : f(ab)_j = f_j(ab) = f_j(a)f_j(b) = f(a)_j f(b)_j \text{ d'où } f(ab) = f(a)f(b)$$

Remarque. Si $A_i = A \quad \forall i$, on écrit A^I au lieu de $\prod_{i\in I} A$. ♢

3. Idéaux

3.1 Définition et opérations sur les idéaux

Définition 3.1.1 - Idéal.
Soit A un anneau (commutatif).
On appelle *idéal* de A tout sous-groupe I de $(A,+)$ absorbant :

$$\forall x \in I, \forall a \in A : ax \in I$$

Exemple d'idéaux.

1. **Idéaux triviaux :** Les ensembles $\{0\}$ et A sont toujours des idéaux de A. Un corps n'a pas d'autres idéaux.
2. **les entiers $\mathbb{Z}$:** les sous-groupes de $\mathbb{Z}$ sont les groupes de la forme $n\mathbb{Z}$ pour $n \geqslant 0$ et ils sont tous absorbant.
3. **Image réciproque :** Si $f : A \to B$ est un morphisme alors $\mathrm{Ker}(f)$ est un idéal de A et plus généralement, l'image réciproque par f d'un idéal de B est un idéal de A.
4. **Intersection :** Si $(I_\lambda)_{\lambda\in\Lambda}$ est une famille d'idéaux de A alors l'intersection $\bigcap_{\lambda\in\Lambda} I_\lambda \subset A$ est un idéal.
   Cela permet de considérer l'*idéal engendré* par une partie S comme le plus petit idéal contenant S. Cet idéal est donc définit par :
   $$\langle S\rangle = \bigcap_{\substack{S\subset I\\ I \text{ idéal}}} I$$
   C'est l'ensemble des combinaison linéaires finies d'éléments de S à coefficients dans A. Ainsi lorsque $S = \{a\}$, l'idéal engendré par S est l'ensemble des multiples de $a \in A$, noté aA, et on dit que c'est un idéal *principal*.
5. **Somme :** Soit $(I_\lambda)_{\lambda\in\Lambda}$ une famille d'idéaux de A. On définit la *somme* de ces idéaux comme l'idéal :
   $$\sum_{\lambda\in\Lambda} I_\lambda = \left\langle \bigcup_{\lambda\in\Lambda} I_\lambda \right\rangle$$
   C'est l'ensemble des sommes finies d'éléments des idéaux I_λ.
6. **Produit :** Soit I et J des idéaux. On définit le *produit* de I et J comme l'idéal :
   $$IJ = \left\langle \left\{ ab \mid a \in I, b \in J \right\} \right\rangle \subset I \cap J$$
   C'est l'ensemble des sommes finies d'éléments de la forme ab avec $a \in I$ et $b \in J$.

△

Définition 3.1.2 - Caractéristique.
Soit A un anneau et $\iota : \mathbb{Z} \to A$ le morphisme canonique.
On appelle *caractéristique* de A, noté $\mathrm{Car}(A)$, l'entier $n \geqslant 0$ tel que $\mathrm{Ker}(\iota) = n\mathbb{Z}$.

Caractéristique des corps connus.

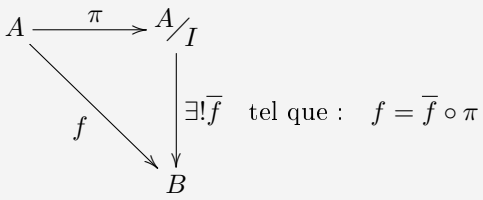
- Les anneaux $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont de caractéristique 0.
- L'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n.
- Un corps fini à $q = p^r$ éléments avec p premier est de caractéristique p.

△

3.2 Anneau quotient

Théorème 3.2.1 - Propriété universelle de l'anneau quotient.
Soit A un anneau et I un idéal différent de A.
Le groupe additif quotient A/I est un anneau par rapport à la loi interne $(x+I)(y+I) := xy+I$ et la projection $\pi : A \to A/I$ est un morphisme d'anneaux. Il satisfait la propriété universelle :

Pour tout anneau B et tout morphisme $f : A \to B$ tel que $I \subset \mathrm{Ker}(f)$, il existe un unique morphisme $\overline{f} : A/I \to B$ tel que le diagramme suivant commute :



Démonstration.
D'après le théorème 1.3.5, il existe un groupe quotient $\left(A/I, +\right)$ et un morphisme de groupes $\pi : A \to A/I$ satisfaisant la propriété universelle au niveau des groupes. Ainsi, il existe un unique morphisme de groupe $\overline{f} : A/I \to B$ satisfaisant $f = \overline{f} \circ \pi$.
La loi

$$(x+I)(y+I) := xy+I$$

est bien défini car I est un idéal : pour $x = x' + a$ et $y = y' + b$:

$$xy + I = \Big(x' + a\Big)\Big(y' + b\Big) + I = x'y' + ay' + x'b + ab + I = x'y' + I$$

On vérifie que $\left(A/I, +, \cdot\right)$ est un anneau et que π et $\overline{f}$ sont des morphismes d'anneaux :

$$\pi(xy) = xy + I = (x+I)(y+I) = \pi(x)\pi(y) \quad \text{et} \quad \pi(1) = 1 + I = 1_{A/I}$$

Notre morphisme de groupe $\overline{f}$ rend le diagramme commutatif et c'est un morphisme d'anneau :

$$\overline{f}\big((x+I)(y+I)\big) = \overline{f}(xy+I) = f(xy) = f(x)f(y) = \overline{f}(x+I)\overline{f}(y+I) \quad \text{et} \quad \overline{f}(1+I) = f(1) = 1$$

Corollaire 3.2.2
Soit A et Q deux anneaux et $f : A \to Q$ un morphisme surjectif.
Alors nous avons l'isomorphisme d'anneaux suivant :

$$A/\mathrm{Ker}\, f \cong Q$$

Démonstration. Pour un morphisme d'anneaux f donné, le théorème 3.2.1 fournit un morphisme d'anneaux

$$\overline{f} : A/\mathrm{Ker}(f) \to Q \text{ avec } f = \overline{f} \circ \pi$$

Il est bijectif, d'après 1.3.6.

3.3 Idéaux principaux et maximaux

On s'intéresse maintenant à certains idéaux importants :

Définition 3.3.1 - Idéal premier et maximal.
Soit A un anneau.

- On appelle idéal *propre* tout idéal différent de A.

- On appelle idéal *premier* tout idéal propre I tel que A/I est intègre :

$$\forall x, y \in A : xy \in I \Rightarrow x \in I \text{ ou } y \in I$$

- On appelle idéal *maximal* tout idéal propre I tel que A/I est un corps :

$$\forall x \notin I, \exists y \in A : xy - 1 \in I$$

Remarque. Tout idéal maximal est donc premier. ♢

Exemple. Dans $\mathbb{Z}$, les idéaux maximaux sont les $p\mathbb{Z}$ avec p premier, les idéaux premiers sont les $p\mathbb{Z}$ avec p premier ou zéro. △

Proposition 3.3.2 - Caractérisation des idéaux maximaux.
Soit A un anneau.
Un idéal propre I est maximal si et seulement s'il n'est contenu dans aucun autre idéal propre.

Pour démontrer l'existence d'idéaux maximaux on a besoin du lemme suivant :

Lemme 3.3.3 - Zorn.
Tout ensemble non vide et inductivement ordonné possède un élément maximal.

Remarque. Le lemme de Zorn est équivalent à l'axiome du choix. ♢

Définition 3.3.4 - Ensemble inductif.
Dans un ensemble $(E, \leqslant)$ partiellement ordonné, on appelle *chaîne* toute partie totalement ordonné $S \subset E$.
Un ensemble E est dit *inductivement ordonné* si chacune de ses chaînes S possède un majorant dans E.

Théorème 3.3.5 - Inclusion dans un idéal maximal.
Soit A un anneau. Tout idéal propre de A est inclus dans un idéal maximal.

Remarque.
En considérant l'idéal $I = \{0\}$ dans le théorème précédent, on obtient que A admet toujours au moins un idéal maximal. De plus, A est un corps si et seulement s'il admet un unique idéal maximal qui est $\{0\}$. ♢

Démonstration. Soit $I \subsetneq A$ un idéal.
Posons E l'ensemble des idéaux propres de A contenant dans I muni de l'inclusion comme ordre partiel. L'ensemble E est non vide et inductivement ordonné. En effet, soit $\{J_\lambda\}_{\lambda \in \Lambda}$ une chaînes de E. Posons :

$$J = \bigcup_{\lambda \in \Lambda} J_\lambda \subset A$$

Alors J est un idéal contenant I et il est propre car sinon $1 \in J$ donc $\exists \lambda : 1 \in J_\lambda$ ce qui est absurde.

Ainsi, $J \subset E$ est un majorant de la chaîne $\{J_\lambda\}_{\lambda \in \Lambda}$.
Par le lemme de Zorn, E contient un élément maximal. C'est un idéal maximal.

Corollaire 3.3.6 - Théorème de Krull.
Tout anneau A contient un idéal maximal.

3.4 Le nilradical

Définition 3.4.1 - nilpotent, nilradical, anneau réduit.
Soit A un anneau (commutatif).
On dit que $x \in A$ est *nilpotent* s'il existe $n \geqslant 0$ tel que $x^n = 0$. On appelle *nilradical* de A l'ensemble $\mathrm{Nil}(A)$ des éléments nilpotents de A.
Si $\mathrm{Nil}(A) = \{0\}$, on dit que A est *réduit*.

Remarque.

- Si $x \in A$ est nilpotent, alors x n'est pas régulier.
- Un anneau intègre est réduit.
- Un sous-anneau d'un anneau réduit est réduit.
- Un produit d'une famille d'anneaux réduits est réduit.

$\diamondsuit$

Lemme 3.4.2 - Structure du nilradical.
Soit A un anneau. Alors le nilradical de A est un idéal de A.

Démonstration. Soit $x, y \in \mathrm{Nil}(A)$.
Il existe m et n tel que $x^m = y^n = 0$ donc :

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

Enfin, $(-x)^m = (-1)^m x^m = 0$ donc $-x \in \mathrm{Nil}(A)$ et si $a \in A$, alors $(ax)^m = a^m x^m = 0$ donc $ax \in \mathrm{Nil}(A)$.

Lemme 3.4.3 - Anneau réduit associé.
Si A est un anneau, ${}^{A}\!/_{\mathrm{Nil}(A)}$ est réduit.

Démonstration. Soit $x + \mathrm{Nil}(A)$ dans le nilradical de ${}^{A}\!/_{\mathrm{Nil}(A)}$. Alors, il existe m tel que $x^m \in \mathrm{Nil}(A)$. Donc, il existe n tel que $x^{mn} = (x^m)^n = 0$. En particulier, $x \in \mathrm{Nil}(A)$.

Proposition 3.4.4 - Forme de Nil(A).
Soit A un anneau.
Alors l'ensemble des éléments nilpotents est l'intersection des idéaux premiers de A :

$$\mathrm{Nil}(A) = \bigcap_{\substack{\mathfrak{p} \subset A \\ \mathfrak{p} \text{ idéal premier}}} \mathfrak{p}$$

Démonstration.
$\subset$: Soit $x \in \mathrm{Nil}(A)$, il existe $n \in \mathbb{N}$ tel que $x^n = 0$. Soit $\mathfrak{p} \subset A$ un idéal premier.
Alors, $x^n = 0 \in \mathfrak{p}$ donc $x \in \mathfrak{p}$ ou $x^{n-1} \in \mathfrak{p}$. Par récurrence, on en déduit que $x \in \mathfrak{p}$.

$\supset$: Soit $x \notin \mathrm{Nil}(A)$. Alors, $0 \notin S = \left\{ x^n \mid n \geqslant 0 \right\} \subset A$. Soit :

$$E = \left\{ I \text{ idéal de } A \mid I \cap S = \varnothing \right\}$$

Nous savons que $E \neq \varnothing$ car $(0) \in E$. L'ensemble E est inductif car si $\{I_\lambda\}_{\lambda \in \Lambda}$ est une chaîne, $I = \bigcup_{\lambda \in \Lambda} I_\lambda$ est un idéal appartenant à E et c'est un majorant de la chaîne.
D'après le lemme de Zorn, E contient un élément maximal, noté $\mathfrak{p}$. En particulier, $x \notin \mathfrak{p}$.

Montrons que $\mathfrak{p}$ est un idéal premier. Supposons que $a \notin \mathfrak{p}$ pour un élément $a \in A$.
Alors $\mathfrak{p} \subset \mathfrak{p} + (a)$. La maximalité de $\mathfrak{p}$ implique que $\mathfrak{p} + (a) \notin E$, donc $S \cap \big(\mathfrak{p} + (a)\big) \neq \varnothing$.

Il existe donc $u \in \mathfrak{p}, v \in A$ et $m \geqslant 0$ tels que :

$$u + va = x^m$$

De même, si $b \notin \mathfrak{p}$ pour un autre élément $b \in A$, on trouve $r \in \mathfrak{p}, t \in A$ et $n \geqslant 0$ tels que :

$$r + tb = x^n$$

Alors :

$$x^{m+n} = x^m x^n = (u+va)(r+tb) = \underbrace{\underbrace{ur}_{\in\mathfrak{p}} + \underbrace{var}_{\in\mathfrak{p}} + \underbrace{tbu}_{\in\mathfrak{p}}}_{\in\mathfrak{p}} + vatb$$

Comme $S \cap \mathfrak{p} = \varnothing$ nous avons $vatb \notin \mathfrak{p}$. De plus, puisque $\mathfrak{p}$ est un idéal, $ab \notin \mathfrak{p}$. Ainsi $\mathfrak{p}$ est donc un idéal premier car pour tout $a, b \notin \mathfrak{p}$ nous avons $ab \notin \mathfrak{p}$.

Corollaire 3.4.5 - Caractérisation des anneaux réduits.
Un anneau A est réduit si et seulement si A s'injecte dans un produit de corps.

Remarque. Rappelons qu'un anneau est intègre si et seulement s'il s'injecte dans un corps.
L'existence d'un tel corps est assuré par le corps des fractions. ♢

Démonstration.
$\Leftarrow$: Si A s'injecte dans un produit de corps, alors A est un sous-anneau d'un anneau réduit.
En effet, les produits d'anneaux réduits sont réduits et les corps est réduits. Ainsi, A est réduit.

$\Rightarrow$: Soit A un anneau réduit. Notons $Spec(A)$ l'ensemble des idéaux premiers dans A.
Pour $\mathfrak{p} \in Spec(A)$, notons :

$$K_{\mathfrak{p}} = \mathrm{Frac}\left(A/\mathfrak{p}\right)$$

Nous lui associons le morphisme d'anneaux $f_{\mathfrak{p}}$:

$$\begin{array}{rccccc} f_{\mathfrak{p}}: & A & \xrightarrow{\pi_{\mathfrak{p}}} & A/\mathfrak{p} & \xhookrightarrow{i_{\mathfrak{p}}} & K_{\mathfrak{p}} \\ & a & \longmapsto & \overline{a} & \longmapsto & \dfrac{\overline{a}}{1} \end{array}$$

Considérons le morphisme d'anneaux φ suivant :

$$\begin{array}{rccc} \varphi: & A & \longrightarrow & \displaystyle\prod_{\mathfrak{p}\in Spec(A)} K_{\mathfrak{p}} \\ & a & \longmapsto & \left(f_{\mathfrak{p}}(a)\right)_{\mathfrak{p}\in Spec(A)} \end{array}$$

Ce morphisme a pour noyau $\displaystyle\bigcap_{\mathfrak{p}\in Spec(A)} \mathfrak{p} = \mathrm{Nil}(A) = \{0\}$ donc le morphisme est injectif ce qui conclut.

4. Modules

4.1 Définition d'un module

Soit A un anneau toujours supposé commutatif.

Définition 4.1.1 - A-Module.
Un A-**module** est une groupe abélien M muni d'une application (appelé *multiplication scalaire*)

$$\begin{array}{rccc} \bullet : & A \times M & \longrightarrow & M \\ & (a, x) & \longmapsto & a \bullet x \end{array}$$

telle que cette application vérifie :

- Stabilité par l'identité : $\forall x \in M : 1_A x = x$.
- L'associativité mixte : $\forall a, b \in A, \forall x \in M : (a \bullet b) \bullet x = a \bullet (b \bullet x)$.
- La distributivité mixte : $\forall a, b \in A, \forall x, y \in M :$

$$a \bullet (x + y) = a \bullet x + a \bullet y \quad \text{et} \quad (a + b) \bullet x = a \bullet x + b \bullet x$$

Remarque. On écrit souvent ax au lieu de $a \bullet x$.

♢

Discutions autour du morphisme.
Soit M un groupe abélien et $\mathrm{End}(M)$ l'ensemble des morphismes de groupes de M dans M.
Muni de l'addition et de la composition, c'est un anneau, généralement non commutatif.
Si M est, de plus, un A-module, considérons :

$$\begin{array}{rccc} \gamma_a : & M & \longrightarrow & M \\ & x & \longmapsto & a \bullet x \end{array}$$

L'axiome de distributivité mixte à gauche implique que $\gamma_a \in \mathrm{End}(M)$.
Les trois autres axiomes impliquent que

$$\begin{array}{rccc} \gamma : & A & \longrightarrow & \mathrm{End}(M) \\ & a & \longmapsto & \gamma_a \end{array}$$

est un morphisme d'anneau.

Réciproquement, si M est un groupe abélien avec un morphisme d'anneau $\gamma : A \to \mathrm{End}(M)$, on définit :

$$\forall a \in A, \forall x \in M : a \bullet x := \gamma_a(x)$$

Ceci muni le groupe abélien M d'une structure de A-module.
Ainsi, les différentes structures de A-modules sur un groupe abélien M donné sont en bijection avec les morphismes d'anneaux entre A et $\mathrm{End}(M)$. ♢

Exemples de modules.

1. **Module zéro et l'anneau :** Les groupes abéliens $\{0\}$ et A sont des A-modules (le dernier par rapport à la multiplication dans A).
2. **Les espaces vectoriels :** Si $A = K$ est un corps, les notions de A-module et de K-espace vectoriel coïncident. Beaucoup de notions pour les espaces vectoriels se généralisent directement à des modules (voir au-dessous).
3. **Les groupes abéliens :** Si $A = \mathbb{Z}$, les notions de $\mathbb{Z}$-module et de groupe abélien coïncident.

En effet, si M est un groupe abélien, il n'y a qu'une manière de définir une structure de $\mathbb{Z}$-module sur M, à savoir en posant, pour $n > 0$,

$$n \cdot x := \underbrace{x + \ldots + x}_{n \text{ fois}} \in A$$

et $n \cdot x := -\big((-n) \cdot x\big)$ pour $n < 0$. Ainsi, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{R}$ sont des $\mathbb{Z}$-modules.

4. **Restriction des scalaires :** Soit $f : A \to B$ un morphisme d'anneaux et M un B-module. Alors M est muni d'une structure de A-module définie par :

$$\forall a \in A, \forall x \in M : a \cdot x = f(a)x$$

Nous avons alors toutes les bonnes propriétés, par exemple :

$$a \cdot (x + y) = f(a)(x + y) = f(a)x + f(a)y = a \cdot x + a \cdot y$$

△

4.2 Sous-module et morphisme de modules

On peut généraliser les notions de sous-espace et d'application linéaire pour les espaces vectoriels à des modules.

Définition 4.2.1 - Sous-A-module.
Soit A un anneau et M un A-module.
On appelle *sous-A-module* de M tout sous-groupe M' de M tel que :

$$\forall a \in A, \forall x \in M' : ax \in M'$$

En particulier, M' est un A-module.

Exemples.

1. **Sous-modules d'anneau :** Les sous-modules d'un anneaux A vu comme A-module sont exactement les idéaux de A.
2. **Image réciproque :** Soit $f : M \to N$ un morphisme. Les groupes $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont des sous-modules. Plus généralement, l'image réciproque d'un sous-module de N par f est un sous-module de M.
3. **Intersection :** Si $(M_\lambda)_{\lambda \in \Lambda}$ est une famille de sous-A-modules de M alors l'intersection $\bigcap_{\lambda \in \Lambda} M_\lambda \subset M$ est un sous-module.
4. **Sous-module engendré :** Soit M un A-module et $S \subset M$ une partie de M. Le sous-module

$$\langle S \rangle = \bigcap_{\substack{S \subset N \\ N \text{ sous-module}}} N$$

est appelé le *sous-module engendré par S*. Il est le plus petit sous-module de M contenant S et ces éléments sont des sommes finies de as avec $a \in A$ et $s \in S$. Si $\langle S \rangle = M$ on dit que M est *engendré par S*.

△

Définition 4.2.2 - Morphisme de A-modules.
Soit A un anneau et M, N deux A-modules.
On appelle *morphisme de A-modules* ou *application A-linéaire* tout morphisme de groupes f tel que :

$$\forall a \in A, \forall x \in M : f(ax) = af(x)$$

On note $\mathrm{Hom}_A(M, N)$ l'ensemble des morphismes de A-modules de M dans N.
On appelle **isomorphisme** tout morphisme bijectif. Dans ce cas, l'application inverse est aussi un morphisme.

Proposition 4.2.3 - Groupe des morphismes de A-modules.
L'ensemble des morphismes de A-modules est un groupe abélien pour la somme.
Car A est commutatif, $\mathrm{Hom}_A(M,N)$ peut être, de plus, muni d'une structure de A-modules en lui associant :

$$\forall b \in A, \forall x \in M : (bf)(x) = bf(x)$$

Démonstration. Soit $f \in \mathrm{Hom}_A(M,N)$. Vérifions que $bf \in \mathrm{Hom}_A(M,N)$. Puisque A est commutatif :

$$\begin{aligned}\forall x,y \in M, \forall a,b \in A : (bf)(ax+y) &= bf(ax+y)\\ &= bf(ax)+bf(y)\\ &= baf(x)+bf(y) = abf(x)+bf(y) = a(bf)(x)+bf(y)\end{aligned}$$

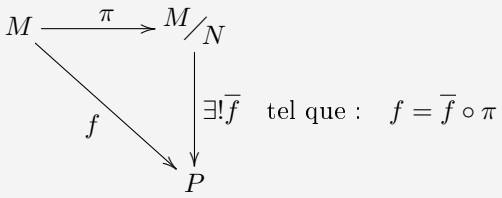
Ainsi, $bf : M \to N$ est A-linéaire. Les axiomes se vérifient facilement.

4.3 Module quotient

On peut généraliser la notion d'un espace vectoriel quotient (par rapport à un sous-espace vectoriel) à des modules.

Théorème 4.3.1 - Propriété universelle du module quotient.
Soit M un A-module et N un sous-module M.
Le groupe abélien quotient ${}^{M}\!/_{N}$ et un A-module par rapport à la multiplication scalaire $a \cdot (m+N) := am+N$ et la projection $\pi : M \to {}^{M}\!/_{N}$ est A-linéaire. Il satisfait la propriété universelle :

Pour tout module P et tout morphisme $f : M \to P$ tel que $N \subset \mathrm{Ker}(f)$, il existe un unique morphisme $\overline{f} : {}^{M}\!/_{N} \to P$ tel que le diagramme suivant commute :



De plus, N est un sous-module de $\mathrm{Ker}\,(f)$ et $\mathrm{Ker}\,(\overline{f}) = {}^{\mathrm{Ker}(f)}\!/_{N}$.

Démonstration. Le théorème 1.3.5 donne le groupe abélien ${}^{M}\!/_{N}$ et le morphisme de groupes π.
L'application

$$\forall a \in A, \forall \overline{x} \in {}^{M}\!/_{N} : a\overline{x} = \overline{ax}$$

est bien défini car $N \subset M$ est un sous-module. Muni de cette multiplication scalaire, ${}^{M}\!/_{N}$ est un A-module et π est A-linéaire.
Pour un morphisme de A-modules f donné, le théorème 1.3.5 fournit un morphisme de groupes $\overline{f}$ rendant le diagramme commutatif.
Montrons que ce $\overline{f}$ est A-linéaire. On a $\overline{f}(x+N) = f(x)$ donc pour $a \in A$:

$$\overline{f}\big(a(x+N)\big) = \overline{f}(ax+aN) = \overline{f}(ax+N) = f(ax) = af(x) = a\overline{f}(x+N)$$

Corollaire 4.3.2
Soient M et Q deux A-modules et $f : M \to Q$ un morphisme surjectif.
Alors nous avons l'isomorphisme suivant :

$${}^{M}\!/_{\mathrm{Ker}\, f} \cong Q$$

Démonstration. D'après le théorème 4.3.1, on a un morphisme

$$\overline{f} : {}^{M}\!/_{\mathrm{Ker}(f)} \to Q \text{ avec } f = \overline{f} \circ \pi$$

Il est bijectif, d'après 1.3.6.

4.4 Produit direct et somme directe de A-modules.

On peut généraliser les notions de produit et sommes directs pour les espaces vectoriels à des familles quelconques de A-modules.

Définition 4.4.1 - Produit direct et somme direct.
Soit I un ensemble, A un anneau et $(M_i)_{i\in I}$ une famille de A-modules.

- Le **produit direct** des M_i est l'ensemble produit cartésien des M_i noté $\prod_{i\in I} M_i$.
- La **somme directe** des M_i est le sous-module de $\prod_{i\in I} M_i$ composé des familles $(x_i)_{i\in I}$ dont tous les termes sont nuls sauf un nombre fini. On le note $\bigoplus_{i\in I} M_i$.

Dans les deux cas, la structure de A-module est définie coordonnées par coordonnées, c'est-à-dire, $(x_i)_i + (y_i)_i := (x_i + y_i)_i$ et $a(x_i)_i := (ax_i)_i$.

Remarque. L'inclusion

$$\iota : \bigoplus_{i\in I} M_i \hookrightarrow \prod_{i\in I} M_i$$

est surjectif si et seulement si il n'y a qu'un nombre fini de M_i non nuls.

Si $M_i = A \quad \forall i$, on écrit $A^{(I)} := \oplus_i M_i$ et $A^I := \prod_i M_i$. ♢

Le produit direct et la somme directe de A-modules vérifient les propriétés universelles suivantes :

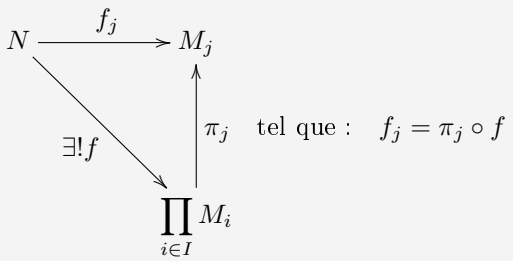
Théorème 4.4.2 - Propriété universelle du produit direct de modules.
Soit $(M_i)_{i\in I}$ une famille de A-modules.
Pour tout $j \in I$, on pose π_j la projection sur le j^{e} coefficient.

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

Ces morphismes vérifient la propriété universelle suivante :
Pour tout A-module N et tout famille de morphisme $f_j : N \to M_j$, il existe un unique morphisme :

$$f : N \to \prod_{i\in I} M_i$$

Tel que le diagramme suivant commute :



tel que : $f_j = \pi_j \circ f$

Démonstration. On définit $\forall j \in I, \forall x \in N : f(x)_j = f_j(x)$.
Cela donne une application $f : M \to \prod_i M_i$ qui rend le diagramme commutatif.

De plus, c'est la seule qui satisfait la condition $f_j = \pi_j \circ f$. Montrons que f est une application A-linéaire :

$$\begin{aligned}\forall a \in A, \forall x, y \in M, \forall j \in I : f(ax+y)_j &= f_j(ax+y) \\ &= af_j(x) + f_j(y) = af(x)_j + f(y)_j \text{ d'où } f(ax+y) = af(x) + f(y)\end{aligned}$$

Théorème 4.4.3 - Propriété universelle de la somme directe de modules.

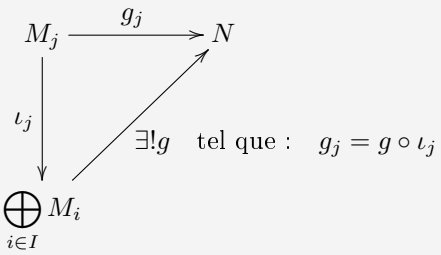
Soit $(M_i)_{i\in I}$ une famille de A-modules.
Pour tout $j \in I$, on pose ι_j l'injection du j^e coefficient.

$$\begin{array}{rccc} \iota_j : & M_j & \longrightarrow & \bigoplus_{i\in I} M_i \\ & x & \longmapsto & (0,\ldots,0,\underset{\substack{\uparrow \\ j^e \text{ coord.}}}{x},0,\ldots,0) \end{array}$$

Ces morphismes vérifient la propriété universelle suivante :
Pour tout A-module N et toute famille de morphisme $g_j : M_j \to N$ il existe un unique morphisme :

$$g : \bigoplus_{i\in I} M_I \to N$$

Tel que le diagramme suivant commute :



Démonstration. On définit $\forall j \in I, \forall x = (x_i)_i \in \bigoplus_i M_i : g(x) := \sum_{i\in I} g_i(x_i)$.

Cela donne une application $g : \bigoplus_i M_i \to N$ qui rend le diagramme commutatif.
De plus, c'est la seule qui satisfait la condition $g_j = g_j \circ \iota_j$. Montrons que g est une application A-linéaire :

$$\begin{aligned}\forall a \in A, \forall x, y \in \bigoplus_i M_i : g(ax+y) &= \sum_{i\in I} g_i(ax_i + y_i) \\ &= \sum_{i\in I} ag_i(x_i) + g_i(y_i) = ag(x) + g(y) \text{ d'où } g(ax+y) = ag(x) + g(y)\end{aligned}$$

Définition 4.4.4 - Somme des sous-modules.

Soit $(M_i)_{i\in I}$ une famille de sous-modules de M.
On appelle *somme* des M_i le plus petit sous-module de M qui contient tous les M_i. On le note $\sum_{i\in I} M_i$.

C'est l'image du morphisme $g : \bigoplus_{i\in I} M_i \to M$ associé à la famille $g_j : M_j \hookrightarrow M$.

5. Modules libres

Soit A un anneau toujours supposé commutatif. On peut généraliser les notions d'indépendance linéaire, de famille génératrice et de base pour les espaces vectoriels à des A-modules.

5.1 Définition d'un module libre

Définition 5.1.1 - Module libre.
Soit A un anneau et I un ensemble.
On appelle *A-module libre standard de base I* le A-module :

$$A^{(I)} = \bigoplus_{i \in I} A$$

Pour tout $i \in I$, on note $e_i \in A^{(I)}$ l'élément $(0, \dots, 0, \underset{\substack{\uparrow \\ i^e \text{ coord.}}}{1}, 0, \dots, 0)$.

Le A-module libre $A^{(I)}$ a une importante propriété universelle.

5.2 Famille libre, génératrice, base

Proposition 5.2.1 - Propriété universelle d'un module libre.
Soit A un anneau et M un A-module.
Pour toute famille $x = (x_i)_{i \in I}$ d'éléments de M, il existe un unique morphisme de A-modules

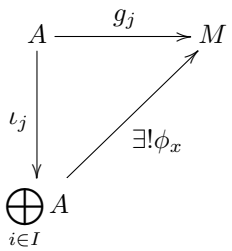
$$\phi_x : A^{(I)} \to M$$

avec la propriété $\phi_x(e_i) = (x_i) \quad \forall i$.

Démonstration. Nous appliquons la propriété universelle de la somme directe pour la famille :

$$\forall j \in I : \quad g_j : \begin{array}{ccc} A & \longrightarrow & M \\ a & \longmapsto & ax_j \end{array}$$

ce qui nous donne le diagramme suivant :



Remarque. On a $\phi_x\left(\sum_i a_i e_i\right) = \sum a_i x_i$ pour des coefficients $a_i \in A$ presque tous nuls. L'ensemble $\mathrm{Im}(\phi_x)$ est donc le sous-module $\langle x \rangle$ de M engendré par les x_i. ♢

Définition 5.2.2 - Famille libre, génératrice et base.
Soit ϕ_x le morphisme associé à $x = (x_i)_{i \in I}$ définit dans 5.2.1.
On dit que :

- La famille x est *libre* si le morphisme ϕ_x est injectif : $\sum_i a_i x_i = 0 \Rightarrow a_i = 0 \quad \forall i$.

- La famille x est *génératrice* si le morphisme ϕ_x est surjectif : $M = \langle x \rangle$.
- La famille x est une *base* si le morphisme ϕ_x est bijectif.

Dans le dernier cas, on dit que M est *libre* de base x.

Remarque. On a les équivalences suivantes :

1. Un A-module M est libre si et seulement s'il existe un ensemble I tel que $M \cong A^{(I)}$.
2. Une famille est libre si et seulement si toutes ses sous-familles sont libres.

♢

Remarque. Attention ! Un partie libre maximale n'est pas nécessairement une base.
De même une partie génératrice minimale n'est pas nécessairement une base.

- Si on prend $A = \mathbb{Z}$, $M = \mathbb{Z}$ et $x = \{2\}$ est une famille libre maximale dans M, mais pas une base.
- Si on prend $A = \mathbb{Z}$, $M = \mathbb{Z}$ et $x = \{2, 3\}$ est une famille génératrice minimale dans M, mais pas une base.

♢

Remarque. Si $A = K$ est un corps, tout K-espace vectoriel admet une base et donc, est libre. ♢

Exemple de modules libres. La plupart des modules ne sont pas libres.

- Le $\mathbb{Z}-$module $\mathbb{Z}/n\mathbb{Z}$ n'est pas libre, pour $n > 1$ cet si on suppose que $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}^{(I)}$, alors l'application suivante doit être nulle ce qui est absurde :

$$\begin{array}{rccc} \bullet_n : & \mathbb{Z}^{(I)} & \longrightarrow & \mathbb{Z}^{(I)} \\ & x & \longmapsto & nx \end{array}$$

- Le $\mathbb{Z}-$module $\mathbb{Q}$ n'est pas libre (exercice).
- Le A-module A est libre par définition (et il admet 1_A comme base).
- Le A-module des polynômes $A[X]$ est libre, une base est donnée par $\{X^n\}_{n \geqslant 0}$.

△

5.3 Modules de type fini

Définition 5.3.1 - Module de type fini.
Un A-module M est de type fini s'il admet une partie génératrice finie :

$$\exists \{x_1, \ldots, x_n\} \subset M : \quad M = Ax_1 + \cdots + Ax_n$$

Remarque.

1. M est de type fini si et seulement s'il existe un morphisme surjectif $\varphi : A^n \to M$.
2. Soit N est un sous-module de M. Alors :
   - Si M est de type fini alors M/N est de type fini.
   - Si N et M/N sont de type fini alors M est de type fini (exercice).

♢

Lemme 5.3.2 - Base finie.
Soit M un A-module libre de base $(e_i)_{i \in I}$. Si M est de type fini, alors l'ensemble I est fini.

Démonstration. Soit $Ax_1 + \cdots + Ax_r = M$.
Pour tout $j \in \{1, \ldots, r\}$ on définit une suite $a_i^{(j)}$ dans A via $x_j = \sum_{i \in I} a_i^{(j)} e_i$. Alors

$$\mathscr{J} = \left\{ i \in I \;\middle|\; \exists j \in \{1, \ldots, r\} : a_i^{(j)} \neq 0 \right\}$$

est un ensemble fini.
Nous avons :

$$M = \sum_{j=1}^{r} Ax_j \subseteq \sum_{j\in\mathscr{J}} Ae_j = \bigoplus_{j\in\mathscr{J}} Ae_j \subseteq \bigoplus_{i\in I} Ae_i = M$$

Donc on a égalité partout, en particulier $\bigoplus_{\mathscr{J}} Ae_i = \bigoplus_{I} Ae_i$ c'est-à-dire $I = \mathscr{J}$ est fini.

Lemme 5.3.3 - Égalité du rang.
Soit A^r et A^s deux A-modules. Si $A^r \cong A^s$, alors $s = r$.

Démonstration. D'après le théorème de Krull 3.3.6, il existe un idéal maximal $\mathfrak{m} \subset A$.
Considérons le sous-module $\mathfrak{m}A^r \subseteq A^r$ engendré par les mx avec $m \in \mathfrak{m}$ et $x \in A^r$.

Soit maintenant $\varphi : A^r \cong A^s$ l'isomorphisme de l'hypothèse.
L'application φ est A-linéaire, donc $\varphi(\mathfrak{m}A^r) = \mathfrak{m}A^s$ et ainsi φ induit un isomorphisme :

$$\overline{\varphi} : {}^{A^r}\!/_{\mathfrak{m}A^r} \xrightarrow{\sim} {}^{A^s}\!/_{\mathfrak{m}A^s}$$

Mais $\mathfrak{m}A^r = \mathfrak{m}^r$ et $\mathfrak{m}A^s = \mathfrak{m}^s$ car $\mathfrak{m}$ est un idéal de A.
Ainsi, en posant K le corps ${}^{A}\!/_{\mathfrak{m}}$, nous observons que $\overline{\varphi} : K^r \to K^s$ est K-linéaire.
La théorie de la dimension pour les espaces vectoriel sur K permet de conclure que $r = s$.

Remarque. La commutativité de A est essentielle à la démonstration de ce resultat. ♢

Définition 5.3.4 - Rang d'un A-module.
Soit M un A-module libre de type fini.
On appelle *rang* de M l'unique entier $r \in \mathbb{N}$ tel que $M \cong A^r$.

Remarque. Ceci est bien définit car nous venons de montrer l'unicité de l'entier r dans le lemme précédent. ♢

6. Algèbre des matrices

6.1 Introduction

De nombreux concepts et résultats d'algèbre linéaire sur les applications linéaires associé à un corps de base restent valable pour les morphismes de modules libres de type fini sur un anneau commutatif quelconque. On discute dans la suivante le calcul matriciel et la théorie du déterminant.

6.2 Algèbres

Une A-algèbre est un A-module et un anneau tel que la multiplication interne et externe soient compatibles. Plus précisément :

Définition 6.2.1 - A-algèbre.
Soit A un anneau commutatif et B un anneau quelconque.
On appelle B un A-algèbre, si B est un A-module tel que la multiplication $\cdot$ dans l'anneau B soit A-bilinéaire :

- Linéarité à gauche : $\forall \lambda \in A, x, y, z \in B : (\lambda x + y) \cdot z = \lambda(x \cdot z) + y \cdot z$
- Linéarité à droite : $\forall \lambda \in A, x, y, z \in B : x \cdot (\lambda y + z) = \lambda(x \cdot y) + x \cdot z$

Proposition 6.2.2
Soit A un anneau commutatif et $(B, +, \cdot)$ un anneau.
La donnée d'une structure de A-algèbre sur B est équivalente à la donnée d'un morphisme d'anneaux $f : A \to B$ tel que $\mathrm{Im}(f) \subseteq \mathcal{Z}(B)$. La multiplication scalaire alors est donnée par la formule :

$$\forall a \in A, \forall b \in B : ab := f(a) \cdot b$$

Remarque. Ainsi, nous pouvons identifier une A-algèbre commutative B à la simple donnée d'un morphisme d'anneaux $A \to B$. ♢

Démonstration. Soit B une A-algèbre. On note $\cdot$ pour la multiplication dans l'anneau B. Soit $f : A \to B$ définie par :

$$\forall a \in A : f(a) := a1_B$$

D'après la distributivité mixte, f est un morphisme de groupes abélien.
De plus $\forall x, y \in A$:

$$f(xy) = (xy)1_B = (xy)(1_B \cdot 1_B) = x\big(y(1_B \cdot 1_B)\big) = x\big(1_B \cdot (y1_B)\big) = (x1_B) \cdot (y1_B) = f(x) \cdot f(y)$$

Et enfin $f(1_A) = 1_A 1_B = 1_B$, d'après l'axiome $1_A x = x$. Ainsi f est un morphisme d'anneaux.
Vérifions que $\mathrm{Im}(f) \subset \mathcal{Z}(B)$:

$$\forall a \in A, \forall b \in B : f(a) \cdot b = (a1_B) \cdot b = a(1_B \cdot b) = a(b \cdot 1_B) = b \cdot (a1_B) = b \cdot f(a)$$

Ce qui vérifie que $\mathrm{Im}(f) \subset \mathcal{Z}(B)$.

Réciproquement, soit $f : A \to B$ un morphisme d'anneaux tel que $\mathrm{Im}(f) \subset \mathcal{Z}(B)$.
On a vu que B est un A-module si l'on définie la multiplication extérieure par :

$$\forall a \in A, \forall b \in B : ab := f(a) \cdot b$$

De plus, comme $\mathrm{Im}(f) \subset \mathcal{Z}(B)$, la multiplication $\cdot : B \times B \to B$ est A-bilinéaire, c'est-à-dire que B est une A-algèbre.

Exemples d'algèbres.

1. L'ensemble des polynômes à coefficients dans A, noté $A[X]$ est une A-algèbre commutative, le morphisme d'anneaux associé est l'inclusion $A \hookrightarrow A[X]$.
2. Tout anneau B est une $\mathbb{Z}$-algèbre, le morphisme d'anneaux correspondant étant le morphisme unique $\iota : \mathbb{Z} \to B$ tel que $\iota(n) = \underbrace{1_B + \ldots + 1_B}_{n \text{ fois}}$ pour $n > 0$.
3. Un anneau de matrices sur A est une A-algèbre.
   Plus généralement, l'anneau $\mathrm{End}_A(M) = \mathrm{Hom}_A(M, M)$ des endomorphismes d'un A-module M est une A-algèbre (voir au-dessous).

△

6.3 Notation matricielle

Soit r, s et t des entiers supérieurs à 1 et A un anneau commutatif.
Le groupe additif usuel de matrices $\mathcal{M}_{r,s}(A)$ est muni d'une structure de A-module définie par :

$$\forall a \in A, \forall X = \big(a_{i,j}\big) \in \mathcal{M}_{r,s}(A) : \quad aX = a\big(a_{i,j}\big)_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant s}} = \big(aa_{i,j}\big)_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant s}}$$

Le produit matriciel $\bullet : \mathcal{M}_{r,s}(A) \times \mathcal{M}_{s,t}(A) \to \mathcal{M}_{r,t}(A)$ est bilinéaire.
En particulier, l'ensemble des matrices carrées $\mathcal{M}_r(A) = \mathcal{M}_{r,r}(A)$ est une A-algèbre.

Dans ce qui suit, on considère des tuplets (E, e) où E est un A-module libre de type fini de base $e = \{e_1, \ldots, e_r\}$. Nous avons donc en particulier $r = \mathrm{Rk}(E)$.

Définition 6.3.1 - Matrice d'une application A-linéaire.
Soit (E, e) et (F, f) ou $r = \mathrm{Rk}(E)$ et $s = \mathrm{Rk}(F)$ et un morphisme de A-modules $u : E \to F$.
Nous posons :

$$\forall j \in \{1, \ldots, r\} : u\big(e_j\big) = \sum_{i=1}^{s} u_{i,j} f_i \text{ avec } u_{i,j} \in A$$

On appelle *matrice de u dans les bases e et f* la matrice $\big(u_{i,j}\big)_{i,j} \in \mathcal{M}_{s,r}$ que l'on note $\mathrm{Mat}_{e,f}(u)$.

Remarque. Si $E = F$ et $e = f$ on note $\mathrm{Mat}_e(u)$ au lieu de $\mathrm{Mat}_{e,f}(u)$. ♢

Comme dans le cas d'un corps, on a un isomorphisme de A-modules entre les morphismes de E dans F et les matrices de taille $s \times r$:

Proposition 6.3.2 - Isomorphisme des matrices et applications A-linéaires.
Soit (E, e) et (F, f). Nous avons l'isomorphisme suivant :

$$\begin{array}{rccc} \mathrm{Mat} : & \mathrm{Hom}_A(E, F) & \longrightarrow & \mathcal{M}_{s,r}(A) \\ & u & \longmapsto & \mathrm{Mat}_{e,f}(u) \end{array}$$

Si $E = F$ et $e = f$ on a un isomorphisme de A-algèbres $\mathrm{End}_A(M) \cong \mathcal{M}_r(A)$.

Proposition 6.3.3 - Composition d'applications A-linéaires.
Soit (E, e), (F, f), (G, g) et deux morphisme de A-modules $u : E \to F$ et $v : F \to G$.
Alors la matrice de la composition $v \circ u$ vérifie :

$$\mathrm{Mat}_{e,g}(v \circ u) = \mathrm{Mat}_{f,g}(v) \bullet \mathrm{Mat}_{e,f}(u) \tag{6.1}$$

6.4 Matrice de passage

La relation (6.1) permet de lier les matrices associées à un même endomorphisme dans des bases différentes.

Définition 6.4.1 - Matrice de passage.
Soit E un A-module libre de type finis et e, e' deux bases de E.

On appelle *matrice de passage* de e à e' la matrice :

$$P_e^{e'} = \mathrm{Mat}_{e',e}(\mathrm{id}_E)$$

Remarque. En appliquant la relation précédente à la composée $(E,e) \xrightarrow{\mathrm{id}} (E,e') \xrightarrow{\mathrm{id}} (E,e)$ on obtient que $1 = P_e^{e'} P_{e'}^{e}$ et donc $P_e^{e'}$ et $P_{e'}^{e}$ sont inversibles. ♢

Proposition 6.4.2 - Formule de changement de base.
Soit $u : E \to F$ une application A-linéaire entre E et F deux modules libres de type fini.

- Soit e et e' deux bases de E et $P = P_e^{e'}$.
- Soit f et f' deux bases de F et $Q = P_f^{f'}$.

Alors nous avons la formule de changement de base pour u :

$$\mathrm{Mat}_{e',f'}(u) = Q^{-1}\,\mathrm{Mat}_{e,f}(u)P$$

Si $E = F$, $e = f$ et $e' = f'$, on a simplement :

$$\mathrm{Mat}_{e'}(u) = P^{-1}\,\mathrm{Mat}_{e}(u)P$$

Démonstration. Il suffit d'appliquer la relation (6.1) à la composée :

$$\left(E,e'\right) \xrightarrow{\mathrm{id}} (E,e) \xrightarrow{u} (F,f) \xrightarrow{\mathrm{id}} \left(F,f'\right)$$

6.5 Déterminant

On considère maintenant la notion de déterminant.

Définition 6.5.1 - Signature.
Soit σ une permutation, un élément du groupe symétrique $\mathfrak{S}_n$.
On appelle signature de σ l'entier $\varepsilon(\sigma) \in \{-1,1\}$ défini par :

$$\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}$$

L'application $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un morphisme de groupes.

Définition 6.5.2 - Déterminant.
Soit A un anneau commutatif, et $B \in \mathcal{M}_n(A)$.
On appelle *déterminant de* B l'élément de A, noté $\det(B)$, défini par :

$$\det(B) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) b_{1,\sigma(1)} \dots b_{n,\sigma(n)}$$

Proposition 6.5.3 - Transposée du déterminant.
Soit $B \in \mathcal{M}_n(A)$ et B^t la transposée de B.
Le déterminant de la transposée de B est le déterminant de B :

$$\det\left(B^t\right) = \det(B)$$

Démonstration.

Il suffit d'écrire :

$$\begin{aligned}\det\Big(B^t\Big) &= \sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)b_{\sigma(1),1}\dots b_{\sigma(n),n}\\ \text{En posant : } \tau=\sigma^{-1} \quad &= \sum_{\tau\in\mathfrak{S}_n}\varepsilon\Big(\tau^{-1}\Big)b_{1,\tau(1)}\dots b_{n,\tau(n)}\\ &= \det(B)\end{aligned}$$

Lemme 6.5.4 - Forme n-linéaire alternée.
Le déterminant est une forme n-linéaire alterné en les lignes et les colonnes de B.

Démonstration. D'après la proposition précédente, il suffit de considérer les lignes.
La multilinéarité est évidente. Supposons que B possède deux lignes égales d'indices u et v.
Soit $\tau=(u\ v)$ la transposition qui échange u et v dans $\mathfrak{S}_n$. Nous avons une partition :

$$\mathfrak{S}_n=\mathfrak{A}_n\sqcup\mathfrak{A}_n\tau \text{ où } \mathfrak{A}_n=\mathrm{Ker}(\varepsilon)$$

Ainsi :

$$\det(B)=\sum_{\sigma\in\mathfrak{A}_n}\varepsilon(\sigma)b_{1,\sigma(1)}\dots b_{n,\sigma(n)}+\sum_{\sigma\in\mathfrak{A}_n}\varepsilon(\sigma\tau)b_{1,\sigma\tau(1)}\dots b_{n,\sigma\tau(n)}$$

Or nous savons que $b_{u,\sigma\tau(u)}b_{v,\sigma\tau(v)}=b_{u,\sigma(u)}b_{v,\sigma(v)}$ et si $i\notin\{u,v\}$ alors $b_{i,\sigma(i)}=b_{i,\sigma\tau(i)}$.
Ainsi :

$$\det(B)=\sum_{\sigma\in\mathfrak{A}_n}\varepsilon(\sigma)b_{1,\sigma(1)}\dots b_{n,\sigma(n)}-\sum_{\sigma\in\mathfrak{A}_n}\varepsilon(\sigma)b_{1,\sigma(1)}\dots b_{n,\sigma(n)}=0$$

Théorème 6.5.5 - Déterminant d'un produit.
Soit B et C deux matrices de taille n à coefficient dans A.
Alors :

$$\det(BC)=\det(B)\det(C)$$

Démonstration. Notons $\mathscr{F}_n$ l'ensemble des fonction de $\{1,\dots,n\}$ dans lui-même.
Écrivons $C=\big(c_{i,j}\big)_{i,j}$. Soit $\tau\in\mathscr{F}_n$. Notons C_τ la matrice de coefficients $c_{\tau(i),j}$.
Si τ n'est pas injectif alors C_τ possède deux lignes égales et $\det C_\tau=0$.

Nous avons donc :

$$\begin{aligned}\det(BC) &= \sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\prod_{i=1}^n\sum_{k=1}^n b_{i,k}c_{k,\sigma(i)}\\ &= \sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\sum_{\tau\in\mathcal{F}_n}\prod_{i=1}^n b_{i,\tau(i)}c_{\tau(i),\sigma(i)}\\ &= \sum_{\tau\in\mathcal{F}_n}\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\prod_{i=1}^n b_{i,\tau(i)}c_{\tau(i),\sigma(i)}\\ &= \sum_{\tau\in\mathcal{F}_n}\prod_{i=1}^n b_{i,\tau(i)}\underbrace{\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\prod_{i=1}^n c_{\tau(i),\sigma(i)}}_{=\det\left(C_\tau\right)}\\ &= \sum_{\tau\in\mathfrak{S}_n}\prod_{i=1}^n b_{i,\tau(i)}\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\prod_{i=1}^n c_{\tau(i),\sigma(i)}\\ \text{Avec } \rho=\sigma\tau^{-1},\ j=\tau(i):\quad &= \sum_{\tau\in\mathfrak{S}_n}\varepsilon(\tau)\prod_{i=1}^n b_{i,\tau(i)}\times\sum_{\rho\in\mathfrak{S}_n}\varepsilon(\rho)\prod_{j=1}^n c_{j,\rho(j)}\\ &= \det(B)\det(C)\end{aligned}$$

Définition 6.5.6 - Mineur et cofacteur.
Soit $B \in \mathcal{M}_n(A)$. Soit (i,j) avec $1 \leqslant i,j \leqslant n$.
On note $B^{i,j}$ la matrice obtenue à partir de B en enlevant la i^{e} ligne et la j^{e} colonne.
On définit :

- Le *mineur* d'indice (i,j) de B comme $\mu_{i,j} = \det\left(B^{i,j}\right)$.
- Le *cofacteur* d'indice (i,j) de B comme $(-1)^{i+j}\mu_{i,j}$.
- La *comatrice* de B comme la matrice des cofacteurs de B : $\mathrm{Com}(B) = \left((-1)^{i+j}\mu_{i,j}\right)_{i,j} \in \mathcal{M}_n(A)$.

Notation. Pour $i \in \{1,\dots,n\}$ on pose $i^* = \{1,\dots,n\} \setminus \{i\}$.
L'ensemble i^* est muni de l'ordre induit par celui de $\{1,\dots,n\}$, d'où une identification de i^* à $\{1,\dots,n-1\}$.
Si $\sigma \in \mathfrak{S}_n$ avec $\sigma(i) = j$ alors $\left(\sigma_{|i^*} : i^* \to j^*\right) \in \mathfrak{S}_{n-1}$. ♢

Lemme 6.5.7 - Signature d'une restriction.
Soit $i,j \in \{1,\dots,n\}$ et $\sigma \in \mathfrak{S}_n$ avec $\sigma(i) = j$. Soit τ la restriction $\sigma_{|i^*}$.
Alors :
$$\varepsilon(\tau) = (-1)^{i+j}\varepsilon(\sigma)$$

Démonstration. On a :
$$\varepsilon(\sigma) = \prod_{u<v} \frac{\sigma(u)-\sigma(v)}{v-u} = \prod_{i<v} \frac{\sigma(v)-j}{v-i} \times \prod_{u<i} \frac{j-\sigma(u)}{i-u} \times \varepsilon(\tau) = \prod_{v\neq i} \frac{\sigma(v)-j}{v-i} \times \varepsilon(\tau)$$
Il faut donc que $\prod_{v\neq j} \frac{\sigma(v)-i}{v-j} = \pm 1$. On compte donc le nombre de facteurs négatifs :

- Le numérateur est négatif lorsque $\sigma(v) \in \{1,\dots,j-1\}$: de cardinal $j-1$.
- Le dénominateur est négatif lorsque $v \in \{1,\dots,i-1\}$: de cardinal $= i-1$.

Ainsi :
$$\varepsilon(\sigma) = (-1)^{i-1+j-1}\varepsilon(\tau) = (-1)^{i+j}\varepsilon(\tau)$$

Proposition 6.5.8 - Développement du déterminant selon les lignes et colonnes.
Soit $B \in \mathcal{M}_n(A)$. Nous avons :

- La formule de développement selon la i^{e} ligne :
$$\det(B) = \sum_{j=1}^{n} b_{i,j}(-1)^{i+j}\mu_{i,j}$$
- La formule de développement selon la j^{e} colonne :
$$\det(B) = \sum_{i=1}^{n} b_{i,j}(-1)^{i+j}\mu_{i,j}$$

Démonstration. D'après la proposition 6.5.3, il suffit de montrer la première égalité. On a :
$$\det(B) = \sum_{j=1}^{n} \sum_{\substack{\sigma\in\mathfrak{S}_n \\ \sigma(j)=i}} \varepsilon(\sigma) \prod_{s=1}^{n} b_{\sigma(s),s}$$
En isolant le facteur $b_{\sigma(j),j} = b_{i,j}$ en posant $\tau = \sigma_{|j^*}$ et en utilisant le lemme 6.5.7, on obtient :
$$\det(B) = \sum_{j=1}^{n} b_{i,j} \sum_{\tau : j^* \to i^*} (-1)^{i+j}\varepsilon(\tau) \prod_{v\in j^*} b_{\tau(v),v} = \sum_{j=1}^{n} b_{i,j}(-1)^{i+j}\mu_{i,j}$$

Proposition 6.5.9 - Formule de la comatrice.
Soit $B \in \mathcal{M}_n(A)$. Nous avons la formule de la comatrice :

$$B\big(\mathrm{Com}(B)\big)^t = \big(\mathrm{Com}(B)\big)^t B = \det(B)\,\mathrm{id}$$

Démonstration. Rappelons que $\mu_{i,j} = \det\Big(B^{i,j}\Big)$.

Les coefficients de $B\big(\mathrm{Com}(B)\big)^t$ sont :

$$c_{i,j} = \sum_{k=1}^{n} b_{i,k}(-1)^{k+j}\mu_{j,k}$$

Si $j = i$, alors d'après la proposition précédente :

$$c_{i,i} = \sum_{k=1}^{n} b_{i,k}(-1)^{k+i}\mu_{i,k} = \det(B)$$

Si $j \neq i$, notons B' la matrice obtenue en remplaçant la j^{e} ligne par la i^{e} ligne.
Comme le déterminant est alterné, $\det\big(B'\big) = 0$. Alors $b'_{j,k} = b_{i,k}$ et $\mu'_{j,k} = \mu_{j,k}$.

En développant selon la j^{e} ligne :

$$0 = \det\Big(B'\Big) = \sum_{k=1}^{n} b'_{j,k}(-1)^{k+j}\mu_{j,k} = \sum_{k=1}^{n} b_{i,k}(-1)^{k+j}\mu_{j,k} = c_{i,j}$$

Ainsi :

$$B\big(\mathrm{Com}(B)\big)^t = \det(B)\,\mathrm{id}$$

Le développant selon les colonnes permet d'obtenir l'autre égalité.

Corollaire 6.5.10 - Inversibilité d'un matrice.
Soit $B \in \mathcal{M}(A)$. On a :

$$B \in \mathcal{M}_n(A)^\times \Leftrightarrow \det(B) \in A^\times$$

Démonstration.
$\Rightarrow$: Si $B \in \mathcal{M}_n(A)^\times$, il existe $B^{-1} \in \mathcal{M}_n(A)$ avec $BB^{-1} = \mathrm{id}$.
Ainsi $\det(B)\det(B)^{-1} = \det(\mathrm{id}) = 1$ donc $\det(B) \in A^\times$.
$\Leftarrow$: Si $\det(B) \in A^\times$, alors d'après la proposition précédente $C = \det(B)^{-1}\big(\mathrm{Com}(B)\big)^t$ vérifie $BC = CB = \mathrm{id}$ et donc $B \in \mathcal{M}_n(A)^\times$ car C est son inverse.

Théorème 6.5.11 - Cayley-Hamilton.
Soit $B \in \mathcal{M}_n(A)$ et $\chi(T) = \det(T\,\mathrm{id} - B)$ son polynôme caractéristique. Alors $\chi(B) = 0$.

Démonstration.
Soit $R = \left\{ \sum_{\text{finie}} a_n B^n \;\middle|\; a_n \in A \right\} \subset \mathcal{M}_n(A)$ (ici $B^0 := \mathrm{id}$). Donc, R est un sous-anneau commutatif de $\mathcal{M}_n(A)$. L'application $a \mapsto a\,\mathrm{id}$ est une morphisme d'anneaux injectif $A \to R$ et on considère A comme un sous-anneau de R.

On considère $R[T]$ l'anneau des polynômes à coefficients dans R, vue comme un sous-anneau commutatif de $\mathcal{M}_n\big(A[T]\big)$.
Donc $T\,\mathrm{id} - B \in R[T]$ et $\chi(T) = \det(T\,\mathrm{id} - B) \in A[T] \subset R[T]$.

D'après le théorème de division euclidienne dans $R[T]$, on peut écrire :

$$\chi(T) = (T\,\mathrm{id} - B)q + r \text{ avec } q, r \in R[T] \text{ et } \deg(r) < 1$$

D'après la proposition 6.5.9 on a dans l'anneau $\mathcal{M}_n\big(A[T]\big)$:

$$\chi(T)\,\mathrm{id} = \det(T\,\mathrm{id} - B)\,\mathrm{id} = (T\,\mathrm{id} - B)\big(\mathrm{Com}(T\,\mathrm{id} - B)\big)^t$$

Soit $C := \big(\mathrm{Com}(T\,\mathrm{id} - B)\big)^t$. On a dans $\mathcal{M}_n\big(A[T]\big)$:

$$0 = (q - C)(T\,\mathrm{id} - B) + r$$

Car $\deg(r) < 1$, une considération du degré en T des coordonnées des matrices dans l'identité montre que $q - C = 0$.

En particulier, $C \in R[T]$ et on peut appliquer le morphisme d'anneaux d'évaluation de $R[T]$:

$$\begin{array}{rccc} \mathrm{ev}_B : & R[T] & \longrightarrow & R \\ & T & \longmapsto & B \end{array} \quad \text{donc } \chi(B) = q(B)(B - B) = 0$$

Pour finir, nous allons étudier les liens entre injectivité, surjectivité et bijectivité des endomorphismes en termes de déterminant.

Proposition 6.5.12 - Lien injectivité, surjectivité et déterminant.
Soit $B \in \mathcal{M}_n(A)$ et soit $f_B : A^n \to A^n$ l'endomorphisme A-linéaire associé.
Alors nous avons :

1. L'application f_B est surjectif si et seulement si f_B est bijectif si et seulement si $\det(B) \in A^\times$.
2. Si $\det(B)$ n'est pas un diviseur de 0 dans A, alors f_B est injectif.

Remarque. Il est en fait aussi possible de démonter la réciproque de 2. ♢

Démonstration. Soit $e_1, \ldots, e_n$ les vecteurs de la base canonique e de A^n.

1. D'après le corollaire 6.5.10, il reste à montrer que f_B est surjectif alors f_B bijectif.

Si f_B est surjectif, il existe $\varepsilon_i \in A^n$ tel que $f_B(\varepsilon_i) = e_i$ pour tout i. Par la propriété universelle de la somme directe 4.4.3, on a un morphisme A-linéaire $g : A^n \to A^n$ induit par $(e_i \mapsto \varepsilon_i)_i$.

Alors pour tout i : $f_B \circ g(e_i) = e_i$ donc $f_B \circ g = \mathrm{id}_{A^n}$.
Si $C = \mathrm{Mat}_e(g)$ alors $\det(B)\det(C) = 1$ donc $\det(B) \in A^\times$ et donc f_B est bijectif.

2. Posons $d = \det(B)$. Soit $v \in \mathrm{Ker}(f_B)$. Si on écrit $v = \sum v_i e_i$, avec $v_i \in A$, alors :

$$B\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = f_B(v) = 0 \text{ donc } 0 = (\mathrm{Com}\,B)^t B \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \det(B)\,\mathrm{id}\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} dv_1 \\ \vdots \\ dv_n \end{bmatrix}$$

Ainsi, $\forall i : dv_i = 0$ donc, comme d n'est pas un diviseur de 0, $\forall i : v_i = 0$ donc $v = 0$ et f_B est injectif.

7. Anneaux factoriels et principaux

7.1 Sous-algèbre

Définition 7.1.1 - Sous-algèbre.
Soit A un anneau commutatif et B une A-algèbre, pas nécessairement commutative.
On appelle *sous-algèbre* de B tout sous-anneau $B' \subset B$ qui est aussi un sous-A-module de B.

Sous-algèbre engendré.

1. **Intersection :** Soit $(B_i)_{i\in I}$ une famille de sous-algèbres de B.
   Alors l'intersection $\bigcap_{i\in I} B_i$ est une sous-algèbre de B.
2. **Sous-algèbre engendré :** Cela permet de considérer l'*algèbre engendré* par une partie S de B comme la plus petite sous-algèbre $A[S]$ de B contenant S, donc

$$A[S] := \bigcap_{\substack{S\subset B' \\ B' \text{ ss-alg}}} B'$$

- Si $A[S] = B$, on dit que l'algèbre B est engendrée par S. Dans ce cas :

$$B = \left\{ \sum_{(i_1,\dots,i_n)}^{\text{finie}} a_{(i_1,\dots,i_n)} s_{i_1} \dots s_{i_n} \;\middle|\; a_{(i_1,\dots,i_n)} \in A, s_{i_k} \in S \right\}$$

- Si $B = A[S]$ et $|S| < \infty$ on dit que l'algèbre B est de *type fini*.
- Si B est commutative et de type fini, c'est-à-dire, $B = A[S]$ avec une partie $S = \{s_1, \dots, s_n\} \subseteq B$ on a un morphisme de A-algèbres, c'est-à-dire un morphisme d'anneaux A-linéaire, qui est surjectif :

$$\begin{array}{rccc} \text{ev}_S : & A[X_1,\dots,X_n] & \longrightarrow & B \\ & X_i & \longmapsto & s_i \end{array}$$

Ce morphisme est construit à partir des propriétés universelle des anneaux de polynômes et son image est $A[S] = B$. Ainsi une A-algèbre commutative et de type fini est simplement un anneau quotient de $A[X_1, \dots, X_n]$.

△

7.2 Anneaux noethériens

Après cette discussion générale, nous allons commencer par étudier les anneaux *noethériens* qui forment une classe d'anneaux jouissant de propriétés de finitude remarquables.

Définition 7.2.1 - Anneau noethérien.
Soit A un anneau.
On dit que A est *noethérien* si toute suite croissante d'idéaux de A, $I_1 \subseteq I_2 \subseteq \dots$ est stationnaire.
C'est-à-dire qu'il existe N avec $I_N = I_{N+1} = \cdots$.

Lemme 7.2.2 - Caractérisation des anneaux noethérien.
Un anneau A est noethérien si et seulement si tout idéal de A est de type fini comme A-module.

Démonstration.

$\Rightarrow$: Supposons par l'absurde qu'il existe un idéal I de A qui n'est pas de type fini.
Construisons une suite d'idéaux non-stationnaire, dont le n^{e} terme I_n est engendré par n éléments de I.

On pose $I_1 = (x_1)$ avec $x_1 \in I$. Si I_n est construit, il existe $x_{n+1} \in I \setminus I_n$ et on pose $I_{n+1} = (x_1, \ldots, x_{n+1})$ (l'ensemble $I \setminus I_n$ est bien non vide car I n'est pas engendré par un nombre fini d'éléments).

Ainsi, nous avons $I_1 \subsetneq I_2 \subsetneq \cdots$ et A n'est pas noethérien. $\lightning$

$\Leftarrow$: Considérons une suite croissante $I_1 \subseteq I_2 \subseteq \cdots$. On pose :

$$I = \bigcup_{n \geqslant 1} I_n$$

C'est un idéal de A donc, par hypothèse, il existe $x_1, \ldots, x_r$ avec $I = \sum_{i=1}^{r} Ax_i$.
On a $\forall i : x_i \in I_m$ pour un m assez grand donc $I_m = I_{m+1} = \ldots = I$ d'où A est noethérien.

Exemple d'anneau noethérien.

- Un corps est noethérien.
- L'anneau $\mathbb{Z}$ est noethérien (chaque idéal est principal).
- Un anneau A avec $|A| < \infty$ est noethérien. En particulier, les anneaux $\mathbb{Z}/n\mathbb{Z}$ sont noethérien.
- Un anneau produit $A = \prod_{i=1}^{n} A_i$, avec A_i noethérien pour tout i, est noethérien.

$\triangle$

Lemme 7.2.3 - Quotient d'anneau noethérien.
Tout quotient d'un anneau noethérien est noethérien.

Démonstration.

Soit A un anneau noethérien et $\pi : A \to C$ un morphisme d'anneaux surjectif.
Soit J un idéal de C. Alors $\pi^{-1}(J) \subset A$ est un idéal donc :

$$\pi^{-1}(J) = \sum_{i=1}^{n} Ax_i \text{ d'où } J = \sum_{i=1}^{n} C\pi(x_i) \text{ est de type fini.}$$

Ainsi, tout idéal de C est de type fini, C est noethérien.

Théorème 7.2.4 - Théorème de la base de Hilbert.
Soit A un anneau noethérien. Alors l'anneau de polynômes $A[X]$ est noethérien.

Démonstration.

Supposons qu'il existe un idéal $I \subset A[X]$ qui n'est pas de type fini.
Alors on construit une suite $(f_k)_k$ d'éléments de I comme suit.

- Soit $f_1 \in I$ de degré minimal.
- Supposons $f_1, \ldots, f_k$ déjà construits. On prend f_{k+1} de degré minimal dans $I \setminus \{f_1, \ldots, f_k\}$. Cet ensemble est bien non vide car I n'est pas engendré par un nombre fini d'éléments.

Pour tout $k \geqslant 1$, soit $a_k X^{d_k}$ le monôme dominant de f_k. Par définition, $(d_k)_k$ est croissante.
Comme A est noethérien, $\left\langle \{a_k\}_{k \geqslant 1} \right\rangle \subset A$ est de type fini donc il existe m tel que :

$$\left\langle \{a_k\}_{k \geqslant 1} \right\rangle = \langle \{a_1, \ldots, a_m\} \rangle$$

En particulier :

$$a_{m+1} = u_1 a_1 + \ldots + u_m a_m \text{ avec } u_j \in A$$

Soit $g = \left(u_1 f_1 X^{d_{m+1} - d_1} + \cdots + u_m f_m X^{d_{m+1} - d_m} \right) - f_{m+1} \in A[X]$.

Le coefficient dominant du polynôme entre parenthèses est a_{m+1} donc $\deg(g) < \deg(f_{m+1})$.
Or, $g \in I \setminus (f_1, \ldots, f_m)$ ce qui contredit la minimalité du degré de f_{m+1} et ainsi $A[X]$ est noethérien.

Corollaire 7.2.5 - Algèbre issu d'un anneau noethérien.
Soit A un anneau noethérien. Toute A-algèbre de type fini est un anneau noethérien.

Démonstration. Par le théorème de la base de Hilbert et par récurrence, $A[X_1, \ldots, X_n]$ est noethérien.
Une A-algèbre de type fini est un quotient de $A[X_1, \ldots, X_n]$ donc le résultat découle du lemme 7.2.3.

Remarque. Si A est noethérien et $A' \subset A$ est un sous-anneau, alors, en général, A' n'est pas noethérien.
Par exemple, $\mathbb{Z}\left[2X, 2X^2, 2X^3, \ldots\right] \subset \mathbb{Z}[X]$ est un sous-anneau non noethérien de $\mathbb{Z}[X]$.
En effet, la suite des idéaux $I_n = \left(2X, 2X^2 \ldots, 2X^n\right)$ est croissante mais n'est pas stationnaire. ♢

7.3 Anneaux euclidiens, principaux et factoriels

Nous allons à présent étudier les anneaux euclidiens, principaux et factoriels.
Ces anneaux sont intéressant car ils possèdent des propriétés arithmétiques proche de celles des entiers.

Définition 7.3.1 - Anneau principal.
Soit A un anneau intègre.
On dit que A est un anneau *principal* si tous ses idéaux sont principaux.

Remarque. Un anneau principal est evidemment noethérien. ♢

Exemples d'anneaux principaux.

- Un corps est un anneau principal.
- L'anneau $\mathbb{Z}$ est un anneau principal.
- Les anneaux euclidiens sont principaux (voir au-dessous). En particulier $K[X]$ avec K un corps est principal.
- L'anneau $\mathbb{Z}[X]$ n'est pas principal parce que $(2, X)$ ne est pas un idéal principal.
- L'anneau $K[X, Y]$ n'est pas principal parce que (X, Y) ne est pas un idéal principal.

△

Définition 7.3.2 - Anneau euclidien.
Soit A un anneau intègre.
On dit que A est un anneau *euclidien* s'il existe une application $\delta : A \setminus \{0\} \to \mathbb{N}$ tel que :

Pour tout éléments $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tel que $a = bq + r$ avec $\delta(r) < \delta(b)$ ou $r = 0$.

Cette application δ est appelée *stathme euclidien*.

Exemples d'anneaux euclidiens.

1. Un corps est euclidien (par exemple, pour le stathme $\delta \equiv 0$).
2. L'anneau $\mathbb{Z}$ est un anneau euclidien pour $\delta(a) = |a|$.
3. L'anneau $K[X]$ où K est un corps est euclidien pour $\delta = \deg$ (division euclidienne!)
4. L'anneau des entiers de Gauss $\mathbb{Z}[i] = \left\{x + iy \,|\, x, y \in \mathbb{Z}\right\} \subset \mathbb{C}$ est euclidien pour la restriction de la fonction $x + iy \mapsto |x + iy|^2 = x^2 + y^2$ à $\mathbb{Z}[i]$:

$$\begin{array}{rccc} \delta : & \mathbb{Z}[i] \setminus \{0\} & \longrightarrow & \mathbb{N} \\ & x + \mathrm{i}y & \longmapsto & |x + iy|^2 = x^2 + y^2 \end{array}$$

En effet, si $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$, soit $q \in \mathbb{Z}[i]$ le plus proche de ab^{-1} et $r = a - bq$.
Alors $\left|q - ab^{-1}\right| \leqslant \frac{\sqrt{2}}{2} < 1$ donc $|r| = |b|\left|ab^{-1} - q\right| < |b|$.

△

Montrons à présent que les anneaux euclidiens sont principaux.

Proposition 7.3.3 - Euclidien ⇒ Principal.
Tout anneau euclidien est principal.

Démonstration. Soit A un anneau euclidien, I un idéal non nul de A.
Alors il existe $a \in I$ non nul avec $\delta(a)$ minimal dans $\Big\{\delta(b) \mid b \in I \setminus \{0\}\Big\}$. Alors $I = (a)$.

En effet, soit $x \in I$. Alors $x = aq + r$ avec $q, r \in A$ et $\delta(r) < \delta(a)$ ou $r = 0$.
Comme $r \in I$, la minimalité de $\delta(a)$ implique que $r = 0$ donc $x \in (a)$ et $I \subset (a)$. L'autre inclusion est triviale puisque $a \in I$.

Tournons nous à présent vers les anneaux factoriels.

Définition 7.3.4 - Divisibilité.
Soit A un anneau, a et b des éléments de A.

- On dit que a *divise* b, noté $a \mid b$, s'il existe $c \in A$ tel que $b = ac$.
- On dit que a et b sont *associés*, noté $a \sim b$, si on a $a \mid b$ et $b \mid a$.

Remarque.

1. La relation $\sim$ est une relation d'équivalence. La classe d'équivalence de 1 est $A^\times$.
2. On a $a \mid b \Leftrightarrow (b) \subset (a)$ et $a \sim b \Leftrightarrow (a) = (b)$.
3. Si A est intègre, on a $a \sim b \Leftrightarrow \exists u \in A^\times : a = ub$.
   En fait, si $a \sim b$, alors $b = ac = \big(bc'\big)c$ donc $b\big(1 - cc'\big) = 0$.
   - Si $b = 0$ ou $a = 0$, on peut prendre $u = 1$.
   - Si $b \neq 0$ alors c et c' sont inversibles.

♢

Définition 7.3.5 - Élément irréductible et premier.
Soit A un anneau intègre et $x \in A$.

- On dit que x est *irréductible* si $x \in A \setminus \big(A^\times \cup \{0\}\big)$ et :
$$\forall a, b \in A : x = ab \Rightarrow a \in A^\times \text{ ou } b \in A^\times$$
- On dit que x est *premier* si $x \in A \setminus \big(A^\times \cup \{0\}\big)$ et $(x) \subset A$ est un idéal premier :
$$\forall a, b \in A : x \mid ab \Rightarrow x \mid a \text{ ou } x \mid b$$

Remarque.

1. Il est commode d'appeler *factorisation non triviale* de p une écriture $p = ab$ telle que ni a ni b n'est inversible. Ainsi, un élément irréductible est un élément non nul, non inversible, qui n'a pas de factorisation non triviale.

2. Si p est premier alors p est irréductible c'est-à-dire : si $p = ab$ alors $a \in (p)$ ou $b \in (p)$.

   Supposons que $a \in (p)$: $a = pu$, $u \in A$ non nul.
   Alors, $a = pu = (ab)u$ donc $a(1 - bu) = 0$ donc, comme $a \neq 0$ et A est intègre, $b, u \in A^\times$.

3. Si p est irréductible et $p \sim q$ alors q est irréductible.

♢

Exemples d'éléments irréductibles.

1. Un corps n'a pas d'éléments irréductibles.
2. Si $A = \mathbb{Z}$ alors p premier si et seulement si $\pm p$ est un nombre premier si et seulement si p est irréductible.

△

Définition 7.3.6 - Anneau factoriel.
Soit A un anneau intègre.
On dit que A est un anneau *factoriel* si :

Tout $a \in A$ non nul possède une décomposition en facteurs irréductibles,
unique à ordre et association près des facteurs, c'est-à-dire de la forme :

$$a = up_1^{\alpha_1} \dots p_r^{\alpha_r} \text{ avec } u \in A^\times, p_1, \dots, p_r \text{ irréductibles deux à deux non associés et } \alpha_1, \dots, \alpha_r \geqslant 1$$

Remarque.

1. L'unicité signifie que si a possède deux décompositions en facteurs irréductibles :
$$a = up_1^{\alpha_1} \dots p_r^{\alpha_r} = vq_1^{\beta_1} \dots q_s^{\beta_s}$$
Alors $r = s$ et il existe $\sigma \in \mathfrak{S}_r$ telle que $p_i \sim q_{\sigma(i)}$ et $\alpha_i = \beta_{\sigma(i)}$.

2. Soit A un anneau factoriel et $\mathcal{P}$ un ensemble de représentants des éléments irréductibles pour la relation $\sim$.
Alors tout élément non nul $a \in A$ possède une unique décomposition
$$a = u \prod_{p \in \mathcal{P}} p^{\alpha_p}$$
Avec $u \in A^\times$ et $\alpha_p = 0$ pour presque tout p. L'entier α_p est appelé la *multiplicité* de p dans a.

3. Dans un anneau factoriel, les éléments irréductibles sont exactement les éléments premiers.
En effet, si p est irréductible et $p \mid ab$, en écrivant :
$$a = up_1 \dots p_r \quad ; \quad b = vq_1 \dots q_s$$
Alors $p \mid uvp_1 \dots p_r q_1 \dots q_s$ donc par unicité de la décomposition, $p \sim p_j$ pour un j ou $p \sim q_k$ pour un k.
Ainsi $p \mid a$ ou $p \mid b$ donc p est premier.

4. Un corps est factoriel car en particulier il n'y a pas d'éléments irréductibles.

5. Nous savons que $\mathbb{Z}^\times = \{\pm 1\}$. Ainsi, le théorème de décomposition des éléments de $\mathbb{N}$ en produit de facteurs premiers montre que $\mathbb{Z}$ est factoriel. Plus généralement, tous les anneaux principaux sont factoriels (voir au-dessous).

♢

Proposition 7.3.7 - Principal ⇒ Factoriel.
Tout anneau principal est factoriel.

Remarque. Attention la réciproque est fausse :

- L'anneau $\mathbb{Z}[X]$ est factoriel mais pas principal car $(2, X)$ n'est pas principal.
- De même, l'anneau $K[X, Y]$ est factoriel mais pas principal car (X, Y) n'est pas principal.

♢

Démonstration.
Existence de la factorisation :
Soit S l'ensemble des idéaux principaux (a) de A tel que $a \neq 0$ n'admette aucune écriture de la forme :

$$a = up_1^{\alpha_1} \dots p_r^{\alpha_r} \text{ avec } u \in A^\times \text{ et } \forall i : p_i \text{ irréductible}$$

Supposons par l'absurde que $S \neq \varnothing$.
Puisque A est principal, A est noethérien donc S possède *un* élément maximal pour l'inclusion.
En effet, dans le cas contraire nous aurions une suite d'idéaux (dans S) non stationnaires.

Soit $(a) \in S$ *un* élément maximal.

Alors $a \notin A^\times$ et a n'est pas irréductible car sinon nous aurions a une factorisation en irréductibles.

Ainsi nous pouvons écrire $a = a_1 a_2$ avec $a_1, a_2 \notin A^\times$.
Nous avons $(a) \subsetneq (a_1)$ et $(a) \subsetneq (a_2)$. Mais comme (a) est maximal, $(a_1), (a_2) \notin S$ donc a_1 et a_2 possèdent une écriture en facteurs irréductibles. Le produit de ces factorisations donne une factorisation de a ce qui est une contradiction. Ainsi $S = \varnothing$ et l'existence est établie.

Unicité de la factorisation :
Si p est irréductible dans A alors p est premier.
En effet, si $p \in A$ est irréductible, soit $\mathfrak{a}$ un idéal tel que $(p) \subset \mathfrak{a} \subsetneq A$ un idéal. Alors $\mathfrak{a} = (a)$ et il existe $c \in A$ tel que $p = ac$. Comme $a \notin A^\times$, car $\mathfrak{a} \subsetneq A$, et p est irréductible, $c \in A^\times$ donc $(p) = (a)$.
Ainsi, (p) est un idéal maximal donc en particulier un idéal premier. Cela montre que p est premier.

Pour l'unicité, soit $a \in A$ non nul tel que :

$$u = p_1 \dots p_n = q_1 \dots q_m \text{ avec } p_i, q_j \text{ irréductibles}$$

Montrons que nous avons alors $n = m$ et $p_i \sim q_i$ (après changement de l'ordre des facteurs).
Procédons par récurrence sur n.

- Si $n = 1$, alors dans ce cas $a = p_1$ est irréductible donc $m = 1$. En particulier $p_1 = q_1$.
- Si $n > 1$, alors $p_1 \mid q_1 \dots q_m$ donc puisque p_1 est premier d'après l'assertion précédente, $p_1 \mid q_j$ pour un j.
  Par changement de l'ordre des facteurs, nous pouvons supposer que $j = 1$.
  Ainsi puisque q_1 est irréductible, $q_1 = up_1$ avec $u \in A^\times$ et $q_1 \sim p_1$.
  En utilisant l'intégrité de A nous remarquons que :

$$\cancel{p_1} p_2 \dots p_n = (u\cancel{p_1}) q_2 \dots q_m$$

  Par hypothèse de récurrence sur $n-1$, nous avons $n - 1 = m - 1$ et donc après changement de l'ordre des facteurs $p_i \sim q_i$ pour $i = 2, \dots, m$.

Nous avons donc le résultat pour tout $n \in \mathbb{N}$ ce qui montre l'unicité et conclut la preuve.

La question à présent est de savoir si $A[X]$ est factoriel lorsque A est factoriel.

Définition 7.3.8 - Pgcd et ppcm.
Soit A un anneau factoriel et $\mathcal{P}$ un ensemble de représentants des éléments irréductibles pour $\sim$.
Soit $a_1, \dots, a_m$ des éléments non nuls de A et $\alpha_p(i)$ la multiplicité de p dans a_i.
Alors on a :

$$\operatorname{pgcd}(a_1, \dots, a_m) = \prod_{p \in \mathcal{P}} p^{\min\limits_i \alpha_p(i)} \quad ; \quad \operatorname{ppcm}(a_1, \dots, a_m) = \prod_{p \in \mathcal{P}} p^{\max\limits_i \alpha_p(i)}$$

Remarque.
Les deux éléments $\operatorname{pgcd}(a_1, \dots, a_m)$ et $\operatorname{ppcm}(a_1, \dots, a_m)$ sont bien définis par les a_i à association près.
Ils ont les propriétés usuelles :

- Si $b \in A$ avec $b \mid a_i$ alors $b \mid \operatorname{pgcd}(a_1, \dots, a_m)$.
- Si $b \in A$ avec $a_i \mid b$ alors $\operatorname{ppcm}(a_1, \dots, a_m) \mid b$.

En fait, le produit de deux éléments non nuls $a = u \prod_{p \in \mathcal{P}} p^{\alpha_p}$ et $b = v \prod_{p \in \mathcal{P}} p^{\beta_p}$ est :

$$ab = uv \prod_{p \in \mathcal{P}} p^{\alpha_p + \beta_p}$$

Ainsi $a \mid b$ si et seulement si $\forall p \in \mathcal{P} : \alpha_p \leqslant \beta_p$. ♢

Proposition 7.3.9 - Caractérisation du pgcd et ppcm.
Soit A un anneau principal, et $a, b \in A$ non nuls.
Alors pour $x \in A$:

1. $(x) = (a, b) \Leftrightarrow x = \text{pgcd}(a, b)$.
2. $(x) = (a) \cap (b) \Leftrightarrow x = \text{ppcm}(a, b)$

Démonstration.
1. :
$\Rightarrow$: Nous avons pour $d \in A$:

$$\big(d \mid a \text{ et } d \mid b\big) \Leftrightarrow \big((a) \subset (d) \text{ et } (b) \subset (d)\big) \Leftrightarrow \big((a, b) \subset (d)\big)$$

Cela montre qu'un générateur x de l'idéal (a, b) est un pgcd de a et b.
$\Leftarrow$: Si $x = \text{pgcd}(a, b)$ alors $(a, b) \subset (x)$. Par unicité du pgcd et par $\Rightarrow$, on a en fait $(a, b) = (x)$.

2.
$\Rightarrow$: Nous avons pour $d \in A$:

$$\big(a \mid d \text{ et } b \mid d\big) \Leftrightarrow \big((d) \subset (a) \text{ et } (d) \subset (b)\big) \Leftrightarrow \big((d) \subset (a) \cap (b)\big)$$

Cela montre qu'un générateur x de l'idéal $(a) \cap (b)$ est un ppcm de a et b.
$\Leftarrow$: Si $x = \text{ppcm}(a, b)$ alors $(a) \cap (b) \subset (x)$. Par unicité du ppcm et par $\Rightarrow$, on a en fait $(a) \cap (b) = (x)$.

Proposition 7.3.10 - Premier dans un anneau principal.
Soit A un anneau principal qui n'est pas un corps et $p \in A$ non nul.
Les assertions suivantes sont équivalentes :

1. p est irréductible.
2. p est premier, c'est-à-dire l'idéal (p) est premier.
3. L'idéal (p) est maximal.

Démonstration.

- Le point 1. $\Rightarrow$ 3. a été démontré dans la preuve de « Principal $\Rightarrow$ Factoriel ».
- Le point 3. $\Rightarrow$ 2. est évident par définition des idéaux maximaux et premiers.
- Le point 2. $\Rightarrow$ 1. est vérifié car l'anneau A est intègre.

Retournons à notre question : $A[X]$ est-il factoriel si A l'est ?

Définition 7.3.11 - Contenu et polynôme primitif.
Soit A un anneau factoriel et $P \in A[X]$ non nul.
On appelle *contenu* de P, noté $c(P)$, le pgcd de ses coefficients. On dit que P est *primitif* si $c(P) = 1$.

Exemple de polynôme primitif.

1. Si un coefficient de P est inversibles, alors P est primitif. En particuliar, si P est unitaire, alors P est primitif.
2. Le polynôme $c(P)^{-1}P \in A[X]$ est toujours primitif.

△

Lemme 7.3.12 - Lemme de Gauss pour les contenus.
Soit A un anneau factoriel et $P, Q \in A[X]$ des polynômes non nuls.
Alors :

$$c(PQ) = c(P)c(Q)$$

En particulier, le produit de deux polynômes primitifs est primitif.

Démonstration. Nous avons clairement $\forall a \in A : c(aP) = ac(P)$.

Écrivons donc $P = aP'$ et $Q = bQ'$ avec $a, b \in A$ tels que P' et Q' soient primitifs. Alors :

$$c(PQ) = ab \cdot c\Big(P'Q'\Big)$$

Ainsi, nous nous somme ramené au cas où P et Q sont primitifs.

Rappelons que ${}^{A[X]}\!/_{pA[X]} \cong \Big({}^{A}\!/_{pA}\Big)[X]$ est intègre pour $p \in A$ irréductible.

Comme P, Q sont primitifs, pour tout p irréductible, nous avons :

- $\overline{P} \neq 0$ et $\overline{Q} \neq 0$ dans ${}^{A[X]}\!/_{pA[X]}$.
- Donc par intégrité $\overline{PQ} = \overline{P} \cdot \overline{Q} \neq 0$ dans ${}^{A[X]}\!/_{pA[X]}$.

Ainsi PQ est primitif car aucun irréductible ne divise son contenu donc $c(PQ) = 1 = c(P)c(Q)$.

Théorème 7.3.13 - Théorème de Gauss pour les polynômes irréductibles.

Si A est un anneau factoriel alors $A[X]$ est aussi factoriel.

De plus, la famille $\mathcal{F}_{A[X]}$ des irréductibles de $A[X]$ est réunion de la famille $\mathcal{F}_A$ des polynômes constants irréductibles dans A et de la famille $\mathcal{F}'$ des polynômes primitifs qui sont irréductibles dans $K[X]$ où $K = \mathrm{Frac}(A)$ est le corps des fractions de A.

Démonstration du théorème (début).

$$\text{Montrons que } \mathcal{F}_A \cup \mathcal{F}' \subset \mathcal{F}_{A[X]}.$$

Étape 1 : Montrons que les irréductibles de A sont irréductible dans $A[X]$.

Soit $a \in \mathcal{F}_A \setminus \{0\}$ tel que $a = QR$ avec $Q, R \in A[X]$. Nous avons $0 = \deg a = \deg Q + \deg R$ donc Q et R sont dans A. Puisque a est irréductible dans A, Q ou R est dans $A^\times \subset A[X]^\times$. Ainsi, a est irréductible dans $A[X]$.

Étape 2 : Montrons que les polynômes de $A[X]$ qui sont primitifs et irréductibles dans $K[X]$ sont irréductible dans $A[X]$.

Soit $P \in \mathcal{F}'$. Supposons que $P = QR$ dans $A[X]$. Alors comme $A[X] \subset K[X]$ et P est irréductible dans $K[X]$, nous avons $Q \in K[X]^\times$ ou $R \in K[X]^\times$. Mais comme nous savons que $K[X]^\times = K^\times$, nous obtenons que :

$$Q \text{ ou } R \text{ est dans } K^\times \cap A[X] = A \setminus \{0\}$$

Considérons le contenu de ces polynômes et appliquons le lemme de Gauss :

$$1 = c(P) = c(Q)c(R)$$

Donc $Q = c(Q) \in A^\times$ ou $R = c(R) \in A^\times$. Ainsi, P est irréductible dans $A[X]$.

Montrons à présent l'existence et l'unicité d'une factorisation en irréductibles dans $A[X]$:

Étape 3 : Montrons l'existence d'une de factorisation dans $A[X]$:

Soit $P \in A[X] \setminus \{0\}$. Alors $P = c(P)P'$ et $P' = c(P)^{-1}P \in A[X]$ est un polynôme primitif.

Puisque A est factoriel, il existe une factorisation en irréductible dans A du contenu $c(P)$ n'utilisant que les éléments de $\mathcal{F}_A$. Comme $\mathcal{F}_A \subset \mathcal{F}_{A[X]}$, il suffit donc de donner une factorisation pour P' en fonction de $\mathcal{F}'$ ce qui est le résultat du lemme suivant :

Lemme 7.3.14 - Factorisation des polynômes primitifs.

Soit $P \in A[X]$ un polynôme primitif.

Alors P admet une factorisation ne contenant que des éléments de $\mathcal{F}'$.

Démonstration du lemme.

Tout polynôme $R \in K[X]$ peut s'écrire sous la forme :

$$R = \frac{r}{s}Q \text{ avec } r, s \in A,\ s \neq 0 \text{ et } Q \in A[X] \text{ primitif.}$$

Pour cela, il suffit de mettre au même dénominateur tous les coefficients puis de factoriser ce dénominateur.

Le numérateur est tout simplement de contenu.

Nous savons que $K[X]$ est factoriel car $K[X]$ est principal donc on peut écrire, pour $P \in A[X]$ primitif :

$$P = \frac{r}{s}\prod_i \left(\frac{r_i}{s_i}Q_i\right)^{\alpha_i} \text{ avec } Q_i \in A[X] \text{ des polynôme primitifs distincts}$$

et les polynômes $\frac{r_i}{s_i}Q_i$ sont irréductibles dans $K[X]$.

En plus :

$$s\prod_i s_i^{\alpha_i} P = r\prod_i r_i^{\alpha_i} Q_i^{\alpha_i} \text{ dans } A[X]$$

En appliquant le contenu nous obtenons donc dans $A[X]$:

$$s\prod_i s_i^{\alpha_i} = r\prod_i r_i^{\alpha_i} \text{ donc par intégrité } P = \prod_i Q_i^{\alpha_i} \text{ dans } A[X]$$

Enfin, Q_i est primitif dans $A[X]$ et irréductible dans $K[X]$ donc par définition $Q_i \in \mathcal{F}'$.

Démonstration du théorème (suite).

$$\text{Montrons que } \mathcal{F}_{A[X]} \subset \mathcal{F}_A \cup \mathcal{F}'$$

Étape 4 : Montrons que $\mathcal{F}_{A[X]} \subset \mathcal{F}_A \cup \mathcal{F}'$.

Soit $P \in \mathcal{F}_{A[X]}$. Nous avons montré que P peut s'écrire comme produit d'éléments de $\mathcal{F}_A$ et de $\mathcal{F}'$ avec éventuellement un facteur de $A^\times$.

Mais puisque $P \in \mathcal{F}_{A[X]}$ et par étape 1, cette factorisation ne contient qu'un seul élément d'où $P \in \mathcal{F}_A$ ou $P \in \mathcal{F}'$.

Étape 5 : Il ne reste plus qu'à montrer l'unicité de la factorisation.

Pour cela, montrons le lemme suivant :

Lemme 7.3.15 - Irréductible $\Rightarrow$ premier dans $A[X]$.

Dans l'anneau $A[X]$, les éléments irréductibles sont premiers.

Démonstration du lemme. Puisque $\mathcal{F}_{A[X]} = \mathcal{F}_A \cup \mathcal{F}'$ nous avons deux cas :

• Cas où $P \in \mathcal{F}_A$:

Si $P \mid QR$ dans $A[X]$, la définition de la multiplication dans $A[X]$ implique $P \mid c(QR)$.

Nous avons alors par le lemme de Gauss que $P \mid c(Q)c(R)$. Comme A est factoriel et P est irréductible, P est premier dans A donc $P \mid c(Q)$ ou $P \mid c(R)$. Nous concluons que $P \mid Q$ ou $P \mid R$ c'est-à-dire que P est premier dans $A[X]$.

• Cas où $P \in \mathcal{F}'$:

Si $P \mid QR$ dans $A[X]$, on se ramène au cas où Q et R sont primitifs. Nous savons que $K[X]$ est factoriel et, par définition, P est irréductible dans $K[X]$ donc P est premier dans $K[X]$. Ainsi $P \mid Q$ ou $P \mid R$ dans $K[X]$. Par exemple, $Q = PS$ avec $S \in K[X]$. Comme précédemment nous avons :

$$S = \frac{r}{s}\prod_i \left(\frac{r_i}{s_i}Q_i\right)^{\alpha_i} \text{ avec } r_i, s_i, r, s, \in A \text{ et } Q_i \in A[X] \text{ primitif et irréductible dans } K[X]$$

Toujours de la même manière, en utilisant le contenu, le fait que Q, P et Q_i sont primitifs et l'intégrité,

nous obtenons :

$$Q = PS = P\prod_i Q_i^{\alpha_i} \text{ d'où } S \in A[X]$$

Nous en déduisons que $P \mid Q$ dans $A[X]$.

Démonstration du théorème (fin).

Étape 5 : Supposons maintenant que $P \in A[X] \setminus \{0\}$ admet deux factorisations en irréductibles :

$$P = p_1 \dots p_n = q_1 \dots q_m$$

On montre par récurrence que $n = m$ et que $\forall i \in [\![1, n]\!] : p_i \sim q_{\sigma(i)}$ pour $\sigma \in \mathfrak{S}_n$.
C'est exactement le même raisonnement que dans la démonstration de Principal $\Rightarrow$ Factoriel.

- Pour $n = 1$: Nous obtenons le résultat par définition de l'irréductibilité.
- Soit $n > 1$: Nous avons $p_1 \mid q_1 \dots q_m$.
  Comme p_1 est premier, il existe $j \in [\![1, m]\!]$ tel que $p_1 \mid q_j$.
  En changeant l'ordre des q_j, on peut supposer que $j = 1$.
  Comme q_1 est irréductible, $q_1 = up_1$ avec $u \in A[X]^\times$. Donc $p_1 \dots p_n = up_1q_2 \dots q_m$.
  Par intégrité de $A[X]$, $p_2 \dots p_m = uq_2 \dots q_m$.
  Par hypothèse de récurrence, $n - 1 = m - 1$ et après changement d'ordre, $\forall i \in \{2, \dots, m\} : q_i \sim p_i$.
  Puisque $q_1 \sim p_1$, on obtient le résultat.

Corollaire 7.3.16 - Anneau factoriel en plusieurs variables.
Si A est un anneau factoriel, $A[X_1, \dots, X_n]$ est aussi un anneau factoriel.

Démonstration. Il suffit de procéder par récurrence :

$$A[X_1, X_2] \cong \big(A[X_1]\big)[X_2]$$

Définition 7.3.17 - Idéaux étrangers.
Soit A un anneau commutatif et I,J deux idéaux de A.
On dit que les idéaux I et J sont *étrangers* si $I + J = A$ c'est-à-dire :

$$\exists (i, j) \in I \times J : i + j = 1$$

Rappel sur le produit d'idéal.
L'idéal produit IJ est l'idéal engendré par les produits ij pour $i \in I, j \in J$.
Bien sûr, $IJ \subset I \cap J$. De plus, si $I + J = A$ alors $IJ = I \cap J$ c'est-à-dire :

$$x \in I \cap J : x = xi + xj \in IJ$$

$\diamondsuit$

Théorème 7.3.18 - Théorème des restes chinois.
Soit A un anneau commutatif et I, J deux idéaux étrangers.
Le morphisme de projection π

$$\begin{array}{rccc} \pi : & A & \longrightarrow & {}^{A}\!/_{I} \times {}^{A}\!/_{J} \\ & a & \longmapsto & (a + I, a + J) \end{array}$$

est surjectif de noyau IJ. En particulier, nous avons un isomorphisme d'anneaux $A/(IJ) \simeq A/I \times A/J$.

Démonstration.
Il est clair que nous avons $\operatorname{Ker} \pi = I \cap J$ De plus, si I et J sont étranger $I \cap J = IJ$.
Ainsi nous avons :

$${}^{A}\!/_{\operatorname{Ker}(\pi)} \cong \operatorname{Im}(\pi)$$

Montrons la surjectivité de π. Soit x et $y \in A$.
Comme I et J sont étrangers, il existe $(i,j) \in I \times J$ tels que $1 = i + j$.
Nous avons donc :

$$i \equiv 1 \mod J \text{ et } i \equiv 0 \mod I \quad ; \quad j \equiv 1 \mod I \text{ et } j \equiv 0 \mod J$$

Ainsi $xj + yi \equiv y \mod J$ et $xj + yi \equiv x \mod I$ d'où $\pi(xj + yi) = (x + I, y + J)$ et π est surjectif.

Exemple d'utilisation de théorème chinois.

Le cas le plus connu de ce théorème est le cas $A = \mathbb{Z}$.
Pour $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, nous avons alors :

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$$

En particulier, $\mathbb{Z}/n\mathbb{Z}$ est réduit si et seulement si $\forall i : \alpha_i = 1$ et est intègre si et seulement si n est premier. $\triangle$

8. Modules sur les anneaux principaux

8.1 Définitions

Dans cette section, A est un anneau commutatif intègre et M est un A-module.

Définition 8.1.1 - Torsion.
Supposons A intègre. Soit $a \in A$ non nul et $x \in M$.

- On dit que x est *de a-torsion* si $ax = 0$.
  On note $M(a)$ l'ensemble des éléments de a-torsion.
- On dit que x est *de a^∞-torsion* s'il existe $n \geqslant 1$ tel que $a^n x = 0$.
  On note $M(a^\infty)$ l'ensemble des éléments de a^∞-torsion.
- On dit que x est *de torsion* s'il existe $b \in A \setminus \{0\}$ tel que $bx = 0$.
  On note $T(M)$ l'ensemble des éléments de torsion.
- On dit que M est *de a-torsion* si $M = M(a)$ et que M est *sans a-torsion* si $M(a) = 0$.
- On dit que M est *de a^∞-torsion* si $M = M(a^\infty)$ et que M est *sans a^∞-torsion* si $M(a^\infty) = 0$.
- On dit que M est *de torsion* si $M = T(M)$ et que M est *sans torsion* si $T(M) = 0$.

Remarque. Nous avons par définition :

$$T(M) = \bigcup_{a \in A} M(a)$$

♢

Définition 8.1.2 - Annulateur.
On appelle *annulateur* de M l'idéal $\mathrm{Ann}(M) = \Big\{ a \in A \,|\, \forall m \in M : am = 0 \Big\}$.

Exemple. Si $I \subset A$ est un idéal, alors $\mathrm{Ann}\big(A/I\big) = I$. En fait, $x \in \mathrm{Ann}\big(A/I\big)$ implique $x(1+I) = 0$, donc $x \in I$. △

Lemme 8.1.3 - Caractérisation de la torsion.
Supposons A intègre. Soit $a \in A$ non nul et $x \in M$.
Nous avons :

1. *Sous-modules :* $M(a), M(a^\infty), T(M)$ sont des sous-A-modules de M.
2. *Caractérisation de la torsion de x :*
   $x \in M$ est de torsion si et seulement si le sous-A-module $Ax \subset M$ n'est pas libre.
3. *Factorisation :*
   - Le quotient $M/M(a^\infty)$ est sans a^∞-torsion et le quotient $M/T(M)$ est sans torsion.
   - Tout morphisme $f : M \to N$ avec N sans a^∞-torsion se factorise par $M/M(a^\infty)$.
   - Tout morphisme $f : M \to N$ avec N sans torsion se factorise par $M/T(M)$.
4. *Libre et sans torsion :* Si M est libre, il est sans torsion.
5. *Cas de type fini :* Si M est de type fini alors M est de torsion si et seulement si $\mathrm{Ann}(M) \neq 0$.

Remarque. Le quotient $M/M(a)$ n'est pas nécessairement sans a-torsion.

Exemple : Si m vérifie $am \neq 0$ et $a^2 m = 0$ alors $\overline{m} \neq \overline{0}$, mais $a\overline{m} = \overline{0}$. ♢

Démonstration.

1. Traitons le cas de $T(M)$. Si $x, y \in T(M)$, il existe $a, b \neq 0$ tels que $ax = 0 = by$. On a $ab(x+y) = 0$ et $ab \neq 0$ car A est intègre donc $x + y \in T(M)$. Si $c \in A$, on a $acx = cax = 0$ donc $cx \in T(M)$. Ainsi $T(M)$ est un sous-module. L'argument pour $M(a)$ et $M(a^\infty)$ est similaire.
2. Supposons Ax libre, disons isomorphe à $A^{(I)}$. En particulier, $x \neq 0$. Comme A est intègre, la multiplication par a sur $A^{(I)} \simeq Ax$, est injective pour tout $a \neq 0$. En particulier, $\forall a \neq 0 : ax \neq 0$, donc x n'est pas de torsion.
   Réciproquement si Ax n'est pas libre, l'application linéaire $A \to Ax, a \mapsto ax$ est surjectif et donc, pas injectif. Donc, il existe $a \neq 0$ tel que $ax = 0$.
   Autrement dit, x est de torsion.
3. Soit $\overline{m} \in {}^{M}\!/_{M(a^\infty)}$ un élément de a^∞-torsion. Alors il existe $n \geqslant 1$ tel que $a^n m \in M(a^\infty)$.
   Donc il existe n' tel que $a^{n+n'} m = 0$. Finalement, $\overline{m} = 0$.
   Soit $f : M \to N$ avec N sans a^∞-torsion. On veut montrer que $M(a^\infty) \subset \operatorname{Ker} f$.
   Soit $m \in M(a^\infty)$ c'est-à-dire $a^n m = 0$. Alors $a^n f(m) = f(a^n m) = 0$ donc $f(m) \in N(a^\infty) = \{0\}$.
   L'argument pour $T(M)$ est similaire.
4. Si M est libre, puisque A est intègre, la multiplication par a sur M est injective pour tout $a \neq 0$.
   Ainsi M est sans torsion.
5. Soit M de torsion et de type fini. Soit $x_1, \ldots, x_n$ des générateurs de M :
   $$M = \sum_{i=1}^{n} Ax_i$$
   Puisque M est de torsion, il existe des $a_i \in A \setminus \{0\}$ tels que $a_i x_i = 0$.
   Alors, $a = a_1 \ldots a_n \in \operatorname{Ann}(M)$ car :
   $$aM = a \sum_{i=1}^{n} Ax_i = \sum_{i=1}^{n} Aax_i = 0$$
   Réciproquement, si $a \in \operatorname{Ann}(M)$ alors chaque $m \in M$ est de a-torsion donc M est de torsion.

8.2 Premiers théorèmes de structure

Définition 8.2.1 - Somme directe.
Soit $(M_i)_{i \in I}$ une famille de sous-modules de M.
On dit que M est *somme directe* des M_i si le morphisme $g : \bigoplus_{i \in I} M_i \to M$ induit par les inclusions $g_j : M_j \to M$ est bijectif. Dans ce cas, on écrit $M = \bigoplus_{i \in I} M_i$.

Lemme 8.2.2 - Torsion d'un module sur un anneau principal.
Soit A un anneau principal et M un module tel que :
$$M \cong A^q \oplus {}^{A}\!/_{(d_1)} \oplus \ldots \oplus {}^{A}\!/_{(d_r)} \quad \text{avec } d_1 \mid \ldots \mid d_r$$
Alors :

1. $T(M) = {}^{A}\!/_{(d_1)} \oplus \ldots \oplus {}^{A}\!/_{(d_r)}$.
2. ${}^{M}\!/_{T(M)}$ est libre de rang q.
3. $\operatorname{Ann}\big(T(M)\big) = (d_r)$.

Remarque. Ce lemme établit des résultats sur des modules qui possèdent une forme particulière.

Cependant, nous allons montrer ensuite, à l'aide du théorème de forme normale de Smith, que tous les modules de type fini sur un anneau principal sont en fait de cette forme. Ainsi toutes les propriétés énoncées ici seront vraie dans le cadre général des modules de type fini sur un anneau principal. ♢

Démonstration.

1. $\subset$: Soit $x \in T(M)$, on écrit $x = x_1 + x_2$ avec $x_1 \in A^q$ et $x_2 \in {}^{A}\!/_{(d_1)} \oplus \ldots \oplus {}^{A}\!/_{(d_r)}$.
   Soit $a \neq 0$ tel que $ax = 0$. Alors $ax_1 = 0$ donc $x_1 = 0$.
   $\supset$: Il est clair que tous les éléments de ${}^{A}\!/_{(d_1)} \oplus \ldots \oplus {}^{A}\!/_{(d_r)}$ sont de torsion.
   En effet, $x \in {}^{A}\!/_{(d_i)}$, alors $d_i x = 0$ et $x \in T(M)$.
2. Nous obtenons ce point comme conséquence de 1. car :
$$M \cong A^q \oplus T(M)$$
3. Puisque A est principal, $\mathrm{Ann}\big(T(M)\big) = (d)$ pour un $d \in A$.
   En particulier, $dA \subset (d_i)$ donc $\forall i : d_i \mid d$. De plus, $d_1 \mid \ldots \mid d_r$ et $d_i\left({}^{A}\!/_{(d_i)}\right) = 0$ donc $d_r\left({}^{A}\!/_{(d_i)}\right)$ d'où $d_r T(M) = 0$. En particulier, $d_r \in \mathrm{Ann}\big(T(M)\big)$ donc $d \mid d_r$. Finalement, $(d) = (d_r)$.

Théorème 8.2.3 - Composantes primaires des modules de torsion.
Soit A un anneau principal et M un A-module de torsion.
Soit $\mathfrak{P}$ un ensemble de représentants des éléments irréductibles de A pour la relation d'association.
Alors :
$$M = \bigoplus_{p \in \mathfrak{P}} M\big(p^\infty\big)$$
Le sous-module $M(p^\infty)$ est appelé *composante p-primaire* de M.

Démonstration. Soit $x \in M$ et $a \neq 0$ tel que $ax = 0$.
Puisque A est principal, il est factoriel. Nous écrivons la décomposition de a en irréductibles :
$$a = u p_1^{\alpha_1} \ldots p_r^{\alpha_r}$$
Pour $1 \leqslant j \leqslant r$, posons $q_j = \prod_{i \neq j} p_i^{\alpha_i}$.
Alors $\mathrm{pgcd}(q_1, \ldots, q_r) = 1$ donc d'après Prop. 7.3.9, on a $(q_1, ..., q_r) = A$. Donc, il existe $a_1, \ldots, a_r \in A$ tels que :
$$\sum_{i=1}^{r} a_i q_i = 1$$
Posons $y_j = q_j x \in M$. Alors $p_j^{\alpha_j} y_j = u^{-1} a x = 0$ donc $y_j \in M\left(p_j^\infty\right)$.
Alors :
$$x = (a_1 q_1 + \ldots + a_r q_r)x = a_1 y_1 + \ldots + a_r y_r \in \sum_{p \in \mathfrak{P}} M\big(p^\infty\big)$$
En particulier, $M = \sum_{p \in \mathfrak{P}} M(p^\infty)$. Montrons que la somme est directe.
Soit $\mathfrak{P}' \subset \mathfrak{P}$ fini et soit $x_p \in M(p^\infty)$ tels que $\sum_{p \in \mathfrak{P}'} x_p = 0$. Soit $n_p \geqslant 0$ tel que $p^{n_p} x_p = 0$. Notons :
$$t_q = \prod_{p \neq q} p^{n_p}$$
Alors $\mathrm{pgcd}\big(t_q, q^{n_q}\big) = 1$ donc il existe $a_q, b_q \in A$ tels que :
$$a_q t_q + b_q q^{n_q} = 1$$

Par ailleurs, $t_q x_p = 0$ si $p \neq q$ car $p^{n_p} \mid t_q$. Ainsi pour tout $q \in \mathfrak{P}'$ on a :

$$\begin{aligned} x_q &= \big(a_q t_q + b_q q^{n_q}\big) x_q = a_q t_q x_q \\ &= a_q t_q x_q + a_q t_q \sum_{p \in \mathfrak{P}' \setminus \{q\}} x_p \\ &= a_q t_q \left(\sum_{p \in \mathfrak{P}'} x_p \right) = 0 \end{aligned}$$

Ainsi ce module est bien libre.

Corollaire 8.2.4 - Cas de type fini.
Soit A un anneau principal et M un A-module de torsion de type fini.
Alors pour presque tout $p \in \mathfrak{P} : M(p^\infty) = (0)$ et $\forall p \in \mathfrak{P}$ il existe $n \geqslant 0$ tel que $M(p^\infty) = M(p^n)$.

Démonstration. Soit $M = \sum_{i=1}^{r} A x_i$ et $x_i = \sum_{p \in \mathfrak{P}} x_{i,p}$.

Alors l'ensemble $\mathfrak{P}' = \Big\{ p \in \mathfrak{P} \mid \exists i : x_{i,p} \neq 0 \Big\}$ est fini et $x_i \in \sum_{p \in \mathfrak{P}'} M\big(p^\infty\big)$ donc :

$$M = \sum_{p \in \mathfrak{P}'} M\big(p^\infty\big) \overset{\text{thm}}{=} \bigoplus_{p \in \mathfrak{P}'} M\big(p^\infty\big)$$

Si $p \notin \mathfrak{P}'$, alors $M(p^\infty) = (0)$. Soit $p \in \mathfrak{P}'$.
Soit $n \geqslant 1$ tel que $\forall i : p^n x_{i,p} = 0$. Alors puisque $M(p^\infty) = \sum_i A x_{i,p}$, nous avons $M(p^\infty) = M(p^n)$.

Exemple de décomposition canonique.

Soit $A = \mathbb{Z}$ et $M = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/45\mathbb{Z}$. Alors d'après le théorème chinois :

$$M \simeq \underbrace{\Big(\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}\Big)}_{M\left(2^\infty\right)} \oplus \underbrace{\Big(\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}\Big)}_{M\left(3^\infty\right)} \oplus \underbrace{\Big(\mathbb{Z}/5\mathbb{Z}\Big)}_{M\left(5^\infty\right)}$$

et $M(2^\infty) = M\Big(2^3\Big), M(3^\infty) = M\Big(3^2\Big), M(5^\infty) = M(5)$. △

8.3 Matrices à coefficients dans un anneau principal

Dans la suite nous allons étudier les matrices à coefficients dans un anneau principal.
Le but est d'établir le théorème de forme normale de Smith qui permettra d'établir le théorème de structure des modules sur un anneau principal.

Notons $\mathcal{M}_{n,p}(A)$ le A-module des matrices de taille $n \times p$. On a vu que :

$$\mathcal{M}_{n,p}(A) \simeq \mathrm{Hom}_A\big(A^p, A^n\big)$$

Nous savons que le module $\mathcal{M}_{n,p}(A)$ est libre et admet comme base canonique $E_{i,j}$. Il est donc de rang np.
Si $E_{i,j} \in \mathcal{M}_{n,p}(A)$ et $E_{k,\ell} \in \mathcal{M}_{p,q}(A)$, nous avons :

$$E_{i,j} E_{k,\ell} = \delta_{j,k} E_{i,\ell} \text{ où } \delta_{j,k} \text{ est le symbole de Kronecker}$$

Nous posons $\mathcal{M}_n(A) = \mathcal{M}_{n,n}(A)$. Alors $\mathcal{M}_n(A) \simeq \mathrm{End}_A(A^n)$ comme A-algèbre.
Nous posons $\mathsf{GL}_n(A) = \mathcal{M}_n(A)^\times$, le groupe multiplicatif des matrices de déterminant inversible.
L'ensemble $\mathsf{SL}_n(A) = \Big\{ M \in \mathsf{GL}_n(A) \mid \det M = 1 \Big\}$ est un sous-groupe de $\mathsf{GL}_n(A)$.

Définition 8.3.1 - Matrice élémentaire.
On appelle *matrice élémentaire* les matrices de $\mathsf{SL}_n(A)$ définie pour $i \neq j$ et $a \in A$ par :

$$E_{i,j}(a) = \mathrm{id} + aE_{i,j}$$

Notons $E_n(A) \subset \mathsf{SL}_n(A)$ le sous-groupe engendré par $\Big\{E_{i,j}(a) \mid \forall i, j, a \text{ avec } i \neq j\Big\}$.

Étudions l'action des matrices élémentaires :

Lemme 8.3.2 - Action des matrice élémentaires.
Soit $M \in \mathcal{M}_{n,p}(A)$ une matrice quelconque et L_i sa i^{e} ligne et C_j sa j^{e} colonne.
Alors :

- Multiplier M à gauche par une matrice élémentaire $E_{ij}(a) \in \mathsf{SL}_n(A)$ a pour effet :

$$L_i \rightsquigarrow L_i + aL_j$$

- Multiplier M à droite par une matrice élémentaire $E_{ij}(a) \in \mathsf{SL}_p(A)$ a pour effet :

$$C_j \rightsquigarrow C_j + aC_i$$

Démonstration. La preuve est identique au cas des matrices sur un corps.

Définition 8.3.3 - Équivalences matricielles.
On dit que des matrices M et N de $\mathcal{M}_{n,p}(A)$ sont :

- *équivalentes* s'il existe $P \in \mathsf{GL}_n(A)$ et $Q \in \mathsf{GL}_p(A)$ tel que $N = PMQ$. On note alors $M \sim N$.
- *S-équivalentes* s'il existe $P \in \mathsf{SL}_n(A)$ et $Q \in \mathsf{SL}_p(A)$ tel que $N = PMQ$. On note alors $M \overset{S}{\sim} N$.
- *E-équivalentes* s'il existe $P \in E_n(A)$ et $Q \in E_p(A)$ tel que $N = PMQ$. On note alors $M \overset{E}{\sim} N$.

Énoncé du théorème de la forme normale de Smith

Théorème 8.3.4 - Forme normale de Smith.
Si A est principal, toute matrice $M \in \mathcal{M}_{n,p}(A)$ non nulle est S-équivalente à une matrice de la forme :

$$D = \mathrm{diag}(d_1, \ldots, d_r, 0, \ldots, 0) \text{ avec } d_i \in A \setminus \{0\} \text{ et } d_1 \mid d_2 \mid \cdots \mid d_r$$

Si A est euclidien, M est même E-équivalente à D.
Cette forme normale de M est unique : Si $\mathrm{diag}(d_1, \ldots, d_r, 0, \ldots, 0) \sim \mathrm{diag}\big(d'_1, \ldots, d'_s, 0, \ldots, 0\big)$ alors $r = s$ et $\forall i : d_i \sim d'_i$.

Remarque.

1. Une telle matrice D est dite en forme normale de Smith.
2. L'unicité implique que la suite d'idéaux $(d_1) \supset (d_2) \supset \cdots \supset (d_r)$ ne dépend que de M.
   Ces idéaux, ou les d_i, sont appelés *facteurs invariants* de M.

♢

Démonstration du théorème de la forme normale de Smith

Pour la preuve de ce théorème, introduisons la taille $\tau(M) = \max(n, p) \geqslant 1$ de M.

- Pour $a \in A \setminus \{0\}$, nous appelons poids de a l'entier $\pi(a) = \begin{cases} \delta(a) \text{ si } A \text{ est euclidien de stathme } \delta \\ \text{nombres de facteurs irréductibles de } a \text{ sinon} \end{cases}$.
  En particulier, $\pi(a) \geqslant 0$.
- Pour $M = \big(m_{ij}\big)$ non nulle, nous appelons poids de M l'entier $\pi(M) = \min\limits_{m_{ij} \neq 0} \pi\big(m_{ij}\big)$.

✧ **Procédure de transformation**

Avant de commencer la preuve du théorème, nous allons décrire trois procédure :

1. Procédure P_1 :
   - Soit $a, b \in A$. La multiplication à droite par des matrices élémentaires permet :

$$(a \quad b) \overset{E}{\sim} (a \quad a+b) \text{ avec } C_2 \rightsquigarrow C_2 + C_1$$

$$(a \quad a+b) \overset{E}{\sim} (-b \quad a+b) \text{ avec } C_1 \rightsquigarrow C_1 - C_2$$

$$(-b \quad a+b) \overset{E}{\sim} (-b \quad a) \text{ avec } C_2 \rightsquigarrow C_2 + C_1$$

     Ainsi nous pouvons échanger les coordonnées à un signe près.
     Pour une matrice quelconque, nous pouvons échanger deux colonnes à un signe près.
   - De même, la multiplication à gauche permet d'échanger deux lignes, à un signe près.

   La procédure P_1 permet de placer tout coefficient de M en position $(1,1)$, à un signe près.

2. Procédure P_2 :
   - Soit $a, q \in A$. Nous avons alors par opération élémentaire à droite :

$$(a \quad qa) \overset{E}{\sim} (a \quad 0) \text{ avec } C_2 \rightsquigarrow C_2 - qC_1$$

     Ainsi, si un coefficient a de M divise un coefficient b de la même ligne, on peut remplacer b par 0 en ne changeant que les éléments de sa colonne.
   - De même, la multiplication à gauche par des matrices élémentaires permet de faire la même chose pour les colonnes.

   La procédure P_2 permet réduire les coefficients par ligne et par colonne.

3. Procédure P_3 :
   - Soit $a, b \in A \setminus \{0\}$ avec $a \nmid b$.
     - Si A est non euclidien, posons $d = \text{pgcd}(a,b)$. Par Prop. 7.3.9, il existe $u, v \in A$ tel que $d = au + bv$.
       En posant $a = da'$ et $b = db'$ nous avons $ub' + vb' = 1$ et $ab' = da'b' = a'b$.
       En particulier :

$$(a \quad b)\begin{pmatrix} u & -b' \\ v & a' \end{pmatrix} = (d \quad 0)$$

       ou la matrice est evidemment dans $\mathsf{SL}_2(A)$.
       Et de plus, $d \mid a$ mais d n'est pas associé à a donc $\pi(d) < \pi(a)$.
       Ainsi $(a \quad b) \overset{S}{\sim} (d \quad 0)$ avec $\pi(d) < \pi(a)$.
     - Si A est euclidien, écrivons $b = aq + r$ avec $\delta(r) < \delta(a)$.
       En particulier :

$$(a \quad b)\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = (a \quad r)$$

       Ainsi $(a \quad b) \overset{E}{\sim} (a \quad r)$ avec $\pi(r) < \pi(a)$.

✧ **Démonstration de l'existence d'une forme normale**

Démonstration du théorème (existence).

Procédons par récurrence sur $\tau(M)$.

Si $\tau(M) = 1$, M est sous forme normale de Smith. Supposons que $\tau(M) \geqslant 2$.
Quitte à appliquer la procédure P_1, nous pouvons supposer $m_{11} \neq 0$ et $\pi(m_{11}) = \pi(M)$.

S'il existe $l > 1$ tel que $m_{11} \nmid m_{1l}$ (ou $c > 1 : m_{11} \nmid m_{c1}$) alors nous appliquons la procédure P_3 :
Nous obtenons une matrice M' tel que $M \sim M'$ avec $\pi(M') < \pi(m_{11}) = \pi(M)$.
Nous recommençons le raisonnement avec M' et ce processus doit terminer car π est minoré par 0.

Sinon, m_{11} divise tous les coefficients de L_1 et C_1. Nous appliquons alors la procédure P_2 à L_1 et C_1 :

- Appliquons P_2 à $(m_{11} \quad m_{1l})$ pour chaque $l > 1$. La ligne L_1 devient $(m_{11} \quad 0 \quad \cdots \quad 0)$
- Appliquons P_2 à $(m_{11} \quad m_{c1})$ pour chaque $c > 1$. La colonne C_1 devient $(m_{11} \quad 0 \quad \cdots \quad 0)^t$.

Nous obtenons que $M \sim \begin{pmatrix} m_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & M_1 & \\ 0 & & & \end{pmatrix}$ avec $\tau(M_1) < \tau(M)$.

Par hypothèse de récurrence, il existe P_1 et Q_1 dans $\mathsf{SL}(A)$ ou $E(A)$ tel que :

$$M_1 = P_1 D_1 Q_1 \text{ avec } D_1 = \operatorname{diag}(d_2, \dots, d_r) \quad \text{et} \quad d_2 \mid d_3 \mid \cdots \mid d_r$$

Posons $P = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & P_1 & \\ 0 & & & \end{pmatrix}$ et $Q = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & Q_1 & \\ 0 & & & \end{pmatrix}$ et $D = \operatorname{diag}(m_{11}, d_2, \cdots)$ et $M = PDQ$.

- Si $m_{11} \mid d_2$, alors $M \sim D$ qui est en forme normale de Smith donc nous avons terminé.
- Sinon, nous observons que $\begin{pmatrix} m_{11} & 0 \\ 0 & d_2 \end{pmatrix} \overset{E}{\sim} \begin{pmatrix} m_{11} & d_2 \\ 0 & d_2 \end{pmatrix}$ en faisant $L_1 \rightsquigarrow L_1 + L_2$.

  Comme $m_{11} \nmid d_2$, la procédure P_3 permet de dire que $M \sim M'$ avec $\pi\big(M'\big) < \pi(M)$.
  Nous recommençons le raisonnement avec M'. Ce processus se termine car π est minoré par 0.

✧ **Idéaux engendrés par les mineurs**

Pour la démonstration de l'unicité, nous avons besoin d'introduire quelques notions :

Définition 8.3.5 - Matrice partielle.
Soit $M \in \mathcal{M}_{n,p}(A)$, $I \subset \{1, \dots, n\}$ et $J \subset \{1, \dots, p\}$.
On appelle matrice partielle $M_{I,J}$ la matrice obtenue en effaçant de M les lignes et colonnes qui n'appartienne pas à I et J. On note son déterminant par $\mu_{IJ} := \det(M_{IJ}) \in A$.

Définition 8.3.6 - Mineur et idéal engendré par les mineurs.
Soit $M \in \mathcal{M}_{n,p}(A)$, $I \subset \{1, \dots, n\}$ et $J \subset \{1, \dots, p\}$.
Si $r := |I| = |J|$, on appelle *mineur de taille r de M* l'élément μ_{IJ}.
On note $I_r(M) \subset A$ l'idéal engendré par tous les mineurs de taille r de M.

Proposition 8.3.7 - Propriété des idéaux engendré par les mineurs.
Soit $r \geqslant 1$, $M \in \mathcal{M}_{n,p}(A)$ et $N \in \mathcal{M}_{p,q}(A)$.
Les idéaux engendré par les mineurs vérifient les propriétés suivantes :

1. Invariance par transposition : $I_r\big(M^t\big) = I_r(M)$.
2. Inclusion décroissante : $I_{r+1}(M) \subset I_r(M)$.
3. Inclusion dans l'intersection : $I_r(MN) \subset I_r(M) \cap I_r(N)$.
4. Stabilité par équivalence : $I_r(PMQ) = I_r(M)$ pour $P \in \mathsf{GL}_n(A)$ et $Q \in \mathsf{GL}_p(A)$.
5. Forme normale de Smith : Soit $D = \operatorname{diag}(d_1, \dots, d_n)$ avec $d_1 \mid d_2 \mid \cdots \mid d_n$, alors :

$$I_r(D) = \begin{cases} (d_1 \dots d_r) & \text{si } 1 \leqslant r \leqslant n \\ \{0\} & \text{si } r > n \end{cases}$$

Démonstration de la proposition.

1. Le déterminant est stable par transposition : $\det(M_{IJ}) = \det\big(M_{IJ}^t\big)$.
   Ainsi nous avons l'égalité des idéaux $I_r(M) = I_r\big(M^t\big)$.
2. D'après le développement par rapport à un ligne du déterminant, tout mineur de taille $r+1$ est combinaison linéaire des mineurs de taille r. En particulier $I_{r+1}(M) \subset I_r(M)$.
3. Soit $M = \big(C_1 \mid \cdots \mid C_p\big)$ avec C_i les colonnes de M.
   Soit $N \in \mathcal{M}_{p,q}(A)$ et $MN = \Big(C'_1 \mid \cdots \mid C'_q\Big)$ avec C'_i les colonnes de MN.

Nous avons $m_{ki} = \sum_{l=1}^{p} m_{kl} n_{li}$ d'où $C'_i = \sum_{l=1}^{p} n_{li} C_l$.
Donc les colonnes de MN sont les combinaisons linéaire des colonnes de M.

Considérons une matrice partielle $(MN)_{I,J}$ de taille r avec les colonnes $\left(C''_1, \dots, C''_r\right)$.
Écrivons la première colonne $C''_1 = \sum_l n_{l1} C'_l$ comme combinaison de colonnes (de longueur r) de M.
La multilinéarité de $\det(C)$ implique que $\det(MN)_{IJ} = \sum_l m_{l1}\mu_l$ où μ_l est le déterminant de $(MN)_{I,J}$ avec la première colonne remplacé par la colonne C'_l (de longueur r) de M.

On continue avec la deuxième colonne de $(MN)_{I,J}$, etc ...

Après la discussion de la q^{e} colonne, on a donc écrit $\det(MN)_{I,J}$ comme une combinaison linéaire des mineurs de taille r de M. En particulier $I_r(MN) \subset I_r(M)$.
De plus nous obtenons directement $I_r(MN) = I_r\left(N^t M^t\right) \subset I_r\left(N^t\right) = I_r(N)$ d'où le résultat.

4. Nous avons l'égalité souhaitée en utilisant la partie 3. plusieurs fois : On a

$$A = I_r(\mathrm{Id}) = I_r\left(P^{-1}P\right) \subseteq I_r(P)$$

(et également pour Q). Donc $I_r(P) = I_r(Q) = A$. Par 3., on déduit

$$I_r(PMQ) \subset I_r(P) \cap I_r(M) \cap I_r(Q) = I_r(M).$$

Pour l'implication réciproque, on utilise 3. une troisième fois. En effet :

$$I_r(M) = I_r\left(P^{-1}PMQQ^{-1}\right) \subset I_r(PMQ).$$

5. Soit $1 \leqslant r \leqslant n$. Nous avons par définition :

$$I_r(D) = \left\langle \left\{ d_{i_1} \dots d_{i_r} \mid 1 \leqslant i_1 < i_2 < \dots < i_r \leqslant n \right\} \right\rangle$$

Puisque $d_1 \mid \dots \mid d_n$, nous avons $(d_1 \dots d_r) \mid \left(d_{i_1} \dots d_{i_r}\right)$ pour tous les $1 \leqslant i_1 < \dots < i_r \leqslant n$.
Nous avons l'égalité car $I_r(D) \subset (d_1 \dots d_r) \subset I_r(D)$ pour $i_1 = 1, \dots, i_r = r$.

Soit $r > n$. Dans ce cas, chaque matrice partielle $D_{I,J}$ contient une ligne égale à 0.
Ainsi $\mu_{I,J} = \det\left(D_{I,J}\right) = 0$ et $I_r(M) = \{0\}$.

✧ **Démonstration de l'unicité de la forme normale**

Démonstration du théorème (unicité).
Soit $D \sim D'$ avec $D = \mathrm{diag}(d_1, \dots, d_s, 0, \dots, 0)$ et $D' = \mathrm{diag}\left(d'_1, \dots, d'_t, 0, \dots, 0\right)$ en forme de Smith.
Soit $P \in \mathsf{GL}_n(A)$ et $Q \in \mathsf{GL}_p(A)$ tels que $D' = PDQ$. Par la partie 3. de la proposition précédente, $I_r(D) = I_r\left(D'\right)$ et donc :

$$s + 1 = \min\left\{ r \mid I_r(D) = 0 \right\} = \min\left\{ r \mid I_r\left(D'\right) = 0 \right\} = t + 1$$

Par la partie 5., nous avons que pour $1 \leqslant r \leqslant s$: $(d_1, \dots, d_r) = I_r(D) = I\left(D'\right) = \left(d'_1 \dots d'_r\right)$.
De plus, pour $r = 1$, on a $(d_1) = \left(d'_1\right) \Rightarrow d_1 \sim d'_1$. Supposons par récurrence que $d_i \sim d'_i$ pour tout $i < r$.
L'égalité $(d_1 \dots d_r) = \left(d'_1 \dots d'_r\right)$ implique que $u' d'_1 \dots d'_{r-1} d_r = d_1 \dots d_r = u'' d'_1 \dots d'_r$ avec $u', u'' \in A^\times$.
Ainsi $\left(d'_1 \dots d'_{r-1}\right)\left(u d_r - d'_r\right) = 0$ avec $u := u'\left(u''\right)^{-1}$ d'où par intégrité $d_r \sim d'_r$.

Étude des modules de type fini sur un anneau principal à partir de Smith

Nous allons à présent utiliser ce théorème pour étudier la structure des modules de type fini sur un anneau principal. Presque tous les résultats suivants sont des corollaires du théorème de forme normale 8.3.4.

Lemme 8.3.8 - Sous module d'un anneau noethérien.
Soit A un anneau noethérien et $n \geqslant 1$. Alors tout sous-module M de A^n est de type fini.
Si A est principal, tout sous-module de A^n est engendré par au plus n éléments.

Démonstration.

Montrons le premier point par récurrence sur n.

Si $n = 1$, c'est clair par définition d'un anneau noethérien.

Soit $n > 1$. Alors nous avons :

$$A^{n-1} = \bigoplus_{i=1}^{n-1} Ae_i \hookrightarrow \bigoplus_{i=1}^{n} Ae_i = A^n$$

Par hypothèse de récurrence, $M \cap A^{n-1}$ est de type fini.

De plus, $M \hookrightarrow A^n$ induit par factorisation : ${}^{M}\!/_{N} \hookrightarrow {}^{A^n}\!/_{A^{n-1}} \cong A$ avec $N = M \cap A^{n-1}$.

Par hypothèse de récurrence, ${}^{M}\!/_{N}$ est de type fini.

Puisque N et ${}^{M}\!/_{N}$ sont de type fini, M est de type fini.

Montrons le second point par récurrence sur n.

Si $n = 1$, il est clair que A^n est engendré par au plus n élément.

Soit $n > 1$. $M \subset A^n$. Posons $N = M \cap A^{n-1}$. Par hypothèse, N est engendré par $n-1$ éléments.

De plus, ${}^{M}\!/_{N} \hookrightarrow A$ est engendré par un élément donc M est engendré par au plus n éléments.

Théorème de la base adaptée

Abordons à présent un théorème important pour l'étude de la structure d'un module sur un anneau principal.

Théorème 8.3.9 - Théorème de la base adaptée.

Soit A un anneau principal et L un A-module libre de type fini de rang l et $K \subset L$ un sous-module.

Alors K est un A-module libre de rang $k \leqslant l$. Il est donc de type fini.

De plus, il existe $d_1, \dots, d_k \in A$ non nuls et une base $\{f_1, \dots, f_l\}$ de L tels que :

$$d_1 \mid \cdots \mid d_k \quad \text{et} \quad \{d_1 f_1, \dots, d_k f_k\} \text{ est une base pour } K$$

La suite d'idéaux $(d_1) \supset \cdots \supset (d_k)$ ne dépend que de L et K.

Remarque. Attention ce théorème utilise crucialement le fait que A est principal. ♢

Démonstration.

D'après le lemme, K est de type fini puisque pour une base fixé, $L \cong A^l$.

Ainsi K est un sous-module de A^l et est engendré par $k \leqslant l$ éléments. Choisissons k minimal. Soit $\phi_x : A^k \twoheadrightarrow K$ le morphisme associé au choix des k générateurs $x = (x_1, \dots, x_k)$. Notons $u : A^k \to K \hookrightarrow L$ la composée.

Choisissons des bases pour A^k et L et soit $M \in \mathcal{M}_{l,k}(A)$ la matrice de u.

Le théorème de Smith assure l'existence d'un entier $r \leqslant \min(k, l) = k$ et de $d_1, \dots, d_r \in A \setminus \{0\}$ avec $d_1 \mid \cdots \mid d_r$ tels qu'il existe des bases $(a_1, \dots, a_k)$ de A^k et $\{f_1, \dots, f_l\}$ de L vérifiant :

$$u(a_i) = \begin{cases} d_i f_i & \text{si } 1 \leqslant i \leqslant r \\ 0 & \text{si } i > r \end{cases}$$

Puisque $K = \operatorname{im}(\phi_x) \cong \operatorname{im}(u)$ et k minimal, nous avons $k = r$.

En plus, puisque $\{f_1, \dots, f_l\}$ est une base donc une famille libre, la famille $\big(u(a_1), \dots, u(a_r)\big)$ est aussi libre.

En particulier, u est injective donc ϕ_x est injective. Mais puisque $K = \operatorname{im}(\phi_x)$, nous avons un isomorphisme $\phi_x : A^k \xrightarrow{\sim} K$ donc K est libre de rang k et $\big\{u(a_1), \dots, u(a_r)\big\} = \{d_1 f_1, \dots, d_r f_r\}$ est une base de K.

Montrons enfin l'unicité de la suite d'idéaux :

Supposons que $d'_1, \dots, d'_k$ et $f'_1, \dots, f'_l$ satisfont aussi la conclusion du théorème. Montrons que $d_i \sim d'_i$.

En particulier le morphisme $\iota : K \hookrightarrow L$ est donné dans les deux bases par les deux matrices :

$$D = \operatorname{diag}(d_1, \dots, d_k, 0, \dots, 0) \text{ et } D' = \operatorname{diag}\Big(d'_1, \dots, d'_k, 0, \dots, 0\Big)$$

De plus $D \sim D'$ via les matrices de passages.

L'unicité du théorème de Smith donne que $\forall i : d_i \sim d'_i$ et les idéaux ne dépendent pas du choix de base.

8.4 Théorème de structure principal

Achevons l'étude par le théorème de structure :

Théorème 8.4.1 - Théorème de structures des modules sur un anneau principal.
Soit A un anneau principal et M un A-module de type fini.
Alors il existe $n \in \mathbb{N}$ et $d_1, \dots, d_n \in A$ non inversibles tels que $d_1 \mid \cdots \mid d_n$ et qu'il existe un isomorphisme :

$$M \cong {}^{A}\!/_{(d_1)} \oplus \cdots \oplus {}^{A}\!/_{(d_n)}$$

L'entier n et la suite d'idéaux $(d_1) \supset \cdots \supset (d_n)$ ne dépendent que de M.
Les d_i sont appelés facteurs invariants de M.

Remarque. Si q est le nombre de facteurs invariants de M nuls et $r = n - q$.
Alors nous avons :

$$M \cong A^q \oplus {}^{A}\!/_{(d_1)} \oplus \cdots \oplus {}^{A}\!/_{(d_r)} \cong {}^{M}\!/_{T(M)} \oplus T(M)$$

Avec $d_1, \dots, d_r$ non nuls et non inversible tels que $d_1 \mid \cdots \mid d_r$.
Les entiers q et r et la suite (d_i) ne dépendent que de M. L'entier q est appelé le rang de M. ♢

Avant de montrer ce théorème, nous avons besoin d'un lemme :

Lemme 8.4.2
Soit A un anneau principal, $d \in A$ et $E = {}^{A}\!/_{(d)}$.
Pour tout élément irréductible $p \in A$ et $h \geqslant 1$, notons $k = {}^{A}\!/_{(p)}$ et $E_h = {}^{p^{h-1}E}\!/_{p^h E}$ un A-module quotient.
Alors E_h est un k-espace vectoriel de dimension 1 si $p^h \mid d$ et 0 sinon.

Démonstration.
Le morphisme A-linéaire s est surjectif :

$$\begin{array}{rccll} s : & A & \longrightarrow & E_h & \text{où } \overline{a} = a \mod d \in E \\ & a & \longmapsto & p^{h-1}\overline{a} \mod p^h E & \end{array}$$

Le noyau de ce morphisme est $\mathrm{Ker}(s) = \left\{ a \in A \mid p^{h-1}a \in \left(d, p^h\right) \right\}$.

- Si $p^h \mid d$, alors $\left(d, p^h\right) = \left(p^h\right)$.
  Ainsi $\mathrm{Ker}(s) = \left\{ a \in A \mid p^h \mid p^{h-1}a \right\} = \left\{ a \in A \mid p \mid a \right\} = (p)$. En particulier $\overline{s} : {}^{A}\!/_{(p)} \xrightarrow{\sim} E_h$.
- Si $p^h \nmid d$ alors $\left(d, p^h\right) = \left(p^t\right)$ pour $t \leqslant h-1$ car puisque A est principal, $\left(d, p^h\right) = (b)$ avec $b \mid p^h$ et $b \mid d$. Ainsi $b = up^t$ avec $u \in A^\times$, avec $t \leqslant h-1$. Nous avons donc $p^{h-1} \in (b) = \left(d, p^h\right)$.
  C'est-à-dire $1 \in \mathrm{Ker}(s)$ d'où $\mathrm{Ker}(s) = A$. Ainsi, l'application surjective s est nulle donc $E_h = \{0\}$.

Démonstration du théorème de structure.
Soit n le nombre minimal d'éléments d'un système de générateur de M.
Soit $\phi_x : A^n \twoheadrightarrow M$ le morphisme associé au choix d'une famille de générateur $x = (x_1, \dots, x_n)$.

D'après le théorème de la base adaptée, $K = \mathrm{Ker}(\varphi_x)$ est libre de rang $r \leqslant n$ et il existe $d_1, \dots, d_r \in A \backslash \{0\}$ tel que $d_1 \mid \cdots \mid d_r$ et une base $(f_1, \dots, f_n)$ de $L = A^n$ tel que $\{d_1 f_1, \dots, d_r f_r\}$ soit une base de K.

Posons $q = n - r$ et complétons le système de facteurs invariant par $d_{r+1} = d_{r+2} = \cdots = d_n = 0$.

Nous observons que :

$$M \cong {}^{A^n}\!/_{K} = {}^{\bigoplus_{i=1}^{n} Af_i}\!/_{\bigoplus_{i=1}^{n} Ad_i f_i}$$
$$\cong A^q \oplus {}^{A}\!/_{(d_1)} \oplus \cdots \oplus {}^{A}\!/_{(d_r)}$$

De plus, n a été choisi minimal, donc $\forall i : {}^{A}\!/_{(d_i)} \neq 0$ car sinon M serais engendré par $n-1$ éléments.

Ainsi $\forall i : d_i \notin A^\times$. Cela montre donc l'existence d'un telle décomposition.

Montrons à présent l'unicité de cette décomposition. Soit M un A-module.
Nous allons montrer que n et les coefficients d_i d'une décomposition :

$$M \cong {}^{A}\!/_{(d_1)} \oplus \cdots \oplus {}^{A}\!/_{(d_n)} \text{ avec } d_1 \mid \cdots \mid d_n \text{ et } d_i \in A \setminus A^\times$$

sont, à association près, uniquement déterminés par M. Pour cela, nous allons les reconstruire à partir de M. Commencons avec les d_i. Posons $d_0 = 1$. Soit $0 \leqslant r \leqslant n$ maximal tel que $d_i \neq 0$ pour $i \leqslant r$. Alors

$$T(M) \cong {}^{A}\!/_{(d_1)} \oplus \cdots \oplus {}^{A}\!/_{(d_r)}$$

et $q := n - r$ est le rang de $M/T(M)$. En particulier, le nombre q est uniquement déterminé par M. Il suffit à présent de reconstruire les quotients $\dfrac{d_{i+1}}{d_i} \in \mathrm{Frac}(A)$ pour $i \leqslant r-1$ (et donc $d_i \neq 0$) et de montrer que n est uniquement déterminé par M.

Fixons $p \in A$ un irréductible.

Notre objectif est de calculer la multiplicité de p dans le quotient $\dfrac{d_{i+1}}{d_i}$ à partir de M.
La connaissance de ces valuations pour tout p permet de reconstruire la suite $d_1, ..., d_r$, à des inversibles près.

Soit $k = {}^{A}\!/_{(p)}$. Posons $\delta_p(h) := \dim_k \left({}^{p^{h-1}M}\!/_{p^h M} \right)$ pour $h \geqslant 1$. Si $E_i = {}^{A}\!/_{(d_i)}$ alors :

$${}^{p^{h-1}M}\!/_{p^h M} \cong \bigoplus_{i=1}^{n} {}^{p^{h-1}E_i}\!/_{p^h E_i}$$

D'après le lemme précédent, $\delta_p(h) = \#\left\{ i \in \{1, \ldots, n\} \;\middle|\; p^h \mid d_i \right\}$.

De plus, $d_1 \mid \cdots \mid d_n$ implique que $\left[\delta_p(h) = n - i \Leftrightarrow p^h \nmid d_i \text{ et } p^h \mid d_{i+1} \right]$ pour $i \in \{0, \ldots, n-1\}$. Ainsi pour $i \in \{0, \ldots, r-1\}$:

$$\sharp \delta_p^{-1}(n-i) = \#\left\{ h \geqslant 1 \mid p^h \nmid d \text{ et } p^h \mid d_{i+1} \right\} = v_p\left(\frac{d_{i+1}}{d_i} \right) \tag{8.1}$$

Où $v_p : \mathrm{Frac}(A) \setminus \{0\} \to \mathbb{Z}$ est la multiplicité de p.

Pour tout $p \in \mathfrak{P}$, les $v_p\left(\dfrac{d_{i+1}}{d_i} \right)$ sont déterminé à partir des fonctions δ_p, elle même uniquement déterminée par M. Ainsi, puisque A est factoriel, les quotients qui sont $\dfrac{d_{i+1}}{d_i}$ déterminés à association près à partir de M et donc par récurrence, nous pouvons reconstruire la suite des d_i.

Finalement, pour montrer l'unicité de n, on peut supposer que $r \geqslant 1$ (sinon $q = n$). Donc d_1 est non nul et non inversible. Nous considérons $h \in \mathbb{N}$ et un irréductible p tel que $p^h \mid d_1$.
Alors d'après (8.1) pour $i = 0$, nous avons $\delta_p(h) = n$ et le nombre n est également intrinsèquement lié à M.

Remarque sur la valuation.

Tout $x \in \mathrm{Frac}(A)$ non nul s'écrit uniquement comme $x = u \prod_{p \in \mathfrak{P}} p^{v_p(x)}$ avec $u \in A^\times$.

Nous remarquons alors que dans ce cas, la fonction v_p est à valeur dans $\mathbb{Z}$ car :

$$\frac{p^a}{p^b} = p^{a-b}$$

♢

Corollaire 8.4.3 - Module de type fini sans torsion.
Si A est principal, tout A module de type fini sans torsion est libre.

Démonstration. Dans la situation du théorème, tous les (d_i) sont nuls et donc :

$$M \cong A^q$$

En effet, sinon le module $A/(d_i)$ est de d_i-torsion et $T(M) \neq 0$ ce qui contredit les hypothèses.

Pour $A = \mathbb{Z}$, nous obtenons un résultat de structure des groupes abéliens de type fini :

Corollaire 8.4.4 - Théorème de structure des groupes abéliens de type fini.
Soit G un groupe abélien de type fini.
Alors il existe un unique entier $q \geqslant 0$ et une unique suite $d_1, \dots, d_r$ d'entiers $\geqslant 2$ tels que $d_1 \mid \cdots \mid d_r$ et :

$$G \cong \mathbb{Z}^q \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}$$

Étude des hypothèses.

1. Dans le théorème, l'hypothèse *de type fini* est essentielle :
   Le $\mathbb{Z}$-module $\mathbb{Q}$ est sans torsion mais n'est pas libre.
2. Dans le théorème, l'hypothèse A *principal* est essentielle :
   Si $A = \mathbb{Z}[X]$, l'idéal $(2, X)$ est sans torsion et de type fini mais n'est pas libre comme A-module.

♢

Comparaison des deux théorèmes de structure.
Soit M de type fini et de torsion. La décomposition en composantes primaires de M (8.2.3) est canonique mais moins fine que la décomposition du théorème précédent 8.4.1.

En effet, soit M tel que :

$$M \cong A/(d_1) \oplus \cdots \oplus A/(d_r) \text{ avec } d_1 \mid \cdots \mid d_r \text{ et } d_i \neq 0$$

Alors il existe une famille d'irréductibles distincts $\mathfrak{P} = \{p_1, \dots, p_s\} \subset A$ tel que :

$$d_i = u_i p_1^{\alpha_1(i)} \cdots p_s^{\alpha_s(i)} \text{ avec } \alpha_k(i) \geqslant 0$$

Ainsi d'après le théorème chinois :

$$A/(d_i) \cong \bigoplus_{j=1}^{s} A/\left(p_j^{\alpha_j(i)}\right)$$

Nous avons donc en regroupant bien les facteurs :

$$\begin{aligned} M &\cong A/(d_1) \oplus \cdots \oplus A/(d_r) \\ &\cong \bigoplus_{j=1}^{s} A/\left(p_j^{\alpha_j(1)}\right) \oplus \cdots \oplus \cong \bigoplus_{j=1}^{s} A/\left(p_j^{\alpha_j(r)}\right) \\ &\cong \left(\bigoplus_{i=1}^{r} A/\left(p_1^{\alpha_1(i)}\right)\right) \oplus \cdots \oplus \left(\bigoplus_{i=1}^{r} A/\left(p_s^{\alpha_s(i)}\right)\right) \\ &\cong M\left(p_1^{\infty}\right) \oplus \cdots \oplus M\left(p_s^{\infty}\right) \end{aligned}$$

car l'image de $\bigoplus_{i=1}^{r} A/\left(p_k^{\alpha_k(i)}\right)$ dans M est exactement $M\left(p_k^{\infty}\right)$. ♢

Partie II

Extensions de corps

1. Notions générales de la théorie des extensions

Pour toute cette partie, posons $(K, +, \cdot)$ un corps.

1.1 Définitions générales

Définition 1.1.1 - Sous-corps et extension.
Soit K un corps.
On appelle *sous-corps* tout sous-ensemble $F \subseteq K$ tel que $(F, +, \cdot)$ est lui-même un corps :

$$1 \in F \quad \text{et} \quad \forall a, b \in F : a - b \in F \text{ et } ab^{-1} \in F$$

On appelle *extension de corps* de K tout corps E dont K est un sous-corps et nous la notons E/K.
Enfin, nous appelons *corps intermédiaire* de l'extension E/K tout sous-corps L de E tel que $K \subseteq L \subseteq E$.

Questions clés

Soit $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in K[X]$ un polynôme non nul.

- Y a-t-il a toujours une extension E/K tel que f a un zéro dans E ?
- Quel est le nombre maximal de zéros de f dans une extension E/K fixée ?

Afin de répondre à ces questions, introduisons la notion de compositum qui repose sur le fait suivant :

Si $(L_i)_{i \in I}$ est une famille de corps intermédiaires de E/K, alors l'intersection $\bigcap_{i \in I} L_i$ est un corps intermédiaire de E/K.

Définition 1.1.2 - Compositum de sous-corps.
Soit E un corps et F, L deux sous-corps de E.
On appelle *compositum* de F et L dans E le sous-corps FL défini par :

$$FL = \bigcap_{\substack{F, L \subseteq k \subseteq E \\ k \text{ ss-corps}}} k$$

C'est le plus petit sous-corps de E contenant F et L.

Définition 1.1.3 - Extension engendrée par des éléments.
Soit E/K une extension et $b_1, \ldots, b_m \in E$.
On appelle *sous-corps de E engendré sur K par $b_1, \ldots, b_m$* le sous-corps $K(b_1, \ldots, b_m)$ défini par :

$$K(b_1, \ldots, b_m) = \bigcap_{\substack{b_i \in k \\ K \subseteq k \subseteq E \\ k \text{ ss-corps}}} k$$

Lorsque $E = K(b_1, \ldots, b_m)$, on dit que l'extension E/K et *de type fini* et *engendré sur K par les b_i*.

Remarque. $K(b_1, \ldots, b_m)$ est le plus petit sous-corps de E qui contient K et $b_1, \ldots, b_m$. ♢

Définition 1.1.4 - Degré d'une extension.
Soit E/K une extension.

Alors E est un espace vectoriel sur K et on appelle *degré* de E/K la quantité :

$$[E : K] := \dim_K(E) \in \mathbb{N} \cup \{+\infty\}$$

Si $[E : K] < +\infty$, on dit que E/K est *une extension finie*.

Premiers exemples d'extension.

- $\mathbb{C} = \mathbb{R}\left(\sqrt{-1}\right)$ et $[\mathbb{C} : \mathbb{R}] = 2$.
- Pour le corps $\mathbb{Q}(X) := \mathrm{Frac}\big(\mathbb{Q}[X]\big)$, on a $\big[\mathbb{Q}(X) : \mathbb{Q}\big] = +\infty$. En fait, $\left\{1, X, X^2, \ldots\right\}$ est une famille $\mathbb{Q}$-libre dans $\mathbb{Q}(X)$.
- $[\mathbb{R} : \mathbb{Q}] = +\infty$ (preuve ?).

△

Remarque. Si E/K est une extension et $b \in E$, alors $K(b) \subseteq E$ est le sous-ensemble de tous les quotients d'éléments non nuls de la forme $a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$ avec $a_i \in K$ et zéro. En fait, tous ces quotients et zéro forment un corps qui contient K et b et chaque sous-corps de E qui contient K et b contient ce corps. ♢

Lemme 1.1.5 - Forme des extensions finies.
Soit E/K une extension finie. Alors, E/K est de type fini, i.e. il existe $b_1, \ldots, b_n \in E$ tels que :

$$E = K(b_1, \ldots, b_n)$$

Démonstration. Soit $b_1, \ldots, b_n$ une base de E comme K-espace vectoriel. Soit $e \in E$. Alors nous avons :

$$e = \sum_{i=1}^{n} \lambda_i b_i \text{ avec } \lambda_i \in K.$$

Ainsi $e \in K(b_1, \ldots, b_n)$ et donc $E \subseteq K(b_1, \ldots, b_n)$. L'inclusion réciproque est évidente d'où le résultat.

Lemme 1.1.6 - Compositum d'un corps intermédiaire.
Soit $b_1, \ldots, b_m \in E$ et L un corps intermédiaire de E/K.
Nous avons $K(b_1, \ldots, b_m)L = L(b_1, \ldots, b_m)$.

Démonstration.
Nous savons que $K(b_1, \ldots, b_m)L$ est le plus petit sous-corps de E contenant : $K(b_1, \ldots, b_m)$ et L
c'est-à-dire contenant : $K, b_1, \ldots, b_m, L$
Or $K \subset L$ donc c'est-à-dire contenant : $b_1, \ldots, b_m, L$
Ce qui est par définition le corps $L(b_1, \ldots, b_m)$ d'où le résultat.

Théorème 1.1.7 - Formule des degré.
Soit E/K une extension et soit L un corps intermédiaire. Alors :

$$[E : K] = [E : L] \cdot [L : K]$$

En particulier, E/K est finie si et seulement si E/L et L/K sont finies.

Démonstration. Soit $\{x_i\}_{i \in I}$ une base de L sur K et $\{y_j\}_{j \in J}$ une base de E sur L.
Alors $B = \{x_i y_j\}_{i,j}$ est une base de E/K. En effet :

- B est libre : Soit $\sum_{i,j} a_{ij} x_i y_j = 0$ avec $a_{ij} \in K$ et $a_{ij} = 0$ sauf pour un nombre fini.

Nous avons alors : $\sum_i \Big(\sum_j a_{ij}x_i\Big)y_j = 0.$
Donc puisque $\{y_j\}_{j\in J}$ est une base de E sur L : $\forall j : \sum_i a_{ij}x_i = 0$
Enfin puisque $\{x_i\}_{i\in I}$ est une base de L sur K : $\forall i,j : a_{ij} = 0.$

- B est génératrice : Soit $z \in E$.
  Alors $z = \sum_j b_j x_j$ avec $b_j \in L$ et $b_j = 0$ sauf pour un nombre fini.
  De plus, $b_j = \sum_i a_{ij}x_i$ avec $a_{ij} \in K$ et $a_{ij} = 0$ sauf pour un nombre fini. D'où :

$$z = \sum_{i,j} a_{ij}x_i y_j$$

1.2 Éléments algébriques

Définition 1.2.1 - Élément algébrique.
Soit E/K une extension.
Un élément $b \in E$ est dit *algébrique sur* K s'il existe $P \in K[X]$ non nul tel que $P(b) = 0$ dans E.
Une extension est dite *algébrique* si tous ses éléments sont algébriques.

Remarque. Tout élément $b \in K$ est algébrique sur K (en fait $P(b) = 0$ pour $P(X) = X - b \in K[X]$). ♢

Théorème 1.2.2 - Finie implique algébrique.
Si E/K est finie alors E/K est algébrique.

Démonstration. Soit $b \in E$.
Premier cas : Si la famille $\{1, b, b^2, \dots\}$ est infinie, alors elle n'est pas libre sur K :

$$\exists a_1, \dots, a_n \in K : \sum_{i=0}^{n} a_i b^i = 0 \text{ et } \exists k : a_k \neq 0$$

Posons $P = \sum_i a_i X^i$. Alors P est non nul et $P(b) = 0$ donc b est algébrique sur K.

Deuxième cas : Si la famille $\{1, b, b^2, \dots\}$ est finie, alors il existe $m \geqslant 0$ tel que $b^m = 1$.
Posons $P = X^m - 1$. Alors P est non nul et $P(b) = 0$ donc b est algébrique sur K.

Exemples.

- L'extension $\mathbb{C}/\mathbb{R}$ est finie, donc algébrique.
- L'extension $\mathbb{Q}(X)/\mathbb{Q}$ n'est pas algébrique : l'élément X n'est pas algébrique sur $\mathbb{Q}$, car $\{1, X, X^2, \dots\}$ est une famille $\mathbb{Q}$-libre (voir au-dessus).
- L'extension $\mathbb{R}/\mathbb{Q}$ n'est pas algébrique : par exemple les éléments $e = \exp(1)$ et π ne sont pas algébrique sur $\mathbb{Q}$ mais sont des nombres transcendants (preuve ?)

△

Définition 1.2.3 - Morphisme de corps.
Soit K et L deux corps.
Un morphisme de corps $\sigma : K \to L$ est un morphisme d'anneaux de K dans L.

Remarque.

1. Un morphisme de corps σ est toujours injectif car son noyau est un est un idéal propre de K.
   Ainsi puisque $\sigma(1) = 1$, $\mathrm{Ker}(\sigma) \neq K$ donc $\mathrm{Ker}(\sigma) = \{0\}$.
2. L'image de σ est un sous-corps de L. Nous identifierons souvent K à son image dans L.
   Nous écrirons simplement $K \subset L$ au lieu de $K \to L$.
3. Un morphisme $\sigma : K \to K$ qui est surjectif est appelé automorphisme de K.

♢

Définition 1.2.4 - Automorphisme de E qui préserve K.
Soit E/K une extension. On note $\mathrm{Aut}\big(E/K\big)$ l'ensemble des automorphisme σ de E avec $\sigma_{|K} = \mathrm{id}_K$.

Remarque.
L'ensemble $\mathrm{Aut}\big(E/K\big)$ est un sous-groupe de l'ensemble $\mathrm{Aut}(E)$ des automorphismes de E. ♢

Exemple d'automorphisme préservant K.
Considérons l'extension $\mathbb{C}/\mathbb{R}$.
La conjugaison $\tau : z \mapsto \overline{z}$ est un élément de $\mathrm{Aut}\big(\mathbb{C}/\mathbb{R}\big)$. On va voir plus tard que $\mathrm{Aut}\big(\mathbb{C}/\mathbb{R}\big) = \{\mathrm{id}, \tau\}$. △

Lemme 1.2.5 - Image d'extension.
Soit $\sigma : K \to L$ un morphisme.

1. Si $E \subseteq K$ est un sous-corps et $a_1, \ldots, a_n \in K$, on a $\sigma\big(F(a_1, \ldots, a_n)\big) = \sigma(F)\big(\sigma(a_1), \ldots, \sigma(a_n)\big)$.
2. Si $F, E \subseteq K$ sont des sous-corps, on a $\sigma(F \cap E) = \sigma(F) \cap \sigma(E)$ et $\sigma(FE) = \sigma(F)\sigma(E)$.

Démonstration.
Montrons le premier point.
L'ensemble $\sigma(F)\big(\sigma(a_1), \ldots, \sigma(a_n)\big) \overset{\text{def}}{=}$ le plus petit sous-corps contenant $\sigma(F)$ et $\sigma(a_1), \ldots, \sigma(a_n)$.
Ainsi $F' := \sigma(F)\big(\sigma(a_1), \ldots, \sigma(a_n)\big) \subseteq \sigma\big(F(a_1, \ldots, a_n)\big)$ et $\sigma^{-1}\big(F'\big) \subseteq F(a_1, \ldots, a_n)$.
Mais F, $a_1, \ldots, a_n$ sont contenu dans $\sigma^{-1}\big(F'\big)$ donc $F(a_1, \ldots, a_n) \subseteq \sigma^{-1}\big(F'\big)$ d'où $\sigma\big(F(a_1, \ldots, a_n)\big) = F'$.

Montrons le second point.
Le morphisme σ est injectif donc $\sigma(E \cap F) = \sigma(E) \cap \sigma(F)$.
D'autre part, $\sigma(F)\sigma(E)$ est le plus petit sous-corps qui contient $\sigma(F)$ et $\sigma(E)$ donc $N = \sigma(F)\sigma(E) \subseteq \sigma(FE)$ et nous avons $\sigma^{-1}(N) \subset FE$. Mais $F, E \subset \sigma^{-1}(N)$ d'où $FE \subset \sigma^{-1}(N)$ ce qui conclut que $\sigma(FE) = N = \sigma(F)\sigma(E)$.

Remarque. Soit $\sigma, \tau : K \to L$. Alors $F = \Big\{z \in K \mid \sigma(z) = \tau(z)\Big\}$ est un sous-corps de K. ♢

Retournons à la première de nos questions clés. Soit $f = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$ non nul.

- Y a-t-il a toujours une extension E/K tel que f a un zéro dans E ?

Théorème 1.2.6 - Image des zéros.
Soit E/K et F/K deux extensions et $\sigma : E \to F$ un morphisme avec $\sigma_{|K} = \mathrm{id}_K$.
Si $\beta \in E$ est un zéro de f dans E alors $\sigma(\beta)$ est un zéro de f dans F.

Démonstration. Nous avons simplement :

$$\begin{aligned} 0 = \sigma(0) = \sigma\big(f(\beta)\big) &= \sigma\big(a_n\beta^n + \cdots + a_1\beta + a_0\big) \\ &= \sigma(a_n)\sigma\big(\beta^n\big) + \cdots + \sigma(a_1)\sigma(\beta) + \sigma(a_0)\sigma(1) \\ &= a_n\sigma(\beta)^n + \cdots + a_1\sigma(\beta) + a_0 = f\big(\sigma(\beta)\big) \end{aligned}$$

Corollaire 1.2.7 - Minoration du nombre de zéros.
Soit β un zéro de f. Si $E = K(\beta)$ alors le morphisme suivant est injectif :

$$\begin{array}{rccc} \mathrm{ev}_\beta : & \mathrm{Aut}\big(E/K\big) & \longrightarrow & \text{Ensemble des zéros de } f \text{ dans } E \\ & \sigma & \longmapsto & \sigma(\beta) \end{array}$$

En particulier $\#\,\mathrm{Aut}\big(E/K\big) \leqslant \#\{\text{zéros de } f \text{ dans } E\}$.

Remarque. Ce morphisme est bien défini d'après le théorème précédent. ♢

Démonstration. Soit $\sigma, \tau \in \mathrm{Aut}\big(E/K\big)$ avec $\sigma(\beta) = \tau(\beta)$.

Alors $\sigma = \tau$ sur $K(\beta)$ car les éléments non nuls de $K(\beta)$ sont des quotients d'éléments de la forme $c_k\beta^k + c_{k-1}\beta^{k-1} + \cdots + c_1\beta + c_0$ avec $c_i \in K$ et que $\sigma_{|K} = \tau_{|K} = \mathrm{id}_K$. Ainsi l'application ev_β injective.

Nous remarquons que pour répondre à notre deuxième question clé, il faut étudier les groupes $\mathrm{Aut}\big(E/K\big)$.

2. Compléments sur les groupes et les polynômes

2.1 Classes modulo un sous-groupe

Définition 2.1.1 - Relation modulo U.
Soit G un groupe et $U \subseteq G$ un sous-groupe (pas nécessairement normal).
On introduit la relation d'équivalence :

$$\forall a, b \in G : a \sim b \Leftrightarrow a^{-1}b \in U$$

Les classes d'équivalences $aU := \left\{au \mid u \in U\right\}$ sont appelées *classes à gauche modulo U*.
De manière équivalence nous définissons la relation d'équivalence :

$$\forall a, b \in G : a \sim' b \Leftrightarrow ba^{-1} \in U$$

Les classes d'équivalences $Ua := \left\{ua \mid u \in U\right\}$ sont appelées *classes à droite modulo U*.

Proposition 2.1.2 - Cardinal des classes.
Soit G un groupe et $U \subseteq G$ un sous-groupe.
Toute classe à gauche ou à droite modulo U est de même cardinal que U.

Démonstration. L'application $u \mapsto au$ (resp. $u \mapsto ua$) est une bijection entre U et aU (resp. entre U est Ua).

Définition 2.1.3 - Indice d'un sous-groupe.
Soit G un groupe et $U \subseteq G$ un sous-groupe.
On appelle *indice* de U dans G la quantité $[G : U] = \#\left(G/\sim\right)$ qui est le nombre de classes à gauche.

Remarque. La quantité $[G : U] = \#\left(G/\sim\right)$ est aussi le nombre de classes à droite : en fait, l'involution $a \mapsto a^{-1}$ de G induit une bijection $aU \mapsto Ua^{-1}$ entre les ensembles $G/\sim$ et $G/\sim'$. ♢

Proposition 2.1.4 - Formule des indices.
Soit G un groupe, K et H deux sous-groupes tels que $K \subseteq H \subseteq G$.
Alors $[G : K] = [G : H] \cdot [H : K]$.

Démonstration.

- Soit $\{g_i\}_i$ un système de représentants de G modulo H.
- Soit $\left\{h_j\right\}_j$ un système de représentants de H modulo K.

Alors $\left\{g_i h_j\right\}_{ij}$ est un système de représentants de G modulo K. En effet, soit $g \in G$.
Il existe i tel que $g \in g_i H \Rightarrow g_i^{-1} g \in H \Rightarrow \exists j : g_i^{-1} g \in h_j K \Rightarrow g \in g_i h_j K$. Ainsi $G = \bigcup_{i,j} g_i h_j K$.
De plus, cette réunion est disjointe car :

$$g_i h_j K = g_{i'} h_{j'} K \Rightarrow g_i H = g_{i'} H \Rightarrow g_i = g_{i'} \Rightarrow h_j K = h_{j'} K \Rightarrow h_j = h_{j'}$$

Définition 2.1.5 - Ordre.

Soit $a \in G$. On appelle *ordre de* a la quantité $\text{ord}(a) = \min\left\{n \in \mathbb{N} \mid a^n = 1\right\} \in \mathbb{N} \cup \{+\infty\}$.

Théorème 2.1.6 - Théorème de Lagrange.
Soit G un groupe fini et U un sous-groupe.
Alors $\#U$ divise $\#G$ et nous avons :

$$\#G = [G : U] \cdot \#U$$

En particulier, pour tout $a \in G$: $\text{ord}(a) \mid \#G$ et $a^{\#G} = 1$.

Démonstration.

1. Nous appliquons la formule des indices avec $K = \{1\}$ et $H = U$.
2. Nous savons que G est fini donc $\left\{1, a, a^2, \ldots\right\}$ est fini et donc $n := \text{ord}(a) < +\infty$.
   Nous pouvons appliquer le point précédent au sous groupe $U = \langle a \rangle \subseteq G$ en utilisant que $\#U = n$.

2.2 Polynômes irréductibles

Définition 2.2.1 - Polynôme irréductible.
Soit K un corps. Considérons l'anneau principal $K[X]$.
On appelle *polynôme irréductible* tout élément irréductible de $K[X]$.

Remarque. Puisque $K[X]$ est principal, les irréductibles sont premiers.
Ainsi pour f est irréductible, l'idéal $(f) \subset K[X]$ est premier et maximal et donc :

$$E = {}^{K[X]}\!/_{(f)} \text{ est un corps.}$$

Alors E peut être vu comme une extension de corps de K en considérant le morphisme injectif :

$$\sigma : K \hookrightarrow K[X] \twoheadrightarrow E = {}^{K[X]}\!/_{(f)}$$

♢

Théorème 2.2.2 - Forme des extensions avec un zéro de f.
Soit K un corps, f un polynôme irréductible de $K[X]$ avec $d = \deg(f) \geqslant 1$ et $E = {}^{K[X]}\!/_{(f)}$.
Considérons l'élément $b := X + (f) \in E$. Alors :

1. La famille $\left\{1, b, b^2, \ldots, b^{d-1}\right\}$ est une K-base de E.
   En particulier, E/K est une extension finie de degré d.
2. L'élément $b \in E$ est un zéro de f.

Démonstration.

1. Montrons que la famille $B = \left\{1, b, b^2, \ldots, b^{d-1}\right\}$ est une K-base de E.
   B est libre : Supposons que $\sum_{i=0}^{d-1} \lambda_i b^i = 0$ dans E pour $\lambda_i \in K$.

Alors $\sum_{i=0}^{d-1} \lambda_i X^i + qf = 0$ dans $K[X]$ pour un certain $q \in K[X]$.
Mais $\deg(qf) = \deg(q) + \deg(f) \geqslant d$ donc il clair que $q = 0$ et :

$$\sum_{i=1}^{d-1} \lambda_i X^i = 0$$

D'où $\lambda_i = 0$ pour tout i puisque X^i est une base de $K[X]$.

B est génératrice : Soit $\overline{h} \in E$. Par division euclidienne dans $K[X]$, nous avons :

$$h = qf + r \text{ avec } q, r \in K[X] \text{ et } \deg(r) < d$$

Ainsi $r = \lambda_0 + \lambda_1 X + \cdots + \lambda_{d-1} X^{d-1}$ avec $\lambda_i \in K$ et donc $\overline{h} = \overline{r} = \lambda_0 + \lambda_1 b + \cdots + \lambda_{d-1} b^{d-1}$.

2. Notons $f = a_0 + a_1 X + \cdots + a_{d-1} X^{d-1} + a_d X^d$. Alors :

$$\begin{aligned} f(b) &= a_d\big(X + (f)\big)^d + a_{d-1}\big(X + (f)\big)^{d-1} + \cdots + a_1\big(X + (f)\big) + a_0 \\ &= a_d X^d + (f) + a_{d-1} X^{d-1} + (f) + \cdots + a_1 X + (f) + a_0 \\ &= f(X) + (f) = 0 \quad \text{dans } E. \end{aligned}$$

Le corollaire suivant donne une réponse complète à notre première question clé.

- Y a-t-il a toujours une extension E/K tel que f a un zéro dans E ?

Corollaire 2.2.3 - Extension finie et zéros.
Soit $f_1, \ldots, f_n \in K[X]$ des polynômes de degré $\geqslant 1$.
Alors il existe une extension finie E/K tel que chaque polynôme a un zéro dans E.

Démonstration. Par récurrence, nous pouvons supposer que $n = 1$.
Écrivons $f_1 = h_1 \ldots h_s$ un produit de polynômes irréductibles de $K[X]$.
En appliquant le théorème précédent à l'un des h_i, nous obtenons une extension finie E/K avec :

$$f(b) = h_1(b) \ldots h_n(b) = 0$$

Retournons à la deuxième question clé. Soit $f \in K[X]$ un polynôme non nul.

- Quel est le nombre maximal de zéros de f dans une extension E/K fixée ?

Théorème 2.2.4 - Majoration du nombre de zéros.
Soit K un corps et $f \in K[X]$ non nul.
Alors $a \in K$ est un zéro de f si et seulement si $(X - a) \mid f$ dans $K[X]$. En particulier :

$$\#\{\text{zéros de } f \text{ dans } K\} \leqslant \deg(f)$$

Démonstration. Procédons la division euclidienne de f par $(X - a)$:

$$f = (X - a)q + r \text{ avec } q, r \in K[X] \text{ et } \deg(r) < 1$$

1. Nous avons $f(a) = 0 \Leftrightarrow r = 0 \Leftrightarrow (X - a) \mid f$.
2. Procédons par récurrence sur $\deg(f)$. Si $\deg(f) = 1$ alors $f = (X - a)$ a une racine qui est a.
   Soit $\deg(f) > 1$. Soit $a \neq b$ deux zéros de f dans K.
   Alors $0 = f(b) = q(b) f(b - a)$ donc $q(b) = 0$ et $\deg(q) < \deg(f)$. Par hypothèse de récurrence :

$$\#\{\text{zéros de } q \text{ dans } K\} \leqslant \deg(q) = \deg(f) - 1$$

   Chaque zéro distincts de a est un zéro de de q :

$$\{\text{zéros de } f \text{ dans } K\} = \{\text{zéros de } q \text{ dans } K\} \cup \{a\}$$

   Ainsi f a moins de $\deg(f)$ zéros.

Corollaire 2.2.5 - Factorisation de f.
Soit $f \in K[X]$ non nul et soient $a_1, \ldots, a_r \in K$ des zéros disctincts de f.
Alors $(X - a_1) \cdots (X - a_r) \mid f$ dans $K[X]$.

Démonstration. D'après la proposition précédente, pour tout i : $(X - a_i) \mid f$.
Mais $(X - a_i)$ est un élément irréductible de $K[X]$ et $(X - a_i) \nsim \big(X - a_j\big)$.
Comme $K[X]$ est factoriel, $(X - a_1) \cdots (X - a_r) \mid f$.

Corollaire 2.2.6 - Caractérisation du polynôme nul.
Soit $f \in K[X]$. Si $f(a) = 0$ pour une infinité d'éléments $a \in K$ alors $f = 0$ dans $K[X]$.

Démonstration. Pour un polynôme non nul, on a vu que le nombre de ses zéros est inférieur à son degré.

Remarque. Attention, une infinité d'éléments est important.
Par exemple, si $p \in \mathbb{Z}$ est un nombre premier, alors $f = X^p - X \in \Big(\mathbb{Z}/p\mathbb{Z}\Big)[X]$ est non nul mais $f(a) = 0$ pour tout $a \in \mathbb{Z}/p\mathbb{Z}$. ♢

Définition 2.2.7 - Groupe cyclique.
Soit G un groupe.
On dit que G est *cyclique* si $G = \langle a \rangle$ pour un $a \in G$.

Théorème 2.2.8 - Sous-groupe de $K^\times$.
Soit K un corps. Tout sous-groupe fini de $K^\times$ est cyclique.

Pour la preuve, nous avons besoin du lemme suivant :

Lemme 2.2.9
Soit H un groupe abélien fini et p un nombre premier tel qu'il n'y a pas d'élément d'ordre p dans H.
Alors $p \nmid \#H$.

Remarque. Ce résultat est plus connu sous la forme :
Pour tout p premier tel que $p \mid \#H$, il existe un élément d'ordre p dans H. ♢

Définition 2.2.10 - Exposant d'un groupe.
Soit G un groupe.
On dit que $n \in \mathbb{N}$ est un *exposant* pour G si $\forall g \in G : g^n = 1$.

Démonstration du lemme. Soit $h \in H$ avec $\operatorname{ord}(h) = pr$.
Alors $\operatorname{ord}(h^r) = p$. Ainsi par hypothèse, $\operatorname{ord}(h)$ n'est pas un multiple de p pour tout $h \in H$ donc $n = \operatorname{ppcm}_{h \in H}\big(\operatorname{ord}(h)\big)$ n'est pas un multiple de p. Par contre, c'est un exposant de H.
Donc il suffit de démontrer que si m est un exposant de H alors $\#H \mid m^k$ pour un $k \geqslant 1$.

Montrons-le par récurrence sur $\#H$.
Si $\#H = 1$, c'est clair. Soit $\#H > 1$ et $h_0 \in H$ différent de 1. Posons $H_0 = \langle h_0 \rangle \subset H$.
Procédons à la division euclidienne de m par $\operatorname{ord}(h_0)$:

$$m = q \operatorname{ord}(h_0) + r \text{ avec } 0 \leqslant r < \operatorname{ord}(h_0)$$

Puisque $1 = h_0^m = \Big(h_0^{\operatorname{ord} h_0}\Big)^q h_0^r = h_0^r$, nous devons avoir $r = 0$ et donc $\#H_0 \mid m$.
Mais m est également un exposant pour le groupe H/H_0. Puisque $\#H/H_0 < \#H$, nous avons par hypothèse de récurrence $\#H/H_0 \mid m^k$ pour un certain $k \geqslant 1$.
Nous en concluons que :

$$\#H = \#H/H_0 \cdot \#H_0 \mid m^{k+1}$$

Cela conclut la démonstration du lemme par le raisonnement précédent.

Démonstration du théorème. Considérons un nombre premier p tel que $p \mid \#U$.

Définissons $U(p) := \Big\{ a \in U \mid \operatorname{ord}(a) = p^k, k \in \mathbb{N} \Big\} \subset U$ et $p^r := \max \Big\{ \operatorname{ord}(a) \mid a \in U(p) \Big\}$.

En particulier, $a^{p^r} = 1$ d'où tous les $a \in U(a)$ sont des zéros dans K du polynôme $X^{p^r} - 1$.

Le théorème 2.2.8 implique que $\#U(p) \leqslant p^r$.

Soit $b_p \in U(p)$ tel que $U\big(b_p\big) = p^r$.

Alors $\#\langle b_p \rangle = p^r$ donc $\langle b_p \rangle = U(p)$ et $U(p)$ est un sous-groupe cyclique de U engendré par b_p.

Le théorème de Lagrange 2.1.6 implique $p^r = \#U(p) \mid \#U$.

Par définition de $U(p)$, le groupe ${}^{U}\!/_{U(p)}$ n'a aucun élément d'ordre p.

D'après le lemme auxiliaire :

$$p \nmid \#{}^{U}\!/_{U(p)} = \big[U : U(p)\big]$$

Ainsi $\#U(p)$ est la puissance maximale de p qui apparait dans la décomposition de $\#U$.

Considérons maintenant tous les facteurs premiers $p_1, \ldots, p_s$ de $\#U$. Nous avons :

$$\#U = \#U(p_1) \cdots \#U(p_s) = \operatorname{ord}\big(b_{p_1}\big) \ldots \operatorname{ord}\big(b_{p_s}\big)$$

Soit $b := b_{p_1} \ldots b_{p_s} \in U$. Pour deux éléments a, b dans un groupe abélien fini avec $\operatorname{pgcd}\big(\operatorname{ord}(a), \operatorname{ord}(b)\big) = 1$, on a $\operatorname{ord}(ab) = \operatorname{ord}(a) \operatorname{ord}(b)$ (exercice). Alors $\operatorname{ord}(b) = \operatorname{ord}\big(b_{p_1}\big) \ldots \operatorname{ord}\big(b_{p_s}\big) = \#U$.

En particulier, l'inclusion $\langle b \rangle \subseteq U$ est une égalité. Ainsi $U = \langle b \rangle$ est cyclique.

Corollaire 2.2.11 - Groupe des inversibles d'un corps fini.

Soit K un corps fini.

Alors le groupe $K^\times$ est cyclique d'ordre $\#K - 1$.

Exemple. Par exemple, $\Big({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\Big)^\times$ est cyclique pour p premier. △

2.3 Critères d'irréductibilité

- Comment peut-on vérifier si un polynôme dans $K[X]$ est irréductible ?

En général, la question est difficile.

Nous allons donc donner deux critères d'irréductibilité dans le cas de $\mathbb{Q}[X]$.

Exemple de polynôme irréductible.

1. Un polynôme linéaire $X - a \in K[X]$ est irréductible.
2. Dans $\mathbb{C}[X]$, tout polynôme irréductible est linéaire.

   C'est une conséquence du théorème fondamental d'algèbre (preuve admise) :

   « Tout polynôme a au moins un zéro dans $\mathbb{C}$. »

△

Proposition 2.3.1 - Réductibilité d'un polynôme entier.

Soit $f \in \mathbb{Z}[X]$ réductible dans $\mathbb{Q}$ avec $\deg(f) \geqslant 1$.

Alors f est réductible dans $\mathbb{Z}[X]$, c'est-à-dire $f = gh$ avec $g, h \in \mathbb{Z}[X]$ tels que $\deg(g), \deg(h) \geqslant 1$.

Démonstration. Par le théorème de Gauss, les irréductibles de $\mathbb{Z}[X]$:

- Les irréductibles de $\mathbb{Z}$.
- Les polynômes primitifs qui sont irréductibles comme éléments de $\mathbb{Q}[X]$.

Puisque $\deg(f) \geqslant 1$, f n'est pas un premier de $\mathbb{Z}$.

La réductibilité dans $\mathbb{Q}[X]$ implique que f n'est pas non plus dans le second cas.

Proposition 2.3.2 - Critère de réduction modulo p.
Soit $f \in \mathbb{Z}[X]$ de coefficient dominant a_n et $p \in \mathbb{Z}$ premier.
Si $p \nmid a_n$ et $\overline{f} \in {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}[X]$ est irréductible, alors f est irréductible dans $\mathbb{Q}[X]$.

Démonstration. Procédons par l'absurde.
Supposons sous ses hypothèse que f soit réductible dans $\mathbb{Q}[X]$. Soit φ le morphisme de réduction :

$$\begin{array}{rccc} \varphi : & \mathbb{Z}[X] & \longrightarrow & {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}[X] \\ & h = \displaystyle\sum_{i\in I} b_i X^i & \longmapsto & \overline{h} = \displaystyle\sum_{i\in I} \overline{b_i} X^i \end{array}$$

Nous le construisons par propriété universelle à partir de $\mathbb{Z} \twoheadrightarrow {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \hookrightarrow {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}[X]$.

Nous avons supposé $f = gh$ avec $\deg(g), \deg(h) \geqslant 1$.
Nous pouvons supposer que $g, h \in \mathbb{Z}[X]$ et donc $\overline{f} = \overline{g}\overline{h}$ dans ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}[X]$. Mais :

$$\deg(f) = \deg\left(\overline{f}\right) = \deg\left(\overline{g}\right) + \deg\left(\overline{h}\right) \leqslant \deg(g) + \deg(h) = \deg(f)$$

En particulier $\deg\left(\overline{g}\right) = \deg(g) \geqslant 1$ et $\deg\left(\overline{h}\right) = \deg(h) \geqslant 1$.
Ainsi $\overline{f} = \overline{g}\overline{h}$ est une décomposition non triviale de f ce qui est impossible.

Proposition 2.3.3 - Critère d'Eisenstein.
Soit $f = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$ et $p \in \mathbb{Z}$ premier.
Si $\forall i < n : p \mid a_i$ et $p \nmid a_n$, $p^2 \nmid a_0$ alors f est irréductible dans $\mathbb{Q}[X]$.

Démonstration. Procédons par l'absurde.
Soit $f = gh$ avec $\deg(g), \deg(h) \geqslant 1$. Nous pouvons supposer $g, h \in \mathbb{Z}[X]$. Écrivons :

$$g = \sum_{i=0}^{r} b_i X^i \quad \text{et} \quad h = \sum_{i=0}^{s} c_i X^i$$

Alors :

- Nous avons $a_0 = b_0 c_0$ avec $p \mid a_0$ et $p^2 \nmid a_0$. Si nous supposons que $p \mid b_0$ alors $p \nmid c_0$.
- Puisque $n = r + s$, $p \nmid a_n = b_r c_s$ donc $p \nmid b_r$.

Soit b_v pour $0 < v \leqslant r < n$ le premier coefficient de g tel que $p \nmid b_v$:

$$a_v = b_v c_0 + b_{v-1} c_1 + \cdots + b_0 c_v$$

Nous savons que $v < n$ donc $p \mid a_v$ et $p \mid b_0, \ldots, b_{v-1}$ d'après le choix de v. Ainsi $p \mid b_v c_0$ et donc puisque $p \nmid c_0$ nous avons $p \mid b_v$ ce qui est impossible. Cela conclut que f est irréductible dans $\mathbb{Q}[X]$.

Application du critère d'Eisenstein.
Le critère d'Eisenstein permet de prouver simplement que $X^n - p \in \mathbb{Q}[X]$ est irréductible dans $\mathbb{Q}[X]$. En particulier $\left[\mathbb{Q}\left(\sqrt[n]{p}\right) : \mathbb{Q}\right] = n$ pour tout n. △

3. Propriétés des extensions

3.1 Polynôme minimal et clôture algébrique

Retournons à nos question clés.
Nous avons vu dans 2.2.2 que pour tout polynôme irréductible $f \in K[X]$ avec $\deg(f) \geqslant 1$, il existe une extension finie E/K telle que f a un zéro c dans E. Montrons maintenant que toute extension E/K dans laquelle f possède un zéro c est essentiellement de la forme décrit en 2.2.2 c'est-à-dire pour le corps intermédiare $K \subseteq K(c) \subseteq E$ on a :

$$K(c) \cong K[X]/(f)$$

Soit E/K une extension et $c \in E$ un élément algébrique sur K.
Nous obtenons un morphisme d'anneaux issu de la propriété universelle de $K[X]$ appliqué à $K \to K(c)$ et à l'élément $c \in K(c)$:

$$\begin{array}{rccc} \mathrm{ev}_c : & K[X] & \longrightarrow & K(c) \\ & f(X) & \longmapsto & f(c) \end{array}$$

Puisque $K(c)$ est un corps, $\mathrm{im}(\mathrm{ev}_c)$ est un anneau intègre donc $\mathrm{Ker}(\mathrm{ev}_c)$ est un idéal premier dans $K[X]$. Or c est algébrique sur K donc $\mathrm{Ker}(\mathrm{ev}_c) \neq \{0\}$ d'où $\mathrm{Ker}(\mathrm{ev}_c)$ est un idéal maximal de $K[X]$. Ainsi :

$$K[X]/\mathrm{Ker}(\mathrm{ev}_c) \hookrightarrow K(c) \subset E$$

En particulier, $\mathrm{Ker}(\mathrm{ev}_c) \subset K[X]$ est un sous-corps. Évidemment, $c = \mathrm{ev}_c(X) \in \mathrm{im}(\mathrm{ev}_c)$ et donc $\mathrm{im}(\mathrm{ev}_c) = K(c)$.
Nous avons montré que :

$$K[X]/\mathrm{Ker}(\mathrm{ev}_c) \cong K(c)$$

Nous obtenons la forme 2.2.2 en remarquant que $\mathrm{Ker}(\mathrm{ev}_c) = (f)$ pour un polynôme irréductible $f \in K[X]$.
Enfin :

$$\deg(f) = \Big[K[X]/(f) : K\Big] = \big[K(c) : K\big]$$

Définition 3.1.1 - Polynôme minimal.
Soit E/K une extension et $c \in E$ un élément algébrique sur K.
Le *polynôme minimal de c sur K* noté $Min(c;K;X)$ est l'unique polynôme unitaire de $K[X]$ tel que $\mathrm{Ker}(\mathrm{ev}_c) = \big(Min(c;K;X)\big)$. Par définition, $\deg\big(Min(c;K;X)\big) = \big[K(c) : K\big]$ et $Min(c;K;X) \in K[X]$ est irréductible.

Théorème 3.1.2 - Extension par des éléments algébriques.
Soit $c_1, \ldots, c_n$ des éléments algébriques sur K et $E = K(c_1, \ldots, c_n)$.
Alors E/K est une extension finie. En particulier E/K est une extension algébrique d'après 1.2.2.

Démonstration. Définissons $K_0 = K$ et $K_i = K_{i-1}(c_i) \subset E$.
Nous avons $K_n = E$ et la discussion précédente permet de dire que K_i/K_{i-1} est une extension finie, car c_i est algébrique sur K et donc aussi algébrique sur K_{i-1}. Nous en concluons par 1.4 que :

$$[E : K] = \prod_{i=1}^{n} [K_i : K_{i-1}] < +\infty$$

Théorème 3.1.3 - Tour d'extensions finies.
Soit E/K une extension finie, L et F deux corps intermédiaires.
Alors :

1. Si L/K est finie alors LF/F est finie.
2. Si L/K et F/K sont finies alors LF/K est finie.

Démonstration.

1. Si L/K est finie, alors d'après 1.1.5, $L = K(c_1, \dots, c_n)$.
   D'après 1.2.2, E/K est algébrique donc pour tout i, c_i algébrique sur K.
   D'après 1.1.6, $LF = K(c_1, \dots, c_n)F = F(c_1, \dots, c_n)$ et bien sûr, les c_i sont algébriques sur F.
   Ainsi LF/F est finie car $[LF : F] = n$.
2. Si L/K est finie alors LF/F est finie.
   Si de plus, F/K est finie alors LF/K finie car d'après la formule des degrés 1.1.7 :

$$[LF : K] = [LF : F] \cdot [F : K]$$

Théorème 3.1.4 - Transitivité du caractère algébrique.
Soit L un corps intermédiaire de E/K. Soit $c \in E$.
Alors :

1. Si c est algébrique sur K, alors c est algébrique sur L.
2. Si c algébrique sur L et L/K algébrique, alors c est algébrique sur K.

Démonstration.

1. Il est clair, car $K[X] \subseteq L[X]$. En fait, nous avons déjà utilisé cet argument précédemment.
2. Soit $Min(c; L; X) = a_0 + a_1X + \cdots + a_{d-1}X^{d-1} + X^d$ avec $a_i \in L$. Puisque L est algébrique sur K, les a_i sont algébriques sur K. Par 3.1.2, l'extension $L_0 = K\big(a_0, \dots, a_{d-1}\big)$ est une extension finie de K.
   De plus, $Min(c; L; X) \in L_0[X]$ et $Min(c; L; X)$ annule c, donc c est algébrique sur L_0.

   D'après 3.1.2, $L_0(c)/L_0$ est finie donc $L_0(c)/K$ est finie et donc algébrique.
   Ainsi, c est algébrique sur K.

Corollaire 3.1.5 - Fermeture algébrique dans une extension.
Soit E/K une extension.
Alors $\big(E/K\big)^{\text{alg}} = \Big\{c \in E \mid c \text{ est algébrique sur } K\Big\} \subseteq E$ est un corps intermédiaire de E/K.
Il est appelé *fermeture algébrique de K dans E*.
Il n'y a aucun élément algébrique sur $\big(E/K\big)^{\text{alg}}$ dans $E \setminus \big(E/K\big)^{\text{alg}}$.

Remarque. Cela permet de construire un corps intermédiaire qui contient tous les éléments algébriques.
Nous pouvons penser l'extension $E/\big(E/K\big)^{\text{alg}}$ comme hautement non algébrique. ♢

Démonstration. Soit x et $y \neq 0$ deux éléments algébriques de E/K.
Alors $K(x)/K$ est algébrique et donc $K(x, y)/K$ aussi.
Ainsi xy^{-1} et $x - y$ sont algébriques sur K et $\big(E/K\big)^{\text{alg}}$ est un corps.

Soit $c \in E$ algébrique sur $\big(E/K\big)^{\text{alg}}$.
L'élément c est algébrique sur K donc par 3.1.4, $c \in \big(E/K\big)^{\text{alg}}$.

Proposition 3.1.6 - Corps algébriquement clos.
Soit K un corps.
On dit que K est un corps *algébriquement clos* s'il satisfait les conditions équivalentes suivantes :

1. Si E/K est une extension algébrique, alors $E = K$.
2. Tout polynôme de $K[X]$ de degré $\geqslant 1$ possède un zéro dans K.
3. Tout polynôme de $K[X]$ de degré $\geqslant 1$ est un produit de polynômes linéaires.
   C'est-à-dire que les polynômes irréductibles sont exactement les polynômes linéaires.

Démonstration.
$3. \Rightarrow 2.$: Il est clair qu'un polynôme linéaire admet un zéro dans K.

$2. \Rightarrow 1.$: Soit E/K une extension algébrique sur K et $c \in E$.
Puisque $Min(c; K; X)$ est irréductible et possède un zéro dans K, d'après 2.2.4 nous avons $\deg\big(Min(c; K; X)\big) = 1$. Ainsi $\big[K(c) : K\big] = \deg\big(Min(c; K; X)\big) = 1$ donc $c \in K$ et $E = K$.

$1. \Rightarrow 3.$: Soit $f \in K[X]$ irréductible.
Alors ${}^{K[X]}\!/_{(f)}$ est une extension finie de degré $\deg(f)$ sur K d'après 2.2.2. Or $K = {}^{K[X]}\!/_{(f)}$ donc $\deg(f) = 1$.

Théorème 3.1.7 - Existence d'une clôture algébrique. ADMIS
Tout corps K possède une extension algébrique $\overline{K}/K$ qui est algébriquement close.
On dit que $\overline{K}$ est une clôture algébrique de K.

Remarque. Dans un certain sens, c'est l'extension de K la plus grande qui reste algébrique sur K.
De plus, cette clôture algébrique est essentiellement unique (voir au-dessous).
La preuve de ce théorème repose sur le lemme de Zorn et sur les anneaux de polynômes à une infinité de variable. ♢

Exemple.

1. Le corps $\mathbb{C}$ est algébriquement clos : C'est le théorème fondamental de l'algèbre.
2. Soit $\overline{\mathbb{Q}} := \big(\mathbb{C}/\mathbb{Q}\big)^{\text{alg}}$ la fermture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ au sens de 3.1.5.
   Alors :
   - Le corps $\overline{\mathbb{Q}}$ est algébriquement clos : Cela vient du fait que $\mathbb{C}$ est algébriquement clos.
     En effet, si $f \in \overline{\mathbb{Q}}[X]$, alors $f \in \mathbb{C}[X]$ donc admet un zéro $c \in \mathbb{C}$. Mais puisque c et algébrique sur $\overline{\mathbb{Q}}$, par 3.1.5, $c \in \overline{\mathbb{Q}}$. Ainsi, $\overline{\mathbb{Q}}$ est algébriquement clos car il satisfait le point 2. de 3.1.6.
   - L'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ est algébrique par construction.
   - Les deux premiers points impliquent que $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$.
   - L'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ n'est pas une extension finie. Par exemple, $\forall n\ X^n - p \in \mathbb{Q}[X]$ est irréductible.

   △

L'extension $\overline{K}/K$ est-elle uniquement déterminée par K ? Contient-elle « toutes » les extensions algébriques de K ?
Pour répondre à ces questions, il faut comparer les extensions de K via des morphismes.

Lemme 3.1.8
Soit E/K une extension algébrique et $\sigma : E \to E$ un morphisme préservant K.
Alors σ est bijectif, c'est-à-dire $\sigma \in \mathrm{Aut}\big(E/K\big)$.

Démonstration. Le morphisme σ est injectif. Montrons la surjectivité.
Soit $c \in E$ et $f = Min(c; K; X) \in K[X]$. Soit $L = K\left(\left\{b \in E \mid f(b) = 0\right\}\right) \subset E$.

D'après 3.1.2, l'extension L/K est finie. Ainsi par 1.2.5 et 1.2.6 :

$$\sigma(L) = \sigma(K)\left(\left\{\sigma(b) \mid b \in E, f(b) = 0\right\}\right) \subseteq K\left(\left\{b \in E \mid f(b) = 0\right\}\right) = L$$

Or $\dim_K(L) = \dim_K\big(\sigma(L)\big)$, donc $L = \sigma(L)$. Enfin, $c \in L$ donc $c \in \mathrm{im}(\sigma)$.

Définition 3.1.9 - Prolongement de σ.
Soit E/K une extension et $\sigma : K \to L$ un morphisme.
On appelle *prolongement de σ à E* tout morphisme $\tau : E \to L$ tel que $\tau_{|K} = \sigma$.

Théorème 3.1.10 - Nombre de prolongement.
Soit $E = K(c)$ une extension algébrique de K et $\sigma : K \to L$ un morphisme.
Le nombre de prolongements de σ à E est égal au nombre de zéros sans multiplicité de $\sigma\big(Min(c; K; X)\big)$ dans L.

Démonstration. Soit $f := Min(c; K; X)$ et soit ev_c l'isomorphisme :

$$\mathrm{ev}_c : {}^{K[X]}\!/_{(f)} \xrightarrow{\sim} K(c)$$

Nous avons $\mathrm{ev}_{c|K} = \mathrm{id}$ et $\mathrm{ev}_c\left(\overline{X}\right) = c$.
Nous en déduisons que le nombre de prolongement de σ à $E = K(c)$ est égal au nombre prolongements à ${}^{K[X]}\!/_{(f)}$ de σ. D'après la propriété universelle du quotient, c'est aussi égal au nombre de morphisme d'anneaux $\beta : K[X] \to L$ avec $\beta_{|K} = \sigma$ et $\beta\big(f(X)\big) = 0$ (c'est-à-dire $\sigma(f)\big(\beta(X)\big)$), donc par propriété universelle de $K[X]$, tout simplement le nombre de $b \in L$ tel que $\sigma(f)(b) = 0$.

Théorème 3.1.11 - Existence d'un prolongement.
Soit E/K une extension algébrique et $\sigma : K \to L$ un morphisme vers un corps L algébriquement clos.
Alors il existe un prolongement de σ à E.

Démonstration. Nous souhaitons appliquer le lemme de Zorn.
Soit S l'ensemble des couples (F, τ) où F est un corps intermédiaire de E/K et τ un prolongement de σ à F.
Nous définissons une relation d'ordre partielle $\leqslant$ sur S :

$$(F, \tau) \leqslant \left(F', \tau'\right) \Leftrightarrow F \subseteq F' \text{ et } {\tau'}_{|F} = \tau$$

Alors $S \neq \varnothing$ car $(K, \sigma) \in S$ et de plus S est inductivement ordonnée.
En effet, soit $\left\{(F_i, \tau_i)\right\}_{i \in I}$ une chaîne dans S.
Alors $F := \bigcup_{i \in I} F_i$ est un corps intermédiaire de E/K et $\tau : a \mapsto \tau_i(a)$ si $a \in F_i$ donne un prolongement de σ à F. Ainsi, l'élément (F, τ) est une borne supérieure dans S pour $\left\{(F_i, \tau_i)\right\}_{i \in I}$.
D'après le lemme de Zorn, il existe un élément maximal (F_0, τ_0) dans S.
Résonnons par contradiction et supposons que $F_0 \neq E$. Soit $c \in E \setminus F_0$. Alors c est algébrique sur K et donc algébrique sur F_0. De plus, par 3.1.2, $F_0(c)/F_0$ est algébrique. Puisque L algébriquement clos, $\tau_0\big(Min(c; F_0; X)\big) \in L[X]$ a un zéro dans L donc par 3.1.10 il existe un prolongement τ de τ_0 à F_0.
Nous en concluons une contradiction à la maximalité de (F_0, τ_0) :

$$(F_0, \tau_0) \lneq \big(F_0(c), \tau\big)$$

Ainsi nous obtenons $E = F_0$ et τ_0 est le prolongement cherché.

Corollaire 3.1.12 - Unicité de la clôture algébrique.
Soit $\overline{K}/K$ et $\tilde{K}/K$ deux extensions algébrique où $\overline{K}$ et $\tilde{K}$ sont algébriquement clos.
Alors il existe un isomorphisme $\tau : \overline{K} \xrightarrow{\sim} \tilde{K}$ avec $\tau_{|K} = \mathrm{id}$.

Démonstration.
Le théorème 3.1.11 appliqué à $E = \overline{K}$ et $L = \tilde{K}$ nous montre qu'il existe un prolongement τ à $\overline{K}$ du morphisme $K \hookrightarrow \tilde{K}$. De plus, $\tau(\overline{K})$ est algébriquement clos par 3.1.6.

En effet, si $f \in \tau(\overline{K})[X]$ alors $\tau^{-1}(f) \in \overline{K}[X]$ possède un zéro $b \in \overline{K}$ et donc $\tau(b)$ est un zéro de f dans $\tau(\overline{K})$.

Ainsi $\tilde{K}/\tau(\overline{K})$ est algébrique donc par le premier point de 3.1.6, $\tilde{K} = \tau(\overline{K})$ et τ est surjectif.

3.2 Extensions normales

Les extensions normales forment une classe particulière d'extension qui se comportent particulièrement bien. Associé au caractère séparable, cela donne un bon environnement pour développer la théorie de Galois.

Définition 3.2.1 - Corps de décomposition.
Soit $f \in K[X]$ un polynôme de degré $\deg(f) \geqslant 1$.
On appelle *corps de décomposition de f sur K* toute extension E/K telle que :

- $f(X) = c(X - a_1)\dots(X - a_n)$ dans $E[X]$.
- $E = K(a_1, \dots, a_n)$.

Remarque.

1. Il existe toujours un corps de décomposition. Il suffit de décomposer f sur la clôture algébrique de K et de considérer $E = K(a_1, \dots, a_n)$ où $a_1, \dots, a_n$ sont les zéros de f dans $\overline{K}$.
2. Tout corps de décomposition est une extension finie.

♢

Théorème 3.2.2 - Unicité du corps de décomposition.
Soit E/K et L/K deux corps de décomposition de $f \in K[X]$ avec $\deg(f) \geqslant 1$.
Alors il existe un isomorphisme $\sigma : E \xrightarrow{\sim} L$ avec $\sigma_{|K} = \mathrm{id}$.

C'est une conséquence de l'unicité de la clôture algébrique.

Démonstration. Soit $\overline{L}/L$ une clôture algébrique de L.

Puisque L/K est algébrique, $\overline{L}/K$ est algébrique d'après 3.1.4 et $\overline{L}$ est une clôture algébrique de K.

Puisque E/K est algébrique, d'après 3.1.11 il existe un prolongement de l'injection $K \hookrightarrow \overline{L}$ à E : un morphisme $\sigma : E \to \overline{L}$ tel que $\sigma_{|K} = \mathrm{id}$. Nous avons alors :

$$f = c(X - a_1)\dots(X - a_n) \text{ dans } E \text{ avec } c \in K \text{ et } a_i \in E = K(a_1, \dots, a_n)$$

Nous obtenons que $f = \sigma\big(f(X)\big) = c\big(X - \sigma(a_1)\big)\dots\big(X - \sigma(a_n)\big)$ dans $\overline{L}[X]$ et par ailleurs :

$$f = c(X - b_1)\dots(X - b_n) \text{ dans } L \text{ avec } b_i \in L = K(b_1, \dots, b_n)$$

Considérons ces décomposition dans $\overline{L}[X]$ qui est factoriel. Par unicité de la décomposition :

$$\big\{\sigma(a_1), \dots, \sigma(a_n)\big\} = \{b_1, \dots, b_n\} \text{ dans } \overline{L}$$

Nous obtenons :

$$\sigma(E) = K\big(\sigma(a_1), \dots, \sigma(a_n)\big) = K(b_1, \dots, b_n) = L$$

Ainsi $\sigma : E \xrightarrow{\sim} L$ avec $\sigma_{|K} = \mathrm{id}$ est le morphisme cherché.

Lemme 3.2.3 - Morphisme et clôture algébrique.
Soit $\overline{K}/K$ un clôture algébrique et $f \in K[X]$ avec $\deg(f) \geqslant 1$.
Alors il existe exactement un corps intermédiaire E de $\overline{K}/K$ qui est un corps de décomposition de f.
De plus, chaque morphisme $\sigma : E \to \overline{K}$ avec $\sigma_{|K} = \mathrm{id}$ est un automorphisme de E.

Démonstration.
Si $a_1, \dots, a_n \in \overline{K}$ sont les zéros de f, alors $E := K(a_1, \dots, a_n)$ est un corps de décomposition de f.
De plus, ce corps de décomposition est unique à isomorphisme près d'après 3.2.2. Cela donne le résultat.

Définition 3.2.4 - Extension normale.
Soit E/K une extension.
On dit que E/K est *normale* si elle est finie et que pour tout polynôme irréductible $f \in K[X]$:

Si f possède un zéro dans E, alors f est un produit de facteurs linéaires dans $E[X]$.

Exemple. Une extension finie de degré 2 est normale (division euclidienne). △

Théorème 3.2.5 - Caractérisation des extension normale.
Soit E/K une extension finie.
L'extension E/K est normale si et seulement si E est un corps de décomposition de $f \in K[X]$ avec $\deg(f) \geqslant 1$.

Démonstration. Soit E/K une extension normale.
Alors $E = K(a_1, \dots, a_n)$ par 1.1.5 car c'est une extension finie. Soit :

$$f = \prod_{i=1}^{n} Min(a_i; K; X) \in K[X]$$

Puisque E/K est normale, f est un produit de facteurs linéaires dans $E[X]$. Ainsi :

$$K(\text{zéros de } f) \subseteq E = K(a_1, \dots, a_n) \subseteq K(\text{zéros de } f)$$

Ainsi $E = K(\text{zéros de } f)$ et donc E est un corps de décomposition de f.

Réciproquement, soit $h \in K[X]$ irréductible avec un zéro $a \in E$. Soit $b \in \overline{E}$ un autre zéro de h.

- Par 3.1.10, il existe un prolongement τ de $K \hookrightarrow E \hookrightarrow \overline{E}$ à $K(a)$ avec $\tau(a) = b$.
- Par 3.1.11, il existe un prolongement σ de τ à E.

Puisque $\overline{E}/K$ est une clôture algébrique, $\sigma : E \to \overline{E}$ est un automorphisme de E par 3.2.3 et :

$$b \in \text{im}(\tau) \subset \text{im}(\sigma) = E$$

Ainsi h est un produit de facteurs linéaire dans $E[X]$ et E/K est normale.

Théorème 3.2.6 - Tour d'extensions normales.
Soit E/K une extension finie, L et F deux corps intermédiaires.
Alors nous avons :

- Si L/K est normale alors LF/F est normale.
- Si E/K est normale alors E/F est normale.
- Si F/K et L/K sont normales alors FL/K et $(L \cap F)/K$ sont normales.

Démonstration.

- Soit L/K normale. Alors L est un corps de décomposition de $f \in K[X]$ par 3.2.5.
  En particulier $L = K(a_1, \dots, a_n)$. Alors par 1.1.6, $LF = F(a_1, \dots, a_n)$ est un corps de décomposition de $f \in F[X]$. Ainsi par 3.2.5, LF/F est normale.
- Il suffit d'appliquer le premier point à $L = E$ car $EF = E$.
- Soit $f \in K[X]$ irréductible.
  1. Si f admet un zéro dans $L \cap F$, tous les zéro de f sont dans L et F car L/K et F/K sont normales. Ainsi les zéros de f sont dans $L \cap F$ et $(L \cap F)/K$ est une extension normale.

2. Si f admet un zéro $a \in LF$, soit $b \in \overline{LF}$ un autre zéro de f.

   Comme dans la preuve précédente en remplaçant E par LF, il existe un morphisme $\sigma : LF \to \overline{LF}$ avec $\sigma_{|K} = \mathrm{id}$ et $\sigma(a) = b$. Par 1.2.5 $\sigma(LF) = \sigma(L)\sigma(F)$.

   Par 3.2.3 appliqué aux extensions $L \subset \overline{LF}$ et $F \subset \overline{LF}$ normales sur K, nous avons $\sigma(L) = L$ et $\sigma(F) = F$. Ainsi nous en concluons que $\sigma(LF) = LF$. En particulier, $b \in \mathrm{im}(\sigma) = LF$.

   Ainsi f est un produit de facteurs linéaires dans $LF[X]$ c'est-à-dire LF/K est normale.

3.3 Extensions séparables

Dans cette section, E/K est toujours algébrique.

Définition 3.3.1 - Extension séparable.
Soit E/K une extension algébrique.

1. Un polynôme $f \in K[X]$ avec $\deg(f) \geqslant 1$ est dit *séparable* si il n'a pas de zéro de multiplicité $\geqslant 2$ dans $\overline{K}$.
2. Un élément $a \in E$ est dit *séparable sur* K si $Min(a; K; X)$ est séparable.
3. Une extension E/K est dite *séparable* si tous ses élément sont séparables sur K.

Remarque.
Par unicité (3.1.12), la notion de séparabilité d'un polynôme de dépend pas du choix de la clôture algébrique. ♢

Lemme 3.3.2 - Majoration du nombre de prolongement.
Soit E/K une extension finie et $\sigma : K \to L$ un morphisme avec L algébrique clos.
Alors le nombre de prolongement à E de σ est $\leqslant [E : K]$.

Démonstration. Soit $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = E$ avec $K_{i+1} = K_i(c_i)$ pour certains éléments $c_i \in E$.
Alors, par 3.1.10, $\big[K_{i+1} : K_i\big] = \deg\big(Min(c_i; K_i; X)\big)$ est supérieur au nombre de prolongements d'un morphisme donné $\tau : K_i \to L$ à K_{i+1}. Ainsi $[E : K] = \prod_i \big[K_{i+1} : K_i\big]$ est supérieur nombre de prolongements de σ à E.

Théorème 3.3.3 - Caractérisation d'une extension séparable.
Soit $E = K(a_1, \ldots, a_n)$.
L'extension E/K est séparable si et seulement si $a_1, \ldots, a_n$ sont séparables sur K.

Démonstration. Par définition, le sens direct est trivial.
Réciproquement, soit $K_i = K(a_1, \ldots, a_i)$. Alors $Min\big(a_{i+1}; K_i; X\big) \mid Min\big(a_{i+1}; K; X\big)$ dans $K_i[X]$.
Ainsi a_{i+1} est séparable sur K_i et le nombre des zéros sans multiplicité de $Min\big(a_{i+1}; K_i; X\big)$ est $\big[K_{i+1} : K_i\big]$.
Par 3.1.10, il y a exactement $\big[K_{i+1} : K_i\big]$ prolongements d'un morphisme $K_i \to \overline{K}$ donné à K_{i+1}.
Par récurrence sur i, il y a exactement $\prod_i \big[K_{i+1} : K_i\big] = [E : K]$ prolongements à E d'un morphisme donné. $(*)$.

Autrement dit, il existe exactement $[E : K]$ morphismes $\sigma : E \to \overline{K}$ tels que $\sigma_{|K} = \mathrm{id}$.

Soit $a \in E$. Montrons par l'absurde que a est séparable sur K.
Si a n'est pas séparable alors $\#\Big\{\tau : K(a) \to \overline{K} \mid \tau_{|K} = \mathrm{id}\Big\} < \big[K(a) : K\big]$ par 3.1.10.
Le lemme 3.3.2 précédent appliqué à $E/K(a)$ nous dit que :

$$\#\Big\{\sigma : E \to \overline{K} \mid \sigma_{|K(a)} = \tau\Big\} \leqslant \big[E : K(a)\big]$$

Nous obtenons alors notre contradiction avec $(*)$:

$$\#\Big\{\sigma : E \to \overline{K} \mid \sigma_{|K} = \mathrm{id}\Big\} \overset{3.1.10}{<} \big[E : K(a)\big] \cdot \big[K(a) : K\big] = [E : K]$$

Ainsi a séparable sur K et l'extension E/K est séparable.

Corollaire 3.3.4 - Nombre de prolongement pour un extension séparable.
Soit E/K une extension finie.
Alors E/K est séparable si et seulement si tout morphisme de K dans un corps algébriquement clos L a exactement $[E : K]$ prolongements à E.

Démonstration.
$1 \Rightarrow 2$: Supposons que E/K est séparable. En particulier, $E = K(a_1, \dots, a_n)$ avec a_i séparable sur K.
Comme dans la preuve précédente, on arrive à l'énoncé $(*)$ qui est en fait 2.
$2 \Rightarrow 1$: Supposons l'énoncé $(*)$ vrai. Supposons qu'il existe $a \in E$ qui n'est pas séparable sur K.
Comme dans la preuve précédente, nous obtenons une contradiction avec $(*)$.

Théorème 3.3.5 - Tour d'extensions séparables.
Soit E/K une extension algébrique, F et L deux corps intermédiaires.
Alors :

- E/K est séparable si et seulement si E/F et F/K sont séparables.
- L/K est séparable si et seulement si LF/F est séparable.
- Si L/K et F/K sont séparable alors LF/K est séparable.

Démonstration.
Premier point :
$\Rightarrow$: Nous avons $F \subseteq E$ donc F/K est séparable. De plus, si $a \in E$ alors $Min(a; F; X) \mid Min(a; K; X)$.
Ainsi a est séparable sur K et donc sur F. Nous en concluons que E/F est séparable.

$\Leftarrow$:

- Si E/F est finie, alors nous appliquons la proposition précédente ?? et la formule des degrés 1.1.7 aux extensions $K \subseteq F \subseteq E$.
- Si E/K est algébrique et non fini, soit $a \in E$ et $f = Min(a; F; X) = a_0 + a_1X \cdots + a_{n-1}X^{n-1} + X^n$.
  Par hypothèse, f est séparable. Soit $F_0 = K\big(a_1, \dots, a_{n-1}\big) \subseteq F$ et considérons $K \subseteq F_0 \subseteq F_0(a)$.
  Puisque $F_0 \subset F$ et F/K est séparable, F_0/K est séparable. Enfin, $f \in F_0[X]$ est séparable, donc puisque f est irréductible, a est séparable sur F_0 et par 3.3.3, $F_0(a)/F_0$ est séparable.
  Le cas fini assure que $F_0(a)/K$ est séparable donc $a \in F_0(a)$ est séparable sur K.
  Puisque a est quelconque, E/K est séparable.

Deuxième point : Soit $a \in LF$.
Écrivons $L = \bigcup_{i \in I} L_i$ avec L_i/K un extension finie. Alors $LF = \bigcup_{i \in I} L_iF$.
Ainsi $a \in F(a_1, \dots, a_n)$ pour certain élément $a_1, \dots, a_n \in L$. De plus, nous savons que a_i est séparable sur K car L/K est séparable sur K. Ainsi par le premier point, a_i est séparable sur F donc par 3.3.3, $F(a_1, \dots, a_n)/F$ est séparable. Si $a \in F(a_1, \dots, a_n) \Rightarrow a$ est séparable sur F. Ainsi LF/F est séparable.

Troisième point : Le troisième point est une conséquence des deux premiers.

Corollaire 3.3.6 - Extension des éléments séparables.
Soit E/K une extension algébrique.
Il existe un corps intermédiaire E^{sep} qui contient tous les éléments séparables de E :

$$E^{\text{sep}} = \Big\{ a \in E \mid a \text{ séparable sur } K \Big\}$$

Il n'y a aucun élément séparable sur E^{sep} dans $E \setminus E^{\text{sep}}$.

Démonstration. Soit a et b deux éléments de E^{sep} non nuls.
Alors d'après 3.3.3, $K(a, b)/K$ est séparable. Par définition $K(a, b) \subset E^{\text{sep}}$ donc E^{sep} est un corps.

Soit $a \in E \setminus E^{\text{sep}}$ un élément séparable. Alors $E^{\text{sep}}(a)/E^{\text{sep}}$ est séparable par 3.3.3.
Puisque a est séparable sur E^{sep}, $E^{\text{sep}}(a)/K$ est séparable par 3.3.5 donc a est séparable sur K.
Par définition, $a \in E^{\text{sep}}$ ce qui contredit l'hypothèse.

Définition 3.3.7 - Corps parfait.
Un corps K est dit *parfait* si toute extension E/K est séparable.

Lemme 3.3.8 - Sous-corps premier.
Tout corps contient exactement un sous-corps K_0 qui est isomorphe à $\mathbb{Q}$ ou à $\mathbb{Z}/p\mathbb{Z}$ avec p premier.
Ce sous-corps K_0 est appelé *sous-corps premier* de K

Démonstration.
Existence : Considérons le morphisme d'anneaux :

$$\begin{array}{rccc} \varepsilon_K : & \mathbb{Z} & \longrightarrow & K \\ & x & \longmapsto & 1_K \cdot x \end{array}$$

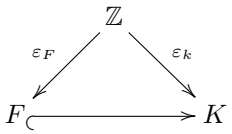
Puisque K est intègre, $\mathrm{Ker}(\varepsilon_K) \subset \mathbb{Z}$ est un idéal premier.

- Premier cas : $\mathrm{Ker}(\varepsilon_K) = p\mathbb{Z}$ donc $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathrm{im}(\varepsilon_K) = K_0 0 \subset K$.
- Second cas : $\mathrm{Ker}(\varepsilon_K) = \{0\}$. Définissons :

$$\begin{array}{rccc} \varepsilon'_K : & \mathbb{Q} & \longrightarrow & K \\ & nm^{-1} & \longmapsto & \varepsilon_K(n)\varepsilon_K(m)^{-1} \end{array}$$

Puisque $\mathbb{Q}$ et K sont des corps, ε'_K est injectif ce qui conclut en posant $K_0 = \mathrm{im}(\varepsilon'_K)$.

Unicité :
Soit $F \subseteq K$ un deuxième corps comme dans l'énoncé.
Considérons le diagramme suivant qui est commutatif suivant car $1_K = 1_F$:



Ainsi, F contient le corps K_0 construit au dessus.

- Premier cas : $K_0 \cong \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \not\subset \mathbb{Q}$.
  Alors $F \cong \mathbb{Z}/p\mathbb{Z}$ et de plus, $|K_0| = |F|$ donc $K_0 = F$.
- Deuxième cas : $\mathbb{Q} \cong K_0 \subseteq F \cong \mathbb{Q}$.
  Si $a \in F$ non nul, alors pour $m \in \mathbb{Z}$ non nul : $ma \in \mathbb{Z} \subset K_0$ donc $a \in \dfrac{1}{m}K_0 = K_0$.

Définition 3.3.9 - Sous-corps premier et caractéristique.
Soit K un corps de sous-corps premier K_0.
La *caractéristique du corps* K est la caractéristique de K comme anneau, donc la quantité définie par :

$$\mathrm{Car}(K) = \begin{cases} 0 & \text{si } K_0 \equiv \mathbb{Q} \\ p & \text{si } K_0 \cong \mathbb{Z}/p\mathbb{Z} \end{cases}$$

En particulier, $\forall a \in K : \mathrm{Car}(K)a = 0$.

Théorème 3.3.10 - Corps parfait classique.
Soit K un corps.

- Si $\mathrm{Car}(K) = 0$ alors K est un corps parfait.
- Si $\mathrm{Car}(K) = p > 0$ alors K est parfait si et seulement si $K = K^p = \{a^p \mid a \in K\}$.

Démonstration. Soit $f \in K[X]$ irréductible.

Supposons par l'absurde que f a un zéro $a \in \overline{K}$ de multiplicité $\geqslant 2$. Dans $\overline{K}[X]$, $f = (X-a)^n g$ avec $n \geqslant 2$.

Ainsi $f' = (X-a)^{n-1}\big(ng + (X-a)g'\big)$ et $X - a \mid \operatorname{pgcd}\big(f, f'\big)$ dans $\overline{K}[X]$ donc $\operatorname{pgcd}\big(f, f'\big) \neq 1$ dans $\overline{K}[X]$ et dans $K[X]$ car si $\operatorname{pgcd}\big(f, f'\big) = 1$ alors $\big(f, f'\big)_{K[X]} = K[X]$ d'où $\big(f, f'\big)_{\overline{K}[X]} = \overline{K}[X]$. Mais f est irréductible dans $K[X]$ donc $\operatorname{pgcd}\big(f, f'\big) = f$. En particulier, $f \mid f'$. Mais $\deg\big(f'\big) < \deg(f)$ et donc $f' = 0$.

Étape caractérisitique 0 :

Si $f' = 0$ alors f est un polynôme constant ce qui est une contradiction car f est irréductible. Ainsi, si $\operatorname{Car}(K) = 0$ alors f est forcément séparable et donc K est parfait.

Étape caractérisitique p :

$\Leftarrow$: Supposons $K = K^p$. Si $f' = 0$ alors :

$$f = a_0 + a_1 X^p + a_2 X^{2p} + \cdots + a_m X^{mp}$$

En effet, tous les exposants qui apparaissent dans f sont divisible par p. Puisque $K = K^p$ donc nous pouvons écrire $a_i = b_i^p$ pour tout i avec $b_i \in K$. Alors f admet une décomposition non triviale dans $K[X]$:

$$f = \sum_i b_i^p X^{ip} = \left(\sum_i b_i X^i\right)^p$$

C'est une contradiction avec l'irréductibilité. Ainsi pour $\operatorname{Car}(K) = p$ et $K = K^p$, K est parfait.

$\Rightarrow$ Si $K \neq K^p$, soit $f \in K[X]$ quelconque. Soit $a \in K \setminus K^p$. Soit $b \in \overline{K}$ avec $b^p = a$.

Affirmation :

Le polynôme $f = X^p - a \in K[X]$ n'est pas séparable mais irréductible.

En effet, $f = (X-b)^p$ dans $\overline{K}[X]$ donc f n'est pas séparable. En plus, les facteurs irréductibles de f dans $K[X]$ doivent être de la forme $(X-b)^i$ avec $0 < i \leqslant p$ et ont b comme zéro. Il existe un unique polynôme qui vérifie ces conditions : $Min(b; K; X)$. Ainsi, il existe un unique i tel que $(X-b)^i$ est irréductible. En particulier, $f = (X-b)^{ij}$ avec $ij = p$. Mais b n'est pas dans K car $a = b^p \in K \setminus K^p$ donc $i \neq 1$. Ainsi $i = p$ et $j = 1$ et car p est premier et donc f est irréductible.

En particulier, $K(b)/K$ n'est pas séparable donc K n'est pas parfait.

Théorème 3.3.1 - Théorème de l'élément primitif.

Soit E/K une extension finie et séparable.

Alors, il existe $a \in E$ tel que $E = K(a)$. Un tel élément et appelé *un élément primitif pour* E/K.

Démonstration.

Si K est un corps fini, puisque $\dim_K(E) < +\infty$, E est aussi un corps fini et par 2.2.11, $E^\times = \langle a \rangle$ pour $a \in E$ et nous avons $E = K(a)$.

Si K est un corps infini alors nous pouvons écrire $E = K(a_1, \ldots, a_n)$.

Par récurrence finie sur les a_i, il suffit de prouver le cas $n = 2$. Cela nous permettra de réduire le nombre de générateurs successivement jusqu'à qu'il n'en reste qu'un.

Supposons que $E = K(b, c)$.

Soit $b_1, \ldots, b_r$ et $c_1, \ldots, c_s$ les zéros de $Min(b; K; X)$ et $Min(c; K; X)$ dans $\overline{K} \supseteq E \supseteq K$ tel que $b = b_1$ et $c = c_1$.

$(*)$ Puisque $|K| = +\infty$, nous pouvons trouver $u \in K$ tel que $u \neq \dfrac{b - 1 - b_i}{c_j - c_1}$ pour $1 \leqslant i \leqslant r$ et $2 \leqslant j \leqslant s$.

$(**)$ Soit $a = b_1 + uc_1 = b + uc \in E$.

Affirmation : $c \in K(a)$. Notons que cela implique $b = a - uc \in K(a)$ et donc $E = K(a)$.

Soit $f = Min(b; K; X)$ et $g = Min(c; K; X)$ ainsi que $f_1(X) = f(a - uX) \in K(a)[X]$. Nous avons $f_1(c) = f(b) = 0$ et $g(c) = 0$ donc $\operatorname{pgcd}(f_1, g) \neq 1$ dans $\overline{K}[X]$ car $X - c$ divise f_1 et g. Mais $c = c_1$ est le seul

zéro dans $\overline{K}$ commun à f_1 et g.

En effet, nous avons par construction de f_1 :

$$\{\text{zéros de } f_1\} = \{c \in \overline{K} : a - uc = b_i\}$$

Et de plus, $a - ucj = b_1 + uc_1 - uc_j = b_1 + u\big(c_1 - c_j\big) = b_1 - u\big(c_j - c_1\big) \neq b_i$ par $(*)$ et $(**)$.

Puisque f est séparable, $X - c = \text{pgcd}(f_1, g)$ dans $K(a)[X]$. En particulier, $c \in K(a)$.

4. Théorie de Galois : Théorème principal

4.1 Définitions générales

Définition 4.1.1 - Extension galoisienne.
Une extension finie est dite *galoisienne* si elle est normale et séparable.

Dans ce cadre, nous avons pouvons classifier les extensions intermédiares : c'est le sujet du théorème principal.

Définition 4.1.2 - Groupe de Galois.
Soit E/K une extension Galoisienne.
On appelle *groupe de Galois* de E/K le groupe $\mathrm{Gal}\big(E/K\big) = \mathrm{Aut}\big(E/K\big)$.

Proposition 4.1.3 - Cardinal du groupe de Galois.
Soit E/K une extension galoisienne. Alors $|\mathrm{Gal}\big(E/K\big)| = [E : K]$.

Démonstration. Soit $\overline{K}$ une clôture algébrique de K dont E un corps intermédiaire.
L'extension E/K est normale donc par 3.2.5, E est un corps de décomposition d'un polynôme dans $K[X]$.
Ainsi, par 3.2.3, $\mathrm{Aut}\big(E/K\big) = \Big\{\sigma : E \to \overline{K} \mid \sigma_{|K} = \mathrm{id}\Big\}$.
Puisque E/K est séparable, 3.3.4 implique que $[E : K] = \#\Big\{\sigma : E \to \overline{K} \mid \sigma_{|K} = \mathrm{id}\Big\}$.

Définition 4.1.4 - Corps fixe.
Soit G un ensemble d'automorphisme d'un corps K.
On appelle *corps fixe de* G le sous-corps de K suivant :

$$K^G = \Big\{a \in K \mid \forall \sigma \in G : \sigma(a) = a\Big\}$$

Remarque. L'ensemble $K^G = \bigcap_{\sigma \in G} \Big\{a \in K \mid \sigma(a) = a\Big\}$ est un corps comme intersection de corps. ♢

4.2 Énoncé et début de la preuve du théorème principal

Théorème 4.2.1 - Théorème principal.
Soit E/K une extension galoisienne et F un corps intermédiaire.
Alors :

- E/F est galoisienne et donc $\mathrm{Gal}\big(E/F\big) \subset \mathrm{Gal}\big(E/K\big)$.
- Nous avons une correspondance bijective entre les ensembles suivants :

$$\begin{array}{ccc} \Big\{ \text{ Sous-groupes de } \mathrm{Gal}\big(E/K\big) \Big\} & \longleftrightarrow & \{ \text{ Corps intermédiaires de } E/K \} \\ H = \mathrm{Gal}\Big(E/E^H\Big) = \mathrm{Gal}\big(E/F\big) & \longleftrightarrow & E^H = E^{\mathrm{Gal}\left(E/F\right)} = F \end{array}$$

- L'extension F/K est galoisienne si et seulement si $\mathrm{Gal}\big(E/F\big)$ est un sous-groupe normal de $\mathrm{Gal}\big(E/K\big)$.

$$\mathrm{Gal}\big(E/F\big) \triangleleft \mathrm{Gal}\big(E/K\big)$$

Dans ce cas, la restriction $\sigma \mapsto \sigma_{|F}$ induit un isomorphisme :

$$\mathrm{Gal}\big(E/K\big)\Big/_{\mathrm{Gal}\big(E/F\big)} \cong \mathrm{Gal}\big(F/K\big)$$

Démonstration. Procédons en plusieurs étapes.

Première étape : E/F est galoisienne.

En effet, E/K est normale et séparable donc d'après 3.2.6 et 3.3.5, E/F est normale et séparable.

Deuxième étape : $E^{\mathrm{Gal}(E/K)} = K$.

Nous avons déjà $K \subset E^{\mathrm{Gal}(E/K)}$ car $\sigma_{|K} = \mathrm{id}$ pour tout $\sigma \in \mathrm{Gal}\big(E/K\big)$.

Montrons que $K \supset E^{\mathrm{Gal}(E/K)}$. Soit $a \in E^G$ et $r = \big[K(a) : K\big]$. Comme E/K est séparable, a est séparable sur K donc par 3.3.4, il existe exactement r prolongements distincts $\beta_1, \dots, \beta_r : K(a) \to \overline{K}$ avec $\beta_{|K} = \mathrm{id}$.

D'après 3.1.11, β_i se prolonge en un morphisme $\sigma_i : E \to \overline{K}$.

Puisque E/K est normale, $\sigma_i(E) = E$ et donc $\sigma_i \in G$. Nous concluons avec :

$$\begin{aligned} a \in E^{\mathrm{Gal}(E/K)} &\Rightarrow \sigma_1(a) = \sigma_2(a) = \cdots = \sigma_r(a) = a \\ &\Rightarrow \beta_1(a) = \beta_2(a) = \cdots = \beta_r(a) = a \\ &\Rightarrow \beta_1 = \cdots = \beta_r \Rightarrow r = 1 \\ &\Rightarrow \beta_1 = \mathrm{id} \Rightarrow a \in K \end{aligned}$$

Troisième étape : L'application retour est injective :

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{Sous-groupes de } \mathrm{Gal}\big(E/K\big) \\ \mathrm{Gal}\big(E/F\big) \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{Corps intermédiaires de } E/K \\ F \end{array} \right\} \\ & \hookleftarrow & \end{array}$$

En effet, les deux premières étapes appliquées à E/F impliquent que $F = E^{\mathrm{Gal}(E/F)}$.

Si L est un autre corps tel que $\mathrm{Gal}\big(E/L\big) = \mathrm{Gal}\big(E/F\big)$ alors :

$$L = E^{\mathrm{Gal}(E/L)} = E^{\mathrm{Gal}(E/F)} = F$$

4.3 Théorèmes intermédiaires et fin de la preuve

Pour continuer la preuve, nous avons besoin de quelques résultats intermédiaires.

Définition 4.3.1 - Compositum de groupes.

Soit H un groupe, U et V deux sous-groupes de H.

Alors on note UV le plus petit sous-groupe qui contient U et V.

Proposition 4.3.2 - Produit et intersection de groupes de Galois.

Soit E/K une extension galoisienne, L et F deux corps intermédiaires.

Alors nous avons :

- Renversement d'inclusion : $L \subseteq F \Leftrightarrow \mathrm{Gal}\big(E/F\big) \subseteq \mathrm{Gal}\big(E/L\big)$.
- Intersection de groupes de Galois : $\mathrm{Gal}\big(E/L\big) \cap \mathrm{Gal}\big(E/F\big) = \mathrm{Gal}\big(E/LF\big)$.
- $E^{\mathrm{Gal}(E/L)\,\mathrm{Gal}(E/F)} = L \cap F$ et donc $\mathrm{Gal}\big(E/L\big)\,\mathrm{Gal}\big(E/F\big) \subseteq \mathrm{Gal}\big(E/L \cap F\big)$.

Démonstration.

Premier point :

$\Rightarrow$: Puisque $L \subseteq F$, si $\sigma \in \mathrm{Aut}(E)$ préserve F alors il préserve L donc $\sigma \in \mathrm{Gal}\big(E/L\big)$.

$\Leftarrow$: D'après la deuxième étape de la preuve de 4.2.1, nous avons $L = E^{\mathrm{Gal}(E/L)} \subseteq E^{\mathrm{Gal}(E/F)} = F$.

Deuxième point :

Soit $H = \mathrm{Gal}\big(E/L\big) \cap \mathrm{Gal}\big(E/F\big)$. Toujours par la deuxième étape :

$$L = E^{\mathrm{Gal}\left(E/L\right)} \subset E^H \quad \text{et} \quad F = E^{\mathrm{Gal}\left(E/F\right)} \subset E^H$$

Ainsi, puisque E^H est un corps, nous avons $LF \subset E^H$ et donc $H \subseteq \mathrm{Gal}\Big(E/E^H\Big) \subseteq \mathrm{Gal}\big(E/LF\big)$.
Réciproquement, si $a \in \mathrm{Gal}\big(E/LF\big)$ alors $\sigma_{|LF} = \mathrm{id}$ donc $\sigma_{|L} = \mathrm{id}$ et $\sigma_{|F} = \mathrm{id}$ c'est-à-dire que $\sigma \in H$.
Ainsi $H = \mathrm{Gal}\big(E/LF\big)$.

Troisième point :
Nous avons :

$$\mathrm{Gal}\big(E/L\big) \text{ et } \mathrm{Gal}\big(E/F\big) \subseteq \mathrm{Gal}\big(E/L\big)\,\mathrm{Gal}\big(E/F\big)$$

Ainsi $E^{\mathrm{Gal}\left(E/L\right)\mathrm{Gal}\left(E/F\right)} \subseteq E^{\mathrm{Gal}\left(E/L\right)} = L$ (et pareil pour F) donc $E^{\mathrm{Gal}\left(E/L\right)\mathrm{Gal}\left(E/F\right)} \subset L \cap F$.
Réciproquement, le premier point implique que, puisque $L \cap F \subset L$ et F :

$$\mathrm{Gal}\big(E/L\big) \text{ et } \mathrm{Gal}\big(E/F\big) \subset \mathrm{Gal}\big(E/L\cap F\big) \text{ donc } \mathrm{Gal}\big(E/L\big)\,\mathrm{Gal}\big(E/F\big) \subseteq \mathrm{Gal}\big(E/L\cap F\big)$$

Ainsi $L \cap F = E^{\mathrm{Gal}\left(E/L\cap F\right)} \subseteq E^{\mathrm{Gal}\left(E/L\right)\mathrm{Gal}\left(E/F\right)}$.

Lemme 4.3.3 - Lemme auxiliaire 1.
Soit E/K une extension algébrique qui est séparable.
Supposons qu'il existe $n \in \mathbb{N}$ tel que $\forall a \in E : \deg\big(Min(a;K;X)\big) \leqslant E$. Alors E/K est finie et $[E:K] \leqslant n$.

Démonstration. Soit $a \in E$ tel que $m := \deg\big(Min(a;K;X)\big) \leqslant n$ soit maximal.
Affirmation : $E = K(a)$ et donc $[E:K] \leqslant n$.
En effet, si $b \in E \setminus K(a)$, alors d'après le théorème de l'élément primitif 3.3.1, $K(a,b) = K(c)$ pour $c \in E$.
Mais $\deg\big(Min(c;K;X)\big) = \big[K(c):K\big] > \big[K(a):K\big] = m$ ce qui contradit la maximalité de m.

Théorème 4.3.4 - Groupe de Galois du corps fixe.
Soit K un corps et $G \subset \mathrm{Aut}(K)$ un sous-groupe fini. Alors K/K^G est galoisienne et $\mathrm{Gal}\Big(K/K^G\Big) = G$.

Démonstration. Soit $n = |G|$. Nous voulons appliquer le lemme auxiliaire précédent.
Soit $a \in K$. Soit $S = \{\sigma_1, \ldots, \sigma_r\} \subset G$ un sous-ensemble maximal d'éléments de G dont les images de a sont deux à deux disjointes. Par maximalité de S, nous savons que pour tout $\tau \in G$, nous avons $\tau\sigma_i(a) \in \big\{\sigma_1(a), \ldots, \sigma_r(a)\big\}$. De plus, τ est injectif donc $\big\{\tau\sigma_1(a), \ldots, \tau\sigma_r(a)\big\}$ est une permutation de $\big\{\sigma_1(a), \ldots, \sigma_r(a)\big\}$. $(*)$

Soit $f_a = \big(X - \sigma_1(a)\big)\cdots\big(X - \sigma_r(a)\big) \in K[X]$. Alors :

- $f_a \in K^G[X]$: En effet, soit $\tau \in G$. Les coefficients de f_a sont des fonctions symétriques élémentaires de $\sigma_1(a), \ldots, \sigma_r(a)$. La propriété $(*)$ implique que chaque fonction est fixé par τ donc les coefficients de f_a sont fixés par τ. En particulier, ils sont tous dans K^G.
- $f_a \in K^G[X]$ est séparable de degré $\leqslant n$.
- $f_a(a) = 0$ car $\mathrm{id}(a) \in \big\{\sigma_1(a), \ldots, \sigma_r(a)\big\}$ par maximalité de l'ensemble S.

Ainsi $\deg\Big(Min\Big(a;K^G;X\Big)\Big) \leqslant n$ et $Min\Big(a;K^G;X\Big)$ est séparable car $Min\Big(a;K^G;X\Big) \mid f_a$.
Cela montre que K/K^G est algébrique et séparable. Par le lemme auxiliaire précédent, K/K^G est donc finie avec $\Big[K:K^G\Big] \leqslant n$. Soit finalement $a_1, \ldots, a_m$ tel que $K = K^G(a_1, \ldots, a_m)$ donc K est un corps de décomposition pour $\prod_{i=1}^m f_{a_i} \in K^G[X]$. D'après 3.2.5, K/K^G est une extension normale et donc galoisienne.
Par construction de K^G, $G \subset \mathrm{Gal}\Big(K/K^G\Big)$ et donc $n \geqslant \Big[K:K^G\Big] = |\,\mathrm{Gal}\Big(K/K^G\Big)| \geqslant |G| = n$.

Retournons à la preuve du théorème principal.

Démonstration.

Quatrième étape : Les applications α et β sont inverses :

$$\begin{array}{rccc} & \{\text{Sous-groupes de } G\} & \longleftrightarrow & \{ \text{ Corps intermédiaires de } E/K\} \\ \alpha : & H & \mapsto & E^H \\ \beta : & \mathrm{Gal}\big(E/F\big) & \hookleftarrow & F \end{array}$$

En effet, d'après la troisième étape, $F = E^{\mathrm{Gal}\left(E/F\right)}$ donc $\alpha \circ \beta(F) = F$ ainsi $\alpha \circ \beta = \mathrm{id}$. Par le théorème précédent appliqué à $H \subset \mathrm{Aut}\big(E/K\big) \subset \mathrm{Aut}(E)$, nous avons $H = \mathrm{Gal}\Big(E/E^H\Big)$ donc $\beta \circ \alpha(H) = H$ et $\beta \circ \alpha = \mathrm{id}$.

Corollaire 4.3.5 - De la quatrième étape.

Soit E/K une extension galoisienne, L et F deux corps intermédiaires.

Alors nous avons $\mathrm{Gal}\big(E/L\big)\,\mathrm{Gal}\big(E/F\big) = \mathrm{Gal}\big(E/L \cap F\big)$.

Démonstration. D'après la quatrième étape appliquée à $H = \mathrm{Gal}\big(E/L\big)\,\mathrm{Gal}\big(E/F\big) \subset \mathrm{Aut}(E)$:

$$H = \beta \circ \alpha(H)$$

D'après la proposition 4.3.2, $\alpha(H) = L \cap F$ donc $H = \beta \circ \alpha(H) = \beta(L \cap F) = \mathrm{Gal}\big(E/L \cap F\big)$.

Lemme 4.3.6 - Lemme auxiliaire 2.

Soit $\sigma \in \mathrm{Gal}\big(E/K\big)$ et F un corps intermédiare de E/K.
Alors $\mathrm{Gal}\big(E/\sigma(F)\big) = \sigma\,\mathrm{Gal}\big(E/F\big)\sigma^{-1}$ dans $\mathrm{Gal}\big(E/K\big)$.

Démonstration.

$\supseteq$: Nous avons $\sigma\,\mathrm{Gal}\big(E/F\big)\sigma^{-1} \subset \mathrm{Gal}\big(E/K\big)$.

De plus, pour $\sigma(x) \in \sigma(F)$ et $\tau \in \mathrm{Gal}\big(E/F\big)$:

$$\sigma\tau\sigma^{-1}\big(\sigma(x)\big) = \sigma\tau(x) = \sigma(x)$$

Donc $\sigma\,\mathrm{Gal}\big(E/F\big)\sigma^{-1} \subset \mathrm{Gal}\big(E/\sigma(F)\big)$.

$\subseteq$: Par le même argument $\sigma^{-1}\,\mathrm{Gal}\big(E/\sigma(F)\big)\sigma \subseteq \mathrm{Gal}\big(E/F\big)$.

On applique l'isomorphisme $\sigma(\bullet)\sigma^{-1}$ de $\mathrm{Gal}\big(E/K\big)$ pour obtenir $\mathrm{Gal}\big(E/\sigma(F)\big) \subset \sigma\,\mathrm{Gal}\big(E/F\big)\sigma^{-1}$.

Terminons de la preuve du théorème principal.

Démonstration.

Cinquième étape : F/K est galoisienne $\Leftrightarrow \mathrm{Gal}\big(E/F\big) \triangleleft \mathrm{Gal}\big(E/K\big)$.

Et dans ce cas, la restriction $\sigma \mapsto \sigma_{|F}$ induit un isomorphisme :

$$\mathrm{Gal}\big(E/K\big)\Big/\mathrm{Gal}\big(E/F\big) \cong \mathrm{Gal}\big(F/K\big)$$

$\Rightarrow$: Soit F/K une extension galoisienne.

Alors F/K est normale donc $\forall \sigma \in \mathrm{Gal}\big(E/K\big)$, $\mathrm{im}\Big(\sigma_{|F}\Big) \subset F$ par 3.2.3.

Le morphisme de groupe suivant est bien définit :

$$\begin{array}{rccc} \mathrm{res} : & \mathrm{Gal}\big(E/K\big) & \longrightarrow & \mathrm{Gal}\big(F/K\big) \\ & \sigma & \longmapsto & \sigma_{|F} \end{array}$$

Ce morphisme est surjectif car E/F est algébrique et donc par 3.1.11 tout morphisme $\tau \in \mathrm{Gal}\big(F/K\big)$ admet un prolongement $\sigma : E \to \overline{K}$. Mais E/K est normale donc par 3.2.3, $\sigma(E) = E$. Ainsi $\sigma \in \mathrm{Gal}\big(E/K\big)$ et $\sigma_{|F} = \tau$.

Par définition, nous avons $\mathrm{Ker}(\mathrm{res}) = \left\{\sigma \in \mathrm{Gal}(E/K) \mid \sigma_{|F} = \mathrm{id}\right\} = \mathrm{Gal}(E/F)$.
En particulier, $\mathrm{Gal}(E/F) \triangleleft \mathrm{Gal}(E/K)$ et res induit un isomorphisme par passage au quotient :

$$\begin{array}{ccc} \mathrm{Gal}(E/K)/\mathrm{Gal}(E/F) & \cong & \mathrm{Gal}(F/K) \\ \sigma\,\mathrm{Gal}(E/F) & \mapsto & \sigma_{|F} \end{array}$$

$\Leftarrow$: Soit $\mathrm{Gal}(E/F) \triangleleft \mathrm{Gal}(E/K)$. Par 3.3.5, puisque E/K est séparable, F/K est séparable.
Supposons pour obtenir une contradiction que F/K n'est pas normale.
Alors il existe un élément $a \in F$ tel que $Min(a; K; X)$ possède un zéro noté b dans $E \setminus F$. Soit :

$$\begin{array}{rccc} \tau : & K(a) & \longrightarrow & E \quad \text{avec } \tau_{|K} = \mathrm{id} \\ & a & \longmapsto & b \end{array}$$

- Par 3.1.10, c'est un morphisme de corps et son image n'est pas contenue dans F car $\tau(a) = b \notin F$.
- Par 3.1.11, τ admet un prolongement σ à E et par 3.2.3, puisque E/K est normale nous avons $\sigma(E) = E$.

En particulier $\sigma \in \mathrm{Gal}(E/K)$. Mais $\tau(a) \in \sigma(F)$ et $\tau(a) \notin F$. Ainsi $\sigma(F) \not\subset F$ donc $\mathrm{Gal}(E/\sigma(F)) \neq \mathrm{Gal}(E/F)$.

Le lemme auxiliaire 2 implique que $\mathrm{Gal}(E/\sigma(F)) = \sigma\,\mathrm{Gal}(E/F)\sigma^{-1} \neq \mathrm{Gal}(E/F)$.
Ainsi $\mathrm{Gal}(E/F)$ n'est pas un sous-groupe normal de $\mathrm{Gal}(E/K)$ ce qui contredit l'hypothèse.
Nous en concluons que F/K est normale ce qui termine la preuve du théorème principal.

4.4 Conséquences du théorème principal

Énonçons à présent des conséquences du théorème principal.

Théorème 4.4.1 - Tour galoisienne.
Soit E/K une extension, L et F deux corps intermédiaires.
Si l'extension L/K est galoisienne alors :

- LF/F et $L/L \cap F$ sont galoisiennes.
- Le morphisme suivant est un isomorphisme :

$$\begin{array}{rccc} \varphi : & \mathrm{Gal}(LF/F) & \longrightarrow & \mathrm{Gal}(L/L \cap F) \\ & \sigma & \longmapsto & \sigma_{|L} \end{array}$$

Et donc en particulier $[LF : F] \mid [L : K]$.

Démonstration.

- L'extension LF/F est normale et séparable par 3.2.6 et 3.3.5 donc galoisienne.
  Puisque L/K est galoisienne, $L/L \cap F$ est galoisienne par le théorème principal 4.2.1.
- Soit $\sigma \in \mathrm{Gal}(LF/F)$ alors $\sigma_{|L} : L \to E$ est un morphisme avec $\sigma_{|K} = \mathrm{id}$.
  Puisque L/K est normale, $\sigma_{|L}(L) = L$. De plus, $\sigma_{|F} = \mathrm{id}$ donc $\left(\sigma_{|L}\right)_{|L\cap F} = \mathrm{id}$ et $\sigma_{|L} \in \mathrm{Gal}(L/L \cap F)$.

  Le morphisme suivant est bien défini :

$$\begin{array}{rccc} \varphi : & \mathrm{Gal}(LF/F) & \longrightarrow & \mathrm{Gal}(L/L \cap F) \\ & \sigma & \longmapsto & \sigma_{|L} \end{array}$$

  Montrons qu'il est injectif :
  Soit $\sigma \in \mathrm{Gal}(LF/F)$ tel que $\sigma_{|L} = \mathrm{id}$. Alors $L \subseteq LF^{\{\sigma\}}$ et bien sur $F \subseteq LF^{\{\sigma\}}$ donc $LF \subset LF^{\{\sigma\}}$ donc $\sigma = \mathrm{id}$.

  Montrons à présent que φ est surjectif : Soit $H = \mathrm{im}(\varphi) \subset \mathrm{Gal}(L/L \cap F)$.
  Affirmation : $L^H = L \cap F$.
  $\supseteq$: Nous avons $L \cap F = L^{\mathrm{Gal}(L/L\cap F)} \subset L^H$ car $H \subset \mathrm{Gal}(L/L \cap F)$.
  $\subseteq$: Soit $a \in L^H$. Par définition de H, $a = \left(\sigma_{|L}\right)(a)$ pour tout $\sigma \in \mathrm{Gal}(LF/F)$.

Ainsi $a \in LF^{\mathrm{Gal}(LF/F)} = F$ et donc $a \in L \cap F$.

Nous en déduisons par le théorème principal que $H = \mathrm{Gal}\Big(L/L^H\Big) = \mathrm{Gal}\big(L/L \cap F\big)$. Ainsi φ est surjectif.

- Nous avons simplement :

$$[L : K] = [L : L \cap F] \cdot [L \cap F : K] = [LF : F] \cdot [L \cap F : K] \Rightarrow [LF : F] \mid [L : K]$$

Théorème 4.4.2 - Tour galoisienne 2.

Soit E/K une extension, L et F deux corps intermédiaires.

Si les extensions L/K et F/K sont galoisiennes alors :

1. LF/K est une extension galoisienne.
2. Le morphisme suivant est surjectif :

$$\begin{array}{rccc} \mathrm{res} : & \mathrm{Gal}\big(LF/K\big) & \longrightarrow & \mathrm{Gal}\big(L/K\big) \times \mathrm{Gal}\big(F/K\big) \\ & \sigma & \longmapsto & \Big(\sigma_{|L}, \sigma_{|F}\Big) \end{array}$$

3. Si $L \cap F = K$ alors l'application res est un isomorphisme.

Démonstration.

1. L'extension LF/K est normale par 3.2.6 et séparable par 3.3.5 donc galoisienne.
2. Comme dans le deuxième point de 4.4.1 :
   - $\sigma \mapsto \sigma_{|L}$ est un morphisme de groupes $\mathrm{Gal}\big(LF/K\big) \to \mathrm{Gal}\big(L/K\big)$ bien défini.
   - $\sigma \mapsto \sigma_{|F}$ est un morphisme de groupes $\mathrm{Gal}\big(LF/K\big) \to \mathrm{Gal}\big(F/K\big)$ bien défini.

   Par la propriété universelle du produit, $\sigma \mapsto \Big(\sigma_{|L}, \sigma_{|F}\Big)$ est un morphisme bien défini de $\mathrm{Gal}\big(LF/K\big)$ dans $\mathrm{Gal}\big(L/K\big) \times \mathrm{Gal}\big(F/K\big)$. De plus, il est injectif car si $\sigma_{|L} = \mathrm{id}$ alors $LF \subset LF^{\{\sigma\}}$ donc $\sigma = \mathrm{id}$.
3. Soit $L \cap F = K$. Soit $\tau \in \mathrm{Gal}\big(L/K\big)$. D'après 4.4.1, il existe $\sigma \in \mathrm{Gal}\big(LF/F\big)$ avec $\sigma_{|L} = \tau$.

   Ainsi, $\sigma_{|L} = \tau$ et $\sigma_{|F} = \mathrm{id}$ donc $\mathrm{Gal}\big(L/K\big) \times \{\mathrm{id}\} \subset \mathrm{im(res)}$. De même, $\{\mathrm{id}\} \times \mathrm{Gal}\big(F/K\big) \subset \mathrm{im(res)}$.

   Nous en concluons que $\mathrm{Gal}\big(L/K\big) \times \mathrm{Gal}\big(F/K\big) \subset \mathrm{im(res)}$.

5. Corps finis et racines de l'unité

5.1 Corps finis

Soit k un corps fini.
D'après 3.3.8, il existe un sous-corps premier $\mathbb{F}_p \subset k$ pour exactement un nombre premier $p = \operatorname{Car} k > 0$.

Alors k est une extension finie de $\mathbb{F}_p$. Soit $\overline{\mathbb{F}_p}/\mathbb{F}_p$ une clôture algébrique fixée.

Par 3.1.11, il existe un morphisme $\sigma : k \hookrightarrow \overline{\mathbb{F}_p}$ avec $\sigma_{|\mathbb{F}_p} = \mathrm{id}$ c'est-à-dire :

$$k/\mathbb{F}_p \cong k'/\mathbb{F}_p \text{ avec } k' = \sigma(k) \subset \overline{\mathbb{F}_p}$$

Pour étudier tous les corps finis, il suffit donc de considérer les corps intermédiaires de $\overline{\mathbb{F}_p}/\mathbb{F}_p$.

Théorème 5.1.1 - Corps intermédiaires de $\overline{\mathbb{F}_p}/\mathbb{F}_p$.
Soit $\overline{\mathbb{F}_p}/\mathbb{F}_p$ une clôture algébrique fixée.
Pour tout $n \geqslant 1$, il existe exactement un corps intermédiaire $\mathbb{F}_{p^n}$ tel que $\left[\mathbb{F}_{p^n} : \mathbb{F}_p\right] = n$.
De plus, nous avons :

1. $|\mathbb{F}_{p^n}| = p^n$.
2. $\mathbb{F}_{p^n}$ est le corps de décomposition de $X^{p^n} - X \in \mathbb{F}_p[X]$.
3. $\mathbb{F}_{p^n} = \left\{a \in \overline{\mathbb{F}_p} \mid a^{p^n} = a\right\}$.
4. $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ si et seulement si $n \mid m$. Dans ce cas, $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ est galoisienne.

Démonstration. Montrons les trois premiers points :

Soit k un corps intermédiaire de $\overline{\mathbb{F}_p}/\mathbb{F}_p$ avec $\left[k : \mathbb{F}_p\right] = n$.
Alors $|k| = |\mathbb{F}_p|^{\left[k:\mathbb{F}_p\right]} = p^n$. D'après 2.2.11, $k^\times$ est cyclique d'ordre $p^n - 1$.
Par le théorème de Lagrange 2.1.6, $\forall a \in k^\times : a^{p^n-1} = 1$ donc $a^{p^n} = a$ et :

$$k = \left\{\text{zéros de } X^{p^n} - X \in \mathbb{F}_p[X]\right\}$$

Ainsi $k = \mathbb{F}_p\left(\text{zéros de } X^{p^n} - X\right)$ donc k est le corps de décomposition dans $\overline{\mathbb{F}_p}$ de $X^{p^n} - X$.

En particulier, k est uniquement déterminé par la condition $\left[k : \mathbb{F}_p\right] = n$.

Réciproquement, soit $n \geqslant 1$ et $f = X^{p^n} - X \in \mathbb{F}_p[X]$. Alors $f' = p^n X^{p^n-1} - 1 = -1 \neq 0$.
Ainsi, f est séparable : En effet, comme dans la preuve de 3.3.10, si f n'était pas séparable, alors $\operatorname{pgcd}(f, f')$ n'est pas égal à 1. Ainsi f a exactement p^n zéros deux à deux distincts dans $\overline{\mathbb{F}_p}$.

Mais $k = \{\text{zéros de } f\} \subset \overline{\mathbb{F}_p}$ est un sous-corps de $\overline{\mathbb{F}_p}$:
En effet, si $a, b \in k$ alors $a^{p^n} = a$ et $b^{p^n} = b$ et $(a \pm b)^{p^n} = a^{p^n} \pm a^{p^n} = a \pm b$ donc $a \pm b \in k$ etc ...
Ce corps contient $\mathbb{F}_p$ car $\forall a \in \mathbb{F}_p : a^{p^n} = a$ et $|k| = p^n$ donc $\left[k : \mathbb{F}_p\right] = n$.

Montrons le dernier point :
$\Rightarrow$: $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \Rightarrow n\left[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}\right] = \left[\mathbb{F}_{p^n} : \mathbb{F}_p\right]\left[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}\right] = \left[\mathbb{F}_{p^m} : \mathbb{F}_p\right] \Rightarrow n \mid m$.
$\Leftarrow$: Supposons que $n \mid m$. Nous avons :

$$\frac{p^m - 1}{p^n - 1} = p^{m-n} + p^{m-2n} + \cdots + 1 \Rightarrow p^n - 1 \mid p^m - 1$$

Donc si $a \in \overline{\mathbb{F}_p}$ non nul avec $a^{p^n} = a$ alors $a^{p^n-1} = 1$ donc $a^{p^m-1} = 1$ ainsi $a^{p^m} = a$.

D'après 3., $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$.

- $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ est normale d'après 3.2.5 car :
  $\mathbb{F}_{p^m}$ est le corps de décomposition du polynôme séparable $X^{p^m} - X \in \mathbb{F}_{p^n}[X]$.
- $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ est séparable car si $a \in \mathbb{F}_{p^m}$ est un zéro de $X^{p^m} - X$ alors $Min\big(a; \mathbb{F}_{p^n}; X\big) \mid X^{p^m} - X$ et donc a est séparable sur $\mathbb{F}_{p^n}$. Par 3.3.3, $\mathbb{F}_{p^m} = \mathbb{F}_{p^n}\Big($ tous les zéros de $X^{p^m} - X\Big)$ est séparable sur $\mathbb{F}_{p^n}$.

  Donc $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ est galoisienne.

Corollaire 5.1.2 - Unicité des corps finis.
Tout corps fini k est isomorphe à un corps $\mathbb{F}_{p^n}$ pour un unique $n \geqslant 1$.
Toute extension finie de k est galoisienne. En particulier, tout corps fini est parfait.

Démonstration. Soit $n = \big[k : \mathbb{F}_p\big]$.

Nous savons que $k \cong k'$ où k' est un sous-corps fini de $\overline{\mathbb{F}_p}$. D'après 5.1.1, $k' = \mathbb{F}_{p^n}$.

Soit E/k une extension finie
Choisissons un isomorphisme $k \cong \mathbb{F}_{p^n}$ et un prolongement $\sigma : E \to \overline{\mathbb{F}_p}$ à E.
Nous avons $E/k \cong \mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ et 5.1.1 implique que E/k est galoisienne.

$$\begin{array}{ccc} E & \xrightarrow{\cong} & \mathbb{F}_{p^m} \\ \uparrow & & \uparrow \\ k & \xrightarrow{\cong} & \mathbb{F}_{p^n} \end{array}$$

Théorème 5.1.3 - Groupe de Galois d'une extension de corps fini.
Le groupe $\mathrm{Gal}\big(\mathbb{F}_{p^n}/\mathbb{F}_p\big)$ et cyclique d'ordre n.
L'automorphisme de Frobenius est un générateur de $\mathrm{Gal}\big(\mathbb{F}_{p^n}/\mathbb{F}_p\big)$:

$$\begin{array}{rccc} \varphi : & \mathbb{F}_{p^n} & \longrightarrow & \mathbb{F}_{p^n} \\ & a & \longmapsto & a^p \end{array}$$

Nous avons donc $\mathrm{Gal}\big(\mathbb{F}_{p^n}/\mathbb{F}_p\big) \cong \mathbb{Z}/n\mathbb{Z}$

Démonstration. Le théorème principal implique que $|\mathrm{Gal}\big(\mathbb{F}_{p^n}/\mathbb{F}_p\big)| = \big[\mathbb{F}_{p^n} : \mathbb{F}_p\big] = n$.

De plus, $\varphi \in \mathrm{Gal}\big(\mathbb{F}_{p^n}/\mathbb{F}_p\big)$ car :

- L'image de φ est dans $\mathbb{F}_{p^n}$ car $\forall a, b \in \mathbb{F}_{p^n}$ nous avons a^p et $b^p \in \mathbb{F}_{p^n}$.
- φ est un morphisme car $(a \pm b) = a^p \pm b^p$ et $(ab)^p = a^p b^p$ et $1^p = 1$.
- φ préserve $\mathbb{F}_p$ car $\forall a \in \mathbb{F}_p : a^p = a$.

Montrons que φ génère $\mathrm{Gal}\big(\mathbb{F}_{p^n}/\mathbb{F}_p\big)$:
On considère le sous-groupe $\langle\varphi\rangle \subset \mathrm{Gal}\big(\mathbb{F}_{p^n}/\mathbb{F}_p\big)$.
Il reste à montrer que $\mathrm{ord}(\varphi) = n$ c'est-à-dire $\varphi, \varphi^2, \ldots, \varphi^{n-1}, \varphi^n = \mathrm{id}_{\mathbb{F}_{p^n}}$ sont distincts.

$$\forall a \in \mathbb{F}_{p^n} : \varphi^n(a) = a^{p^n} = a$$

Supposons pour obtenir une contradiction que $\varphi^k = \varphi^{k+i}$. Donc $\varphi^i = \mathrm{id}$ pour un $1 \leqslant i < n$. Ainsi :

$$\forall x \in \mathbb{F}_{p^n} : x^{p^i} = \varphi^i(x) = x \Rightarrow \mathbb{F}_{p^n} \subset \mathbb{F}_{p^i} \Rightarrow n \mid i$$

C'est impossible, ainsi $\langle\varphi\rangle = \mathrm{Gal}\big(\mathbb{F}_{p^n}/\mathbb{F}_p\big)$.

5.2 Racines de l'unité

Soit K un corps et $n \in \mathbb{N}$.

Définition 5.2.1 - Racine n^e de l'unité.
Soit K un corps.
On appelle *racine n^e de l'unité* tout élément $\zeta \in K$ tel que $\zeta^n = 1$.
Nous notons $\mathbb{U}_n(K)$ l'ensemble des racines n^e de K.

Lemme 5.2.2 - Groupe des racines n^e.
Soit K un corps. Alors :
1. $\mathbb{U}_n(K) := \{\zeta \in K : \zeta^n = 1\}$ est un sous-groupe fini cyclique de $K^\times$.
2. Soit $\operatorname{Car} K = p > 0$ et $n = p^r m$ avec $p \nmid m$. Alors $\mathbb{U}_n(K) = \mathbb{U}_m(K)$.

Démonstration.
1. Nous savons que $\mathbb{U}_n(K)$ est un sous-groupe de $K^\times$.
Par définition, $\mathbb{U}_n(K) = \{\text{zéros de } X^n - 1 \text{ dans } K\}$ d'où $|\mathbb{U}_n(K)| \leqslant n$.
Ainsi par 2.2.8, $\mathbb{U}_n(K)$ est cyclique.
2. Soit $\zeta \in \mathbb{U}_n(K)$. Alors :
$$0 = \zeta^n - 1 = \left(\zeta^m\right)^{p^r} - 1 = \left(\zeta^m - 1\right)^{p^r} \Rightarrow \zeta^m - 1 = 0$$
Ainsi $\zeta \in \mathbb{U}_m(K)$ et donc $\mathbb{U}_n(K) \subseteq \mathbb{U}_m(K)$.

Fixons une clôture algébrique $\overline{K}/K$.

Définition 5.2.3 - Racine primitif.
Soit K un corps et $n \geqslant 2$.
On appelle *racine n^e primitif de K* tout élément $\zeta \in \mathbb{U}_n(\overline{K})$ tel que $\operatorname{ord}(\zeta) = n$.

À partir de maintenant, on suppose que $\operatorname{Car} K = 0$ ou $\operatorname{Car} K \nmid n$.

Proposition 5.2.4 - Séparabilité de $X^n - 1$.
Soit K un corps tel que $\operatorname{Car} K = 0$ ou $\operatorname{Car} K \nmid n$.
Alors :
1. $X^n - 1 \in K[X]$ est séparable et donc $|\mathbb{U}_n(\overline{K})| = n$.
2. Si $\zeta \in \mathbb{U}_n(\overline{K})$ est primitif alors $\mathbb{U}_n(\overline{K}) = \langle\zeta\rangle$ et $K(\zeta)$ est un corps de décomposition de $X^n - 1 \in K[X]$.

Démonstration.
1. Nous savons que $nX^{n-1} \neq 0$ donc en utilisant le raisonnement de la preuve de 3.3.10, $X^n - 1$ est séparable.
2. Ce résultat est clair car $K(\zeta) = K\big(\langle\zeta\rangle\big) = K\Big(\mathbb{U}_n(\overline{K})\Big)$

Introduisons à présent la quantité $\kappa(\sigma)$.

Soit $K_n \subseteq \overline{K}$ le corps de décomposition de $X^n - 1 \in K[X]$.
Alors K_n/K est normal d'après 3.2.5 et séparable d'après 5.2.4. Ainsi K_n/K et galoisienne.

Théorème 5.2.5 - Quantité $\kappa(\sigma)$.
Soit $\mathbb{U}_n = \mathbb{U}_n(\overline{K})$ et $G_n = \operatorname{Gal}\big(K_n/K\big)$. Soit $\sigma \in G_n$.
Alors :
1. Il existe un entier $\kappa(\sigma) \in \mathbb{Z}$ tel que $\forall \zeta \in \mathbb{U}_n : \sigma(\zeta) = \zeta^{\kappa(\sigma)}$.
2. Les entiers $\kappa(\sigma)$ et n sont premiers entre eux.
3. Soit $b \in \mathbb{Z}$ tel que $\forall \zeta \in \mathbb{U}_n : \sigma(\zeta) = \zeta^b$. Alors $n \mid \big(b - \kappa(\sigma)\big)$.

Démonstration.

1. Soit $\zeta_0 \in \mathbb{U}_n$ une racine primitif. Alors $\mathbb{U}_n = \langle \zeta_0 \rangle$.
   Nous avons $\sigma(\zeta_0) = \zeta_0^{\kappa(\sigma)} \in \mathbb{U}_n$ pour un entier $\kappa(\sigma) \in \mathbb{Z}$ d'où :
   $$\forall \zeta \in \mathbb{U}_n : \sigma(\zeta) = \sigma(\zeta_0)^a = (\zeta_0)^{\kappa(\sigma)a} = \zeta^{\kappa(\sigma)}$$
2. Soit $d = \operatorname{pgcd}\big(\kappa(\sigma), n\big)$. Alors :
   $$\mathbb{U}_n = \sigma(\mathbb{U}_n) = \big\langle \sigma(\zeta_0) \big\rangle = \left\langle \left(\zeta_0^d\right)^{\frac{\kappa(\sigma)}{d}} \right\rangle$$
   Mais $\operatorname{ord}\left(\zeta_0^d\right) = \dfrac{n}{d}$ donc $n = |\mathbb{U}_n| \leqslant \dfrac{n}{d}$ et $d = 1$.
3. Nous avons $\zeta_0^b = \sigma(\zeta_0) = \zeta_0^{\kappa(\sigma)}$ d'où $\zeta_0^{b-\kappa(\sigma)} = 1$. Ainsi $n = \operatorname{ord}(\zeta_0) \mid \big(b - \kappa(\sigma)\big)$.

Proposition 5.2.6 - Morphisme $\overline{\kappa}$.
L'application $\overline{\kappa}$ est un morphisme de groupes injectif :
$$\begin{array}{rccc} \overline{\kappa} : & G_n & \longrightarrow & \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \\ & \sigma & \longmapsto & \kappa(\sigma) \mod n\mathbb{Z} \end{array}$$
En particulier G_n est abélien.

Démonstration. Les deux premiers point de 5.2.5 assure que l'application suivante est bien définie.
$$\begin{array}{rccc} \phi : & G_n & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & \sigma & \longmapsto & \kappa(\sigma) \mod n\mathbb{Z} \end{array}$$
D'après le deuxième point $\kappa(\sigma) \mod n\mathbb{Z} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ donc nous obtenons $\phi : G_n \to \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$:

Montrons que ϕ est un morphisme de groupe. Soit $\sigma, \tau \in G_n$. Alors :
$$\sigma\big(\tau(\zeta_0)\big) = \sigma\left(\zeta^{\kappa(\tau)}\right) = \sigma(\zeta_0)^{\kappa(\tau)} = \zeta_0^{\kappa(\sigma)\kappa(\tau)}$$
Si $\zeta \in \mathbb{U}_n$ alors $\zeta = \zeta_0^a$ et donc $\sigma\tau(\zeta) = \zeta^{\kappa(\sigma)\kappa(\tau)}$.
Soit $b = \kappa(\sigma)\kappa(\tau) \in \mathbb{Z}$. D'après 3., $n \mid \big(b - \kappa(\sigma\tau)\big)$ donc $\big(\kappa(\sigma) \mod n\mathbb{Z}\big)\big(\kappa(\tau) \mod n\mathbb{Z}\big) = \kappa(\sigma\tau) \mod n\mathbb{Z}$.

Enfin, ce morphisme est injectif car si $\kappa(\sigma) = 1 \mod n\mathbb{Z}$ alors :
$$\forall \zeta \in \mathbb{U}_n : \sigma(\zeta) = \zeta^{\kappa(\sigma)} = \zeta$$
Ainsi $K_n = K(\zeta_0) \subseteq K_n^{\{\sigma\}}$ donc $\sigma = \mathrm{id}$.

Remarque.
On peut démontrer à l'aide du critère d'Eisenstein que pour $K = \mathbb{Q}$ on a $[\mathbb{Q}_n : \mathbb{Q}] = |\big(\mathbb{Z}/n\mathbb{Z}\big)^\times|$ (irréductibilité du n^{e} polynôme cyclotomique). Il suit que l'application $\overline{\kappa}$ est surjective pour $K = \mathbb{Q}$:
$$\operatorname{Gal}\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \text{ où } \zeta \in \mathbb{U}_n(\overline{\mathbb{Q}}) \text{ est une racine } n^{\text{e}} \text{ primitif.}$$
Par exemple, pour $n = p$ premier, on sait que $Min(\zeta; \mathbb{Q}; X) = X^{p-1} + X^{p-2} + ... + X + 1$ et $|\big(\mathbb{Z}/p\mathbb{Z}\big)^\times| = p - 1$. ♢