Module ALGB

Cours : Laurent Moret–Bailly

16 janvier 2011

Table des matières

Chapitre 1

Groupes, anneaux, corps et modules

1.1 "Rappels" sur les ensembles quotients

Définition 1.1.1 (Relation binaire)
Une relation binaire sur un ensemble E est une partie $\mathcal{R}$ de $E \times E$.

✍ On notera en général $x\mathcal{R}y$ pour dire que $(x, y) \in \mathcal{R}$.

Définition 1.1.2 (Classe d'équivalence)
Soit E un ensemble et soit $\mathcal{R}$ une relation d'équivalence (i.e réflexive, transitive et symétrique) sur E.
Pour $x \in E$, on appelle classe d'équivalence de x modulo $\mathcal{R}$ l'ensemble :

$$\overline{x} = \{y \in E \,|\, x\mathcal{R}y\}$$

Exemple fondamental : Soient E et F deux ensembles et soit $f : E \to F$. On définit alors une relation d'équivalence (appelée relation associée à f) sur E par :

$$\mathcal{R} = \{(x, y) \in E^2 \,|\, f(x) = f(y)\}$$

Si $x \in E$, on a alors :

$$\overline{x} = f^{-1}(\{f(x)\})$$

Proposition 1.1.1
Soit E un ensemble et soit $\mathcal{R}$ une relation d'équivalence sur E.
Alors :

(i) si $x, y \in E$, on a :

$$x\mathcal{R}y \Leftrightarrow \overline{x} = \overline{y} \Leftrightarrow \overline{x} \cap \overline{y} \neq \emptyset$$

(ii) les classes modulo $\mathcal{R}$ forment une partition de E (i.e sont des parties non vides deux à deux disjointes dont la réunion est égale à E) ;

(iii) Inversement, toute partition π de E est l'ensemble des classes modulo une unique relation d'équivalence définie par :

$$\mathcal{R}_\pi = \left\{(x, y) \in E^2 \,|\, \exists C \in \pi,\ \{x, y\} \subset C\right\}$$

Exemple : Dans le cas où $E = \mathbb{Z}$ et où $x\mathcal{R}y \Leftrightarrow x \equiv y[3]$ alors on a trois classes d'équivalences modulo $\mathcal{R}$:

$$\overline{0} = 3\mathbb{Z}$$
$$\overline{1} = 1 + 3\mathbb{Z}$$
$$\overline{2} = 2 + 3\mathbb{Z} = \overline{-1}$$

Définition 1.1.3 (Ensemble quotient, projection canonique)
Soit E un ensemble et soit $\mathcal{R}$ une relation d'équivalence sur E.
Alors on note $E/\mathcal{R}$ l'ensemble des classes d'équivalences modulo $\mathcal{R}$, appelé ensemble quotient de E par $\mathcal{R}$.
On a alors une application naturelle, appelée projection canonique, $\pi_{\mathcal{R}} : E \to E/\mathcal{R}$ définie par :

$$\forall x \in E,\ \pi_{\mathcal{R}}(x) = \overline{x}$$

Proposition 1.1.2
Soit E un ensemble et soit $\mathcal{R}$ une relation d'équivalence sur E.
Alors :

(i) $\pi_{\mathcal{R}}$ est surjective (car les classes modulo $\mathcal{R}$ sont non vides) ;

(ii) la relation associée à $\pi_{\mathcal{R}}$ est $\mathcal{R}$, i.e :

$$\forall x \in E,\ \overline{x} = \pi_{\mathcal{R}}^{-1}\left(\{\pi_{\mathcal{R}}(x)\}\right)$$

☞ Toute relation d'équivalence $\mathcal{R}$ sur E est de la forme $\mathcal{R}_f$, avec $f : E \to F$ une application surjective. F et f dépendent alors de $\mathcal{R}$.

Définition 1.1.4 (Compatibilité d'une relation et d'une application)
Soient E et F deux ensembles.
Soit $\mathcal{R}$ une relation d'équivalence sur E et soit $f : E \to F$.
Alors on dit que f et $\mathcal{R}$ sont compatibles si pour tous $x, y \in E$, si $x\mathcal{R}y$ alors $f(x) = f(y)$, i.e si f est constante sur chaque classe modulo $\mathcal{R}$.

Exemples :

1. $\mathcal{R}$ et $\pi_{\mathcal{R}}$ sont toujours compatibles.
2. Une fonction $f : \mathbb{R} \to F$ est paire si elle est compatible avec la relation "$x = \pm y$".
3. Une fonction $f : \mathbb{R} \to F$ est T–périodique ($T \in \mathcal{R}$) si elle est compatible avec la relation "$x - y \in T\mathbb{Z}$".

Proposition 1.1.3 (Propriété universelle du quotient)
Soient E et F deux ensembles.
Soit $\mathcal{R}$ une relation d'équivalence sur E et soit $\varphi : E \to F$.
Les propriétés suivantes sont alors équivalentes :

(i) φ et $\mathcal{R}$ sont compatibles ;

(ii) φ se factorise[1] par $\pi_{\mathcal{R}}$, i.e $\exists \overline{\varphi} : E/\mathcal{R} \to F$ telle que :

$$\varphi = \overline{\varphi} \circ \pi_{\mathcal{R}}$$

De plus, lorsque c'est le cas, $\overline{\varphi}$ est unique.

✌ On résume souvent la proposition 1.1.3 par le diagramme suivant :

$$\begin{tikzcd}
E \arrow[r, "\varphi"] \arrow[d, "\pi_{\mathcal{R}}"'] \arrow[dr, phantom, "\circlearrowleft"] & F \\
E/\mathcal{R} \arrow[ur, "\exists!\overline{\varphi}"'] &
\end{tikzcd}$$

Le symbole "$\circlearrowleft$" indique que le diagramme commute, i.e que $\varphi = \overline{\varphi} \circ \pi_{\mathcal{R}}$.
DÉMONSTRATION :

$(i) \Rightarrow (ii)$ – *Unicité.* Soient $\overline{\varphi}$ et $\overline{\varphi}'$ deux applications vérifiant la condition. Alors $\overline{\varphi} \circ \pi_{\mathcal{R}} = \overline{\varphi}' \circ \pi_{\mathcal{R}}$ et donc (modulo l'axiome du choix), comme $\pi_{\mathcal{R}}$ est surjective on a que $\overline{\varphi} = \overline{\varphi}'$.

1. On dit parfois "passe au quotient".

– *Existence.* Si $\xi \in E/\mathcal{R}$, remarquons que φ est constante sur ξ. On peut donc définir $\overline{\varphi}(\xi)$ comme la valeur de φ sur cette classe (ce qui est possible car, rappelons–le, les classes d'équivalence sont non vides). De plus, si $x \in E$ alors :

$$\overline{\varphi}\left(\pi_{\mathbb{R}}(x)\right) = \overline{\varphi}(\overline{x}) = \varphi(x) \quad \text{en particulier.}$$

D'où le résultat.

☞ Les seules propriétés de $\pi_{\mathcal{R}}$ que nous avons utilisées ici sont sa surjectivité et le fait que la relation d'équivalence qui lui est associée est $\mathcal{R}$. Autrement dit, toute application de E dans un ensemble quelconque ayant ces propriétés peut "servir de quotient par $\mathcal{R}$". Par exemple, pour $n \geq 1$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ peut être défini comme le "quotient" de $\mathbb{Z}$ par l'application qui à un entier associe le reste de sa division euclidienne par n.

Définition 1.1.5 (Groupe)
Soit G un ensemble et soit $*$ une loi de composition interne (LCI) sur G, i.e une application de $G \times G$ dans G.
Alors on dit que le couple $(G, *)$ est un groupe si :

(i) la loi $*$ est associative, i.e :

$$\forall x, y, z \in G,\ x * (y * z) = (x * y) * z$$

(ii) G possède un élément neutre pour $*$, i.e :

$$\exists e_G \in G, \forall x \in G,\ e_G * x = x * e_G = x$$

(iii) tout élément de G est inversible, i.e :

$$\forall x \in G, \exists \widehat{x} \in G,\ x * \widehat{x} = \widehat{x} * x = e_G$$

Si de plus $*$ est commutative, i.e si $\forall x, y \in G,\ x * y = y * x$, on dit que G est abélien.

✍ Dans un groupe G, l'inverse d'un élément x est souvent noté x^{-1} (si la loi de G est notée multiplicativement) ou $-x$ (si la loi de G est notée additivement).

Définition 1.1.6 (Loi quotient)
Soit E un ensemble muni d'une relation d'équivalence $\sim$ de projection canonique π et d'une LCI $* : E \times E \to E$.
Alors, on dit que $*$ passe au quotient par $\sim$ si il existe une LCI $\overline{*}$ sur $E/\sim$, appelée loi quotient, telle que π soit un morphisme de $(E, *)$ dans $(E/\sim, \overline{*})$.

✘ Les ensembles $(E, *)$ et $(E/\sim, \overline{*})$ ne sont pas nécessairement des groupes !

Remarques :

1. Si $\overline{*}$ existe, elle est unique, car si $\xi = \pi(x), \eta = \pi(y) \in E/\sim$ alors nécessairement :

$$\xi \overline{*} \eta = \pi(x) \overline{*} \pi(y) = \pi(x * y)$$

2. Si il existe $x, x', y, y' \in E$ tels que $\pi(x) = \pi(x')$ et $\pi(y) = \pi(y')$ mais vérifiant que $\pi(x*y) \neq \pi(x'*y')$, alors il n'existe pas de loi quotient $\overline{*}$.
3. Si la loi quotient existe, elle hérité de l'éventuelle associativité/commutativité de $*$. De même, si e est un neutre pour $*$, $\pi(e)$ en est un pour $\overline{*}$ et si x, x' sont symétriques pour $*$ alors $\pi(x)$ et $\pi(x')$ le sont pour $\overline{*}$.

Proposition 1.1.4
Soit E un ensemble muni d'une relation d'équivalence $\sim$ de projection canonique π et d'une loi de composition interne (LCI) $* : E \times E \to E$.
Alors, les propriétés suivantes sont équivalentes :

(i) $*$ passe au quotient pour $\sim$;

(ii) $*$ *et* $\sim$ *sont compatibles, i.e pour tous* $x, x', y, y' \in E$ *tels que* $x \sim x'$ *et* $y \sim y'$ *alors* $x * y \sim x' * y'$.

DÉMONSTRATION :

$(i) \Rightarrow (ii)$ Soient $x, x', y, y' \in E$ tels que $x \sim x'$ et $y \sim y'$. Alors on a $\pi(x) = (x')$ et $\pi(y) = (y')$ donc $\pi(x)\overline{*}\pi(y) = \pi(x')\overline{*}\pi(y')$ ce qui implique que $\pi(x * y) = \pi(x' * y')$, donc $x * y \sim x' * y'$.

$(ii) \Rightarrow (i)$ Comme $*$ et $\sim$ sont compatibles, si on fixe $\xi, \eta \in E/\sim$ l'application $(x, y) \mapsto \pi(x * y)$ est constante sur $\xi \times \eta$. On peut alors définir $\xi\overline{*}\eta$ comme la valeur de cette application. On obtient alors une LCI sur $E/\sim$ telle que π soit un morphisme de $(E, *)$ dans $(E/\sim, \overline{*})$.

✌ Calculer dans $E/\sim$ revient donc à calculer dans E en traitant la relation $\sim$ comme une égalité.

1.2 Groupes quotients

Définition 1.2.1 (Sous–groupe)
Soit $(G, *)$ *un groupe.*
On dit que $H \subset G$ *est un sous–groupe de* G *si* $*$ *induit sur* H *une structure de groupe, i.e si :*

(i) $e_G \in H$ *;*

(ii) $\forall x, y \in H,\ x * y^{-1} \in H$

Définition 1.2.2 (Morphisme de groupes, noyau, image)
Soient $(G, *)$ *et* $(H, \diamond)$ *deux groupes.*
Une application $f : G \to H$ *est alors appelée morphisme de groupes (de* G *sur* H*) si elle vérifie la condition suivante :*

$$\forall x, y \in G, \quad f(x * y) = f(x) \diamond f(y)$$

On définit le noyau de f *de la façon suivante :*

$$\mathrm{Ker}(f) := \{x \in G \,|\, f(x) = e_H\} \subset G$$

On appelle image de f *l'ensemble suivant :*

$$\mathrm{Im}(f) := \{f(x) \,|\, x \in G\} \subset H$$

☞ Ainsi, $\forall x \in G$, $f(x*e_G) = f(e_G)\diamond f(x)$ et donc $f(e_G) = e_H$. De plus, $f(x*x^{-1}) = f(x)\diamond f(x^{-1})$ donc $f(x)^{-1} = f(x^{-1})$.

✍ On note $\mathrm{End}(G)$ l'ensemble des endomorphismes du groupe G (i.e des morphismes de G sur lui–même).

Soit $\sim$ une relation d'équivalence sur G, de projection canonique π. Alors, si $\sim$ est compatible avec la loi de G, π est un morphisme surjectif vers la loi quotient, ce qui entraîne que l'ensemble G/π est un groupe d'élément neutre $\pi(e_G)$.

De plus, $\sim$ est la relation associée à π, i.e :

$$\forall x, y \in G, \quad x \sim y \Leftrightarrow \pi(x) = \pi(y)$$

En particulier,

$$\mathrm{Ker}\,\pi = \pi^{-1}\left(\{\pi(e_G)\}\right) = \overline{e_G}$$

Ainsi, $\overline{e_G}$ est un sous–groupe de G.

Proposition 1.2.1
Soient G *et* H *deux groupes.*
Soit $f : G \to H$ *un morphisme.*
Alors la relation associée à f *est déterminée par* $\mathrm{Ker}\,f$*, i.e si* $x, y \in G$ *on a :*

$$f(x) = f(y) \Leftrightarrow xy^{-1} \in \mathrm{Ker}\,f \Leftrightarrow x^{-1}y \in \mathrm{Ker}\,f$$

✍ Ainsi, si $x \in G$, on a :

$$\overline{x} = f^{-1}\left(\{f(x)\}\right) = x\,\mathrm{Ker}(f) = \mathrm{Ker}(f)x$$

En particulier :

$$\forall x \in G,\ x\,\mathrm{Ker}(f)x^{-1} = \mathrm{Ker}(f) \tag{1.1}$$

Définition 1.2.3 (Sous–groupe distingué)
Un sous–groupe N d'un groupe G est dit distingué (dans G) si l'une des trois conditions équivalentes suivantes est vérifiée[2] *:*

(i) $\forall x \in G, \forall n \in N, xnx^{-1} \in N$;

(ii) $\forall x \in G, xNx^{-1} = N$;

(iii) *N est invariant par les automorphismes intérieurs (i.e de la forme $g \mapsto xgx^{-1}$) de G.*

✍ On note alors $N \lhd G$.

Remarques :

1. D'après (1.1), si $f : G \to H$ est un morphisme de groupes, alors $\mathrm{Ker}(f) \lhd G$.
2. Toute relation d'équivalence compatible avec la loi d'un groupe G est de la forme "$xy^{-1} \in N$", avec $N = \overline{e_G} \lhd G$.

Exemples :

1. Pour tout groupe G, on a $\{e_G\} \lhd G$ et $G \lhd G$.
2. Si G est un groupe abélien, tout sous–groupe y est distingé (la réciproque est fausse).
3. Si $\mathbb{K}$ est un corps, alors $SL_n(\mathbb{K}) \lhd GL_n(\mathbb{K})$ car $SL_n(\mathbb{K}) = \mathrm{Ker}(\det)$. Par contre :
$$D_n(\mathbb{K}) := \{\mathrm{diag}(\lambda_1, \dots, \lambda_n) \,|\, \lambda_1, \dots, \lambda_n \in \mathbb{K}^*\} \ntriangleleft GL_n(\mathbb{K})$$
En effet, une matrice diagonalisable n'est pas nécessairement diagonale (on a un résultat similaire pour les matrices triangulaires).

Proposition 1.2.2
Soit G un groupe et soit $N \lhd G$.
Alors :

(i) si $x, y \in G$, on a :
$$xy^{-1} \in N \Leftrightarrow x^{-1}y \in N$$

1. la relation "$xy^{-1} \in N$" est une relation d'équivalence sur G compatible avec sa loi. Pour cette relation, on a $\forall x \in G$:
$$\overline{x} = xN = Nx$$

Démonstration :

(i) Soient $x, y \in G$. Alors :
$$\begin{aligned} xy^{-1} \in N &\Leftrightarrow x \in Ny \\ &\Leftrightarrow x \in yN \text{ car } yNy^{-1} = N \\ &\Leftrightarrow y^{-1}x \in N \\ &\Leftrightarrow x^{-1}y = (y^{-1}x)^{-1} \in N \end{aligned}$$

(ii) Contentons–nous de vérifier la compatibilité. Si $x, y, x', y' \in G$, avec $x \sim x'$ et $y \sim y'$; i.e $\exists \alpha, \beta \in N$, $xx'^{-1} = \alpha$, $yy'^{-1} = \beta$; alors $x = \alpha x'$ et $y = \beta y'$ donc $xy(x'y')^{-1} = \alpha x' \beta x'^{-1}$, ce qui permet de conclure.

Définition 1.2.4 (Groupe quotient)
Soit G un groupe et soit $N \lhd G$.
Alors le quotient de G par la relation d'équivalence modulo N (i.e "$xy^{-1} \in N$") muni de la loi quotient est un groupe, appelé groupe quotient de G par N.

✍ On note ce groupe G/N.

On a alors un morphisme $\pi : G \to G/N$ surjectif et de noyau N. On en déduit que tout sous–groupe distingué est le noyau d'un morphisme de groupes, ce qui nous fournit une réciproque à (1.1).

2. Le lecteur taquin remarquera que cela ne veut rien dire : soit les trois le sont, soit aucune ne l'est !

Remarque : Si H est un sous–groupe d'un groupe G, alors "$x^{-1}y \in H$" (resp. "$xy^{-1} \in H$") est une relation d'équivalence sur G vérifiant que pour $x \in G$, $\overline{x} = xH$ (resp. Hx). Si $H \ntriangleleft G$, ces deux relations sont différentes et non compatibles avec la loi de groupe : elles engendrent donc deux ensembles quotients, notés G/H (pour les classes "xH") et $H\backslash G$ (pour les classes "Hx").

Proposition 1.2.3 (Propriété universelle du groupe quotient)
Soient G et Γ deux groupes.
Soit $N \triangleleft G$ et $\varphi : G \to \Gamma$ un morphisme de groupes.
Alors, les trois conditions suivantes sont équivalentes :

(i) $\varphi(N) = \{e_\Gamma\}$ *;*

(ii) $N \subset \operatorname{Ker}\varphi$ *;*

(iii) Il existe un morphisme $\overline{\varphi} : G/N \to \Gamma$ tel que :

$$\varphi = \overline{\varphi} \circ \pi$$

Où π est la projection canonique sur G/N.

Dans ce cas, le morphisme $\overline{\varphi}$ est unique et vérifie :

$$\operatorname{Im}\overline{\varphi} = \operatorname{Im}\varphi \quad \textit{et} \quad \operatorname{Ker}\overline{\varphi} = \pi\,(\operatorname{Ker}\varphi) = \operatorname{Ker}\varphi/N$$

✌ Une fois n'est pas coutume, cette propriété peut–être résumée par un joli diagramme commutatif :

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft" near start] & \Gamma \\
G/N \arrow[ur, "\exists!\overline{\varphi}"'] &
\end{tikzcd}$$

Démonstration : Seule l'implication $(ii) \Rightarrow (iii)$ mérite que l'on s'y attarde. Si l'on a $x, y \in G$ tels que $xy^{-1} \in N$ alors $xy^{-1} \in \operatorname{Ker}(\varphi)$, donc $\varphi(x) = \varphi(y)$ par propriété de morphisme. D'où l'existence de l'application $\overline{\varphi}$ d'après la proposition 1.1.3 appliquée à G, Γ et à l'égalité modulo N. Cette application est de plus un morphisme car si $\xi, \eta \in G/N$, on a par surjectivité de π qu'il existe $x, y \in G$ tels que $\xi = \pi(x)$ et $\eta = \pi(y)$, donc :

$$\begin{aligned}
\overline{\varphi}(\xi\eta) &= \overline{\varphi}(\pi(x)\pi(y)) \\
&= \overline{\varphi}(\pi(xy)) \\
&= \varphi(xy) \\
&= \varphi(x)\varphi(y) \\
&= \overline{\varphi}(\xi)\overline{\varphi}(\eta)
\end{aligned}$$

La fin de la démonstration est immédiate.

☞ Pour démontrer la proposition 1.2.3, on a seulement utilisé le fait que π est un morphisme surjectif de noyau N.

Corollaire 1.2.3.1
Soient G et H deux groupes et soit $f : G \to H$ un morphisme de groupes.
Alors :

$$G/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$$

Où le (honteux) symbole "$\cong$" dénote (tout aussi honteusement) l'existence d'un isomorphisme entre ces deux groupes.

Démonstration : On applique la proposition 1.2.3 à $N = \operatorname{Ker} f$ et $\varphi = f$. On obtient ainsi un morphisme $\overline{f} : x \mapsto f(x)$ de même image que f et dont le noyau est $\operatorname{Ker}(f)/\operatorname{Ker}(f) = \{e\}$, ce qui fait d'elle une (fort sympathique) injection. D'où le résultat.

Exemple : Soit $f : (\mathbb{C}, +) \to (\mathbb{C}^*, \times)$ définie par $f(z) = e^{2i\pi z}$. f est alors un morphisme de groupes surjectif de noyau $\mathbb{Z}$, donc on a que :

$$\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^*$$

La restriction de f à $\mathbb{R}$ nous livre de plus un isomorphisme entre $\mathbb{R}/\mathbb{Z}$ et $(\mathcal{U}, +)$, où $\mathcal{U}$ est le noyau du morphisme $(z \in \mathbb{C}^*) \mapsto (|z| \in \mathbb{R}_+^*)$.

Proposition 1.2.4 (Sous–groupes d'un groupe quotient)
Soit G un groupe et soit $N \lhd G$. On note π la projection canonique sur G/N.
On a alors des bijections naturelles, réciproque l'une de l'autre, entre l'ensemble E des sous–groupes de G contenant N et l'ensemble F des sous groupes de G/N. Ces bijections sont données par :

$$(H \in E) \mapsto (H/N = \pi(H) \in F) \quad et \quad (K \in F) \mapsto (\pi^{-1}(K) \in E)$$

De plus, si $H \in E$, on a que :

$$G/H \cong (G/N)/(H/N) \tag{1.2}$$

Démonstration : Démontrons (1.2). Pour ce faire, considérons le morphisme $\rho \circ \pi$, où $\rho : G/N \to (G/N)/(H/N)$ est la projection canonique. Ce morphisme est surjectif et son noyau est :

$$\mathrm{Ker}(\rho \circ \pi) = \pi^{-1} \mathrm{Ker}\, \rho = \pi^{-1}(H/N) = \pi^{-1}(\pi(H))$$

Or, comme π est surjective, $\pi^{-1}(\pi(H)) = H$, d'où le résultat par le corollaire 1.2.3.1.

1.3 Anneaux, idéaux et anneaux quotients

Définition 1.3.1 (Anneau unitaire)
Soit $\mathbb{A}$ un ensemble et soient $+$ et $\times$ deux LCI sur $\mathbb{A}$.
Alors on dit que le triplet $(\mathbb{A}, +, \times)$ est un anneau (unitaire) si :

(i) $(\mathbb{A}, +)$ *est un groupe abélien (on note en général $0_{\mathbb{A}}$ — ou 0 — le neutre de ce groupe) ;*

(ii) $\times$ *est associative ;*

(iii) $\times$ *est distributive par rapport à $+$, i.e :*

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

(iv) $\mathbb{A}$ *contient un élément neutre pour $\times$, noté en général $1_{\mathbb{A}}$ (ou 1).*

Si de plus la loi $\times$ est commutative, on dit que $\mathbb{A}$ est commutatif[3].

Définition 1.3.2 (Sous–anneau)
Soit $(\mathbb{A}, +, \times)$ un anneau (unitaire[4]*) et soit $\mathbb{B} \subset \mathbb{A}$.*
Alors on dit que $\mathbb{B}$ est un sous–anneau de $\mathbb{A}$ si celui–ci induit sur $\mathbb{B}$ une structure d'anneau, i.e si :

(i) $1_{\mathbb{A}} \in \mathbb{B}$;

(ii) $\forall x, y \in \mathbb{B},\ x - y \in \mathbb{B}$;

(iii) $\forall x, y \in \mathbb{B},\ xy \in \mathbb{B}$.

Définition 1.3.3 (Morphisme d'anneaux)
Soient $\mathbb{A}$ et $\mathbb{B}$ deux anneaux.
On dit qu'une application $f : \mathbb{A} \to \mathbb{B}$ est un morphisme d'anneaux si elle vérifie que :

(i) *f est un morphisme* de groupes *de $(\mathbb{A}, +)$ dans $(\mathbb{B}, +)$;*

(ii) $f(1_{\mathbb{A}}) = 1_{\mathbb{B}}$;

(iii) $\forall x, y \in \mathbb{A},\ f(xy) = f(x)f(y)$.

On appelle noyau et image du morphisme f son noyau et son image en tant que morphisme de groupes.

3. On ne parle pas d'"anneau abélien". Je ne suis pas sur qu'il y ait une raison profonde. C'est un peu comme manger la bouche ouverte : cela ne se fait pas.
4. C'est la dernière fois que je l'écrit. Désormais, ils le seront tous.

Proposition 1.3.1
Soit $\mathbb{A}$ un anneau.
Alors :

(i) il existe un unique morphisme (d'anneaux) de $\mathbb{A}$ dans l'anneau trivial $\{0\}$;

(ii) il existe un unique morphisme φ de $\mathbb{Z}$ dans $\mathbb{A}$ défini par :

$$\forall n \in \mathbb{Z},\ \varphi(n) := n1_{\mathbb{A}} = \underbrace{1_{\mathbb{A}} + \ldots + 1_{\mathbb{A}}}_{n \text{ fois}}$$

Proposition 1.3.2
Soient $\mathbb{A}$ et $\mathbb{B}$ deux anneaux.
Soit $f : \mathbb{A} \to \mathbb{B}$ un morphisme (d'anneaux).
Alors :

(i) pour tout sous–anneau $\mathbb{B}'$ de $\mathbb{B}$, $f^{-1}(\mathbb{B}')$ est un sous–anneau de $\mathbb{A}$;

(ii) pour tout sous–anneau $\mathbb{A}'$ de $\mathbb{A}$, $f(\mathbb{A}')$ est un sous–anneau de $\mathbb{B}$.

Proposition 1.3.3 (Intersection de sous–anneaux)
Toute intersection de sous–anneaux d'un même anneau en est un sous anneau.

✌ Par convention, une intersection d'une famille de sous–anneaux indexée par l'ensemble vide est égale à l'anneau tout entier.

Proposition 1.3.4 (Sous–anneau engendré par une partie)
Soit $\mathbb{A}$ un anneau et soit $S \subset \mathbb{A}$.
Alors l'intersection de tous les sous–anneaux de $\mathbb{A}$ contenant S est le plus petit sous–anneau de $\mathbb{A}$ contenant S. On l'appelle sous–anneau engendré par S.

✌ Une description "par le bas" de cet ensemble nous apprend qu'il est égal au groupe engendré par S dans $(\mathbb{A}, +)$.

Définition 1.3.4 (Élément régulier)
Soit $\mathbb{A}$ un anneau.
Alors on dit qu'un élément $\alpha \in \mathbb{A}$ est régulier[5] à gauche si l'une[6] des conditions équivalentes suivantes est vérifiée :

(i) l'application $(x \in \mathbb{A}) \mapsto \alpha x$ est injective ;

(ii) $\forall x, y \in \mathbb{A}$, si $\alpha x = \alpha y$ alors $x = y$;

(iii) $\forall x \in \mathbb{A}$, si $\alpha x = 0$ alors $x = 0$.

On définit symétriquement la notion d'élément régulier à gauche.

Définition 1.3.5 (Élément inversible)
Soit $\mathbb{A}$ un anneau.
Alors on dit qu'un élément $\alpha \in \mathbb{A}$ est inversible à gauche (resp. à droite) si il existe $\beta \in \mathbb{A}$ tel que $\beta\alpha = 1_{\mathbb{A}}$ (resp. $\alpha\beta = 1_{\mathbb{A}}$). S'il est inversible à droite et *à gauche, on dira simplement qu'il est inversible.*

✘ Dire qu'un élément est inversible à gauche signifie qu'il faut le multiplier à gauche par son inverse, faisant de lui l'élément de droite du produit, tandis que l'on ne peut simplifier par un régulier à gauche que s'il se trouve à gauche d'un produit.

Exercice :

1. Démontrer que si un élément est inversible ses inverses à droite et à gauche sont égaux.
2. Démontrer qu'un inversible à gauche est régulier à gauche.

Définition 1.3.6 (Groupe des inversibles)
L'ensemble des éléments inversibles d'un anneau $\mathbb{A}$ est un groupe pour la multiplication.

✍ On le note $\mathbb{A}^{\times}$.

5. On dit aussi "non–diviseur de zéro", mais cela revient à considérer que le verre est à moitié vide, non ?
6. Oui, je sais ...

Exemples :

1. $\mathbb{Z}^\times = \{-1, 1\}$;
2. $\mathbb{R}^\times = \mathbb{R}[X]^\times = \mathbb{R}^*$;
3. $\mathcal{M}_n(\mathbb{R})^\times = GL_n(\mathbb{R})$.

✌ Et l'anneau trivial me direz vous... Eh bien on a que :

$$\{0\}^\times = \{0\}$$

Définition 1.3.7 (Anneau intègre)
Soit $\mathbb{A}$ un anneau.
Alors on dit que $\mathbb{A}$ est intègre si :

(i) *$\mathbb{A}$ est commutatif;*
(ii) *$\mathbb{A}$ est non trivial;*
(iii) *tout élément non nul de $\mathbb{A}$ est régulier.*

Définition 1.3.8 (Corps)
Soit $\mathbb{A}$ un anneau.
Alors on dit que $\mathbb{A}$ est un corps si :

(i) *$\mathbb{A}$ est commutatif;*
(ii) *$\mathbb{A}$ est non trivial;*
(iii) *tout élément non nul de $\mathbb{A}$ est inversible.*

☞ On peut résumer (*ii*) et (*iii*) par : $\mathbb{A}^\times = \mathbb{A} \setminus \{0\}$.

✌ Si $\mathbb{A}$ ne vérifie que (*ii*) et (*iii*), on dit que c'est un anneau à division.

Exemples / exercices en vrac :

1. $\mathbb{Z}$ et $\mathbb{R}[X]$ sont intègres mais ne sont pas des corps ;
2. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{R}(X)$ sont des corps ;
3. si $n \geq 1$, alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier ;
4. un anneau intègre fini est un corps ;
5. tout sous–anneau d'un anneau intègre est intègre ;
6. $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$ n'est pas intègre ;
7. si $\mathcal{U}$ est un ouvert connexe de $\mathbb{C}$, alors $\mathcal{H}(\mathcal{U})$ est un anneau intègre ;
8. le produit de deux anneaux non nuls n'est *jamais* intègre. Non, vraiment.

Définition 1.3.9 (Idéal)
Soit $\mathbb{A}$ un anneau et $\mathcal{I} \subset \mathbb{A}$.
Alors on dit que $\mathcal{I}$ est un idéal à gauche de $\mathbb{A}$ si :

(i) *$(\mathcal{I}, +)$ est un sous–groupe de $(\mathbb{A}, +)$;*
(ii) *$\forall a \in \mathbb{A}, \forall x \in \mathcal{I}$, $ax \in \mathcal{I}$.*

On définit symétriquement la notion d'idéal à droite. Si $\mathcal{I}$ est un idéal à gauche et *à droite, on parle d'idéal bilatère.*

Exercices :

1. $\{0\}$ et $\mathbb{A}$ sont des idéaux bilatères de tout anneau $\mathbb{A}$, appelés idéaux triviaux.
2. Si un idéal contient un élément inversible, il est égal à l'anneau tout entier.
3. Le noyau d'un morphisme d'anneaux est un idéal bilatère de l'ensemble de départ.
4. Une intersection d'idéaux reste un idéal.
5. Soit $\mathbb{K}$ un corps, E un $\mathbb{K}$–e.v et F un s–e.v de E. Alors :
   (a) $\{u \in \mathcal{L}(E) \,|\, u_{|_F} = 0\}$ est un idéal à gauche de $\mathcal{L}(E)$;
   (b) $\{u \in \mathcal{L}(E) \,|\, \mathrm{Im}(u) \subset F\}$ est un idéal à droite de $\mathcal{L}(E)$

Si E est de dimension finie, ce sont les seuls idéaux non bilatères de $\mathcal{L}(E)$. De plus, les seuls idéaux bilatères de $\mathcal{L}(E)$ sont $\mathcal{L}(E)$ et $\{0\}$

Proposition 1.3.5 (Idéaux d'un anneau à division)
Soit $\mathbb{A}$ un anneau à division.
Alors ses seuls idéaux sont $\{0\}$ et $\mathbb{A}$.

Proposition 1.3.6
Soit $\mathbb{A}$ un anneau commutatif non trivial. Alors :

$$\mathbb{A} \textit{ est un corps} \Leftrightarrow \{0\} \textit{ et} \mathbb{A} \textit{ sont les seuls idéaux de } \mathbb{A}$$

Proposition 1.3.7 (Idéal engendré par un élément, par une partie)
Soit $\mathbb{A}$ un anneau.

1. *Soit $\alpha \in \mathbb{A}$. Alors $\alpha\mathbb{A}$ (resp. $\mathbb{A}\alpha$) est le plus petit idéal à droite (resp. à gauche) contenant α. On l'appelle idéal à droite (resp. à gauche) engendré par α. Si $\mathbb{A}$ est commutatif, ces deux idéaux coincident, et on note l'idéal engendré par α (α).*
2. *Soit $S \subset \mathbb{A}$. Alors le plus petit idéal à gauche contenant S est l'ensemble :*

$$\left\{ \sum_{i=1}^{n} a_i s_i \,|\, n \geq 1, (a_i)_i \in \mathbb{A}^n, (s_i)_i \in S^n \right\}$$

On l'appelle idéal à gauche engendré par S. On définit de même l'idéal à droite engendré par S.

Remarques :

1. L'idéal à droite (resp. à gauche) engendré par un élément (ou une partie) est toujours égal à l'intersection des idéaux à droite (resp. à gauche) contenant cet élément (ou partie).
2. Un idéal engendré par un seul élément est dit principal.

Proposition 1.3.8 (Anneau quotient)
Soit $\mathbb{A}$ un anneau et soit $\sim$ une relation d'équivalence sur $\mathbb{A}$.
On a alors équivalence entre les propriétés suivantes :

(i) *$\sim$ est compatible avec $+$ et $\times$;*
(ii) *il existe un anneau $\mathbb{B}$ et un morphisme (d'anneaux) $\varphi : \mathbb{A} \to \mathbb{B}$ tel que $\sim$ soit la relation associée à φ ;*
(iii) *$\sim$ est de la forme "$x - y \in \mathcal{I}$", où $\mathcal{I}$ est un idéal bilatère de $\mathbb{A}$ qui est alors nécessairement égal à la classe de 0 pour $\sim$.*

Dans ce cas, on peut munir $\mathbb{A}/\sim$ d'une structure d'anneau induite par les lois quotients. Ce quotient se note $\mathbb{A}/\mathcal{I}$ est appelé anneau quotient de $\mathbb{A}$ par $\mathcal{I}$. Notons que le groupe $(\mathbb{A}/\mathcal{I}, +)$ est isomorphe au groupe quotient de $(\mathbb{A}, +)$ par $(\mathcal{I}, +)$.

☞ On obtient alors un morphisme naturel d'anneaux $\pi : \mathbb{A} \to \mathbb{A}/\mathcal{I}$, surjectif et de noyau $\mathcal{I}$.

DÉMONSTRATION :

$(i) \Rightarrow (ii)$ Il suffit de poser $\mathbb{B} = \mathbb{A}/\sim$ et d'appliquer la proposition 1.1.4.

$(ii) \Rightarrow (iii)$ Comme φ est un morphisme de groupes, la relation qui lui est associée est "$x - y \in \operatorname{Ker}\varphi$, ce qui permet de conclure (*exercice :* vérifier que $\operatorname{Ker}\varphi$ est un idéal bilatère de $\mathbb{A}$).

$(iii) \Rightarrow (i)$ Trivial.

Proposition 1.3.9
Soient $\mathbb{A}$ et $\mathbb{B}$ deux anneaux.
Soit $\mathcal{I}$ un idéal bilatère de $\mathbb{A}$ de projection associée $\pi : \mathbb{A} \to \mathbb{A}/\mathcal{I}$.
Soit $f : \mathbb{A} \to \mathbb{B}$ un morphisme d'anneaux tel que :

$$f(\mathcal{I}) = \{0\} \quad i.e \quad \mathcal{I} \subset \operatorname{Ker}(f)$$

Alors il existe un unique morphisme $\overline{f} : \mathbb{A}/\mathcal{I} \to \mathbb{B}$ tel que :

$$f = \overline{f} \circ \pi$$

De plus,

$$\operatorname{Im}(\overline{f}) = \operatorname{Im}(f) \quad et \quad \operatorname{Ker}(\overline{f}) = \pi\left(\operatorname{Ker}(f)\right) = \operatorname{Ker}(f)/\mathcal{I}$$

✌ Un petit diagramme commutatif pour la route ...

$$\begin{tikzcd} \mathbb{A} \arrow[r, "f"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{B} \\ \mathbb{A}/\mathcal{I} \arrow[ur, "\exists!\overline{f}"'] & \end{tikzcd}$$

Démonstration : Il suffit d'appliquer la proposition 1.2.3 à f vu comme morphismes de groupes.

Proposition 1.3.10
Soient $\mathbb{A}$ et $\mathbb{B}$ deux anneaux.
Soit $f : \mathbb{A} \to \mathbb{B}$ un morphisme d'anneaux.
Alors :

$$\mathbb{A}/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$$

Démonstration : L'isomorphisme nous est livré par l'application $\widehat{x} \mapsto f(x)$.

Exemples :

1. Soit $f : (P \in \mathbb{R}[X]) \mapsto (P(i) \in \mathbb{C})$. Alors f est un morphisme surjectif de noyau (X^2+1). Ainsi, on a :
$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$$
Ce qui représente en fait la définition du corps des complexes.
2. *Construction de $\mathbb{R}$ via les suites de Cauchy rationnelles.* Soit $\mathbb{A}$ l'anneau des suites de Cauchy de rationnels. On a alors un morphisme d'anneau :
$$\begin{aligned} f : \mathbb{A} &\to \mathbb{R} \\ u &\mapsto \lim_{n\to\infty} u_n \end{aligned}$$
Le noyau de f est l'ensemble J de suites de rationnels convergeant vers 0, ce qui nous livre un isomorphisme de $\mathbb{R}$ dans $\mathbb{A}/J$, qui représente en fait la définition du corps des réels.

Proposition 1.3.11 (Idéal premier)
Soit $\mathbb{A}$ un anneau commutatif.
Soit $\mathcal{I}$ un idéal de $\mathbb{A}$.
Alors :

$$\mathbb{A}/\mathcal{I} \text{ est intègre} \iff \mathcal{I} \text{ est premier.}$$

Où un idéal $\mathcal{I}$ est dit premier si il vérifie :

(i) $\mathcal{I} \neq \mathbb{A}$, i.e si $1 \notin \mathbb{A}$;

(ii) $\forall a, b \in \mathbb{A}$, si $ab \in \mathcal{I}$, alors $a \in \mathcal{I}$ ou $b \in \mathcal{I}$.

Exemple : Un idéal $n\mathbb{Z}$ de $\mathbb{Z}$ est premier si et seulement si $n = 0$ ou n est premier.

Proposition 1.3.12 (Idéal maximal)
Soit $\mathbb{A}$ un anneau commutatif.
Soit $\mathcal{I}$ un idéal de $\mathbb{A}$.
Alors :

$$\mathbb{A}/\mathcal{I} \text{ est un corps} \iff \mathcal{I} \text{ est maximal.}$$

Où un idéal $\mathcal{I}$ est dit maximal si il vérifie :

(i) $\mathcal{I} \neq \mathbb{A}$, i.e si $1 \notin \mathbb{A}$;

(ii) le seuls idéaux de $\mathbb{A}$ contenant $\mathcal{I}$ sont $\mathbb{A}$ et $\mathcal{I}$.

Proposition 1.3.13 (Idéaux et sous–anneaux d'un anneau quotient)
Soit $\mathbb{A}$ un anneau.
Soit J un idéal à gauche de $\mathbb{A}$, de projection canonique associée $\pi : \mathbb{A} \to \mathbb{A}/J$.
On a alors des bijections naturelles, réciproque l'une de l'autre, entre l'ensemble E des idéaux à gauche de $\mathbb{A}$ contenant J et l'ensemble F des idéaux à gauche de $\mathbb{A}/J$. Ces bijections respectent les inclusions et les intersections et sont données par :

$$(I \in E) \mapsto (I/J = \pi(I) \in F) \quad \textit{et} \quad (K \in F) \mapsto (\pi^{-1}(K) \in E)$$

On dispose du même type de résultat si J est un idéal à droite ou bilatère ou un sous–anneau de $\mathbb{A}$.

Exemple : Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$, où $d|n$. Ainsi, on les idéaux de $\mathbb{Z}/6\mathbb{Z}$ peuvent être représentés par le schéma suivant (les flèches représentent les inclusions) :

$$\begin{tikzcd}
& \mathbb{Z}/6\mathbb{Z} & \\
2\mathbb{Z}/6\mathbb{Z} \arrow[ur] & & 3\mathbb{Z}/6\mathbb{Z} \arrow[ul] \\
& \{0\} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Remarque : Sous les hypothèses de la proposition 1.3.13, si $\mathcal{I}$ est un idéal quelconque de $\mathbb{A}$, $\pi(\mathcal{I})$ est un idéal de $\mathbb{A}/J$ correspondant (au sens de la proposition) à $\pi^{-1}(\pi(\mathcal{I})) = I + J$.

1.4 Lemme de Zorn

Définition 1.4.1 (Élément maximal, plus grand élément)
Soit $(E, \leq)$ un ensemble ordonné.
Soit $m \in E$.
Alors :

(i) on dit que m est un élément maximal de E si :

$$\nexists x \in E \setminus \{m\},\ m \leq x$$

1. on dit m est un plus grand élément de E si :

$$\forall x \in E,\ x \leq m$$

Définition 1.4.2 (Ensemble inductif)
Soit $(E, \leq)$ un ensemble ordonné.
Alors on dit que E est inductif si toute partie totalement ordonnée (on dit aussi chaîne) de E est majorée dans E.

Remarques :

1. Un ensemble inductif est non vide. En effet, $\emptyset$ est une chaîne de E donc y est majorée.
2. Si E est totalement ordoné, l'inductivité est équivalente à l'existence d'un plus grand élément.

Lemme 1.4.1 (Zorn)
Tout ensemble inductif admet un élément maximal.

Le lemme de Zorn est équivalent à l'axiome du choix, que nous utiliserons dans toute la suite de ce cours.

Axiome 1 (Axiome du choix)
Soit I un ensemble et soit $(E_i)_{i\in I}$ une famille d'ensembles tous non vides.
Alors :

$$\prod_{i\in I} E_i \neq \emptyset$$

Proposition 1.4.1
Tout anneau commutatif non trivial admet un idéal maximal.

Démonstration : Soit $\mathbb{A}$ un anneau commutatif non trivial. Soit E l'ensemble des idéaux stricts de $\mathbb{A}$, i.e différents de $\mathbb{A}$ tout entier, ordonné par l'inclusion. Alors E est un ensemble inductif. En effet, si C est une chaîne de E, alors :

Cas 1 : $C = \emptyset$. Alors $\{0\}$ majore C dans E.

Cas 2 : $C \neq \emptyset$. Alors, si on pose :

$$J := \bigcup_{\mathcal{I}\in C} \mathcal{I}$$

J est un idéal de $\mathbb{A}$ car C est totalement ordonnée pour l'inclusion, et est strict $\forall \mathcal{I} \in C$, $1 \notin \mathcal{I}$ (car $\mathbb{A} \neq \{0\}$) donc $1 \notin J$.

Corollaire 1.4.1.1
Soit $\mathbb{A}$ un anneau commutatif non trivial.
Alors il existe un corps $\mathbb{K}$ tel qu'il existe un morphisme d'anneau surjectif de $\mathbb{A}$ dans $\mathbb{K}$.

1.5 Modules

Dans tout ce paragraphe, on se donne un anneau $(\mathbb{A}, +, \times)$.

Définition 1.5.1 (Module)
Un $\mathbb{A}$–module à gauche (resp. à droite) est un triplet $(E, +, .)$ où :

(i) $(E, +)$ *est un groupe abélien*[7] *;*

(ii) . *est une loi de composition externe (LCE) à gauche (resp. à droite), i.e une application de la forme* $((\lambda, x) \in \mathbb{A} \times E) \mapsto (\lambda.x \in E)$ *(resp.* $x.\lambda$*) vérifiant :*

- *(a)* $\forall x, y \in E, \forall \lambda \in \mathbb{A},\ \lambda.(x + y) = \lambda.x + \lambda.y$ *(resp.* $(x + y).\lambda = x.\lambda + y.\lambda$*) ;*
- *(b)* $\forall x \in E, \forall \lambda, \mu \in \mathbb{A},\ (\lambda + \mu).x = \lambda.x + \mu.x$ *(resp.* $x.(\lambda + \mu) = x.\lambda + x.\mu$*) ;*
- *(c)* $\forall x \in E,\ 1_{\mathbb{A}}.x = x$ *(resp.* $x.1_{\mathbb{A}} = x$*) ;*
- *(d)* $\forall x \in E, \forall \lambda, \mu \in \mathbb{A},\ (\lambda \times \mu).x = \lambda.(\mu.x)$ *(resp.* $x.(\lambda \times \mu) = (x.\lambda).\mu$*) ;*

☞ On peut également définir un $\mathbb{A}$–module à gauche comme un groupe abélien $(E, +)$ muni d'un morphisme d'anneaux $\varphi : \mathbb{A} \to (\mathrm{End}(E), +, \circ)$.

Pour démontrer que ces deux définitions sont équivalentes, il nous suffit dans un sens de poser $\varphi(\lambda) := x \mapsto \lambda.x$ et dans l'autre de poser $\lambda.x := \varphi(\lambda)(x)$ et de vérifier[8] que cela convient.

De façon symétrique, un $\mathbb{A}$–module à droite peut être vu comme un groupe abélien $(E, +)$ muni d'un antimorphisme[9] d'anneaux $\psi : \mathbb{A} \to (\mathrm{End}(E), +, \circ)$.

Remarques :

1. $\mathbb{A}$ et $\{0\}$ sont des $\mathbb{A}$–modules à droite et à gauche.
2. Tout groupe abélien $(E, +)$ a une unique (pour une loi + donnée) structure de $\mathbb{Z}$–module. Ainsi, il y a correspondance "bijective" entre groupes abéliens et $\mathbb{Z}$–modules.
3. Un module sur un anneau à division est appelé *espace vectoriel*.

Définition 1.5.2 (Sous–module)
Soit E un $\mathbb{A}$–module à gauche (resp. à droite).
Soit $F \subset E$.
Alors on dit que F est un sous–module de E si :

(i) $F \neq \emptyset$ *;*

(ii) $\forall x, y \in E, \forall \lambda \in \mathbb{A},\ \lambda x + y \in F$ *(resp.* $x\lambda + y \in F$*).*

7. "+" n'est en général pas l'addition sur $\mathbb{A}$ (que l'on note pourtant de la même façon) !
8. Ce qui est assez long ...
9. Ce qui signifie que $\psi(\lambda \times \mu) = \psi(\mu) \circ \psi(\lambda)$.

Remarques :

1. E et $\{0\}$ sont des sous–modules de E.
2. Une intersection de sous–modules est un sous–module.

Définition 1.5.3 (Application linéaire)
Soient E et F deux $\mathbb{A}$–modules.
Une application $\varphi : E \to F$ est dite $\mathbb{A}$–linéaire si :

(i) φ *est un morphisme de groupes de* $(E,+)$ *dans* $(F,+)$ *;*

(ii) $\forall x \in E, \forall \lambda \in \mathbb{A},\ \varphi(\lambda x) = \lambda \varphi(x)$.

✍ On note $\mathrm{Hom}_{\mathbb{A}}(E,F)$ l'ensemble des applications $\mathbb{A}$–linéaires de E dans F.

Proposition 1.5.1
Soient E et F deux $\mathbb{A}$–modules.
Alors :

(i) $(\mathrm{Hom}_{\mathbb{A}}(E,F),+)$ *est un groupe abélien ;*

(ii) $(\mathrm{Hom}_{\mathbb{A}}(E,F),+)$ *est un* $\mathbb{A}$*–module si* $\mathbb{A}$ *est commutatif*

✗ $(\mathrm{Hom}_{\mathbb{A}}(E,F),+)$ n'est **PAS** en général un $\mathbb{A}$–module !

Proposition 1.5.2
Soient E et F deux $\mathbb{A}$–modules.
Soit $f \in \mathrm{Hom}_{\mathbb{A}}(E,F)$.
Alors :

(i) $\mathrm{Ker}(f)$ *est un sous–module de* E *;*

(ii) $\mathrm{Im}(f)$ *est un sous–module de* F *;*

(iii) si F' *est un sous–module de* F*, alors* $f^{-1}(F')$ *est un sous–module de* E *;*

(iv) si E' *est un sous–module de* E*, alors* $f(E')$ *est un sous–module de* F*.*

Proposition 1.5.3 (Quotient de modules)
Soit E un $\mathbb{A}$–module à gauche.
Soit F un sous–module de E.
Alors il existe une unique structure de $\mathbb{A}$–module sur le quotient E/F telle que la projection canonique $\pi : E \to E/F$ soit $\mathbb{A}$–linéaire.

Proposition 1.5.4 (Propriété universelle du module quotient)
Soient E et F deux $\mathbb{A}$–modules.
Soit H un sous–module de E.
Soit $\varphi \in \mathrm{Hom}_{\mathbb{A}}(E,F)$. On note $\pi : E \to E/H$ la projection canonique.
On a alors équivalence entre les propriétés suivantes :

(i) $H \subset \mathrm{Ker}(\varphi)$ *;*

(ii) $\exists! \overline{\varphi} \in \mathrm{Hom}_{\mathbb{A}}(E/H,F)$ *tel que :*

$$\varphi = \overline{\varphi} \circ \pi$$

✌ Résumons cet propriété par un nouveau diagramme commutatif[10] :

$$\begin{tikzcd}
E \arrow[r, "\varphi"] \arrow[d, "\pi"'] \arrow[dr, phantom, "\circlearrowleft"] & F \\
E/H \arrow[ur, "\exists!\overline{\varphi}"'] &
\end{tikzcd}$$

10. Avouez que cela vous manquait ...

Reformulation de la proposition 1.5.4 :
Soit :

$$\begin{aligned}\psi \ : \ \mathrm{Hom}_{\mathbb{A}}(E/H, F) &\to \mathrm{Hom}_{\mathbb{A}}(E, F)\\ \overline{\varphi} &\mapsto \overline{\varphi} \circ \pi\end{aligned}$$

Alors ψ induit un isomorphisme de groupes de $\mathrm{Hom}_{\mathbb{A}}(E/H, F)$ sur le sous–groupe de $\mathrm{Hom}_{\mathbb{A}}(E, F)$ formé des morphismes nuls sur H.

Corollaire 1.5.4.1
Soient E et F deux $\mathbb{A}$–modules.
Soit $\varphi \in \mathrm{Hom}_{\mathbb{A}}(E, F)$.
Alors :

$$E/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$$

✍ On rappelle que le symbole "$\cong$" dénote un isomorphisme *pour les structures concernées.* Ici, on parle donc d'isomorphisme $\mathbb{A}$–linéaire.

Proposition 1.5.5 (Sous–modules d'un quotient)
Soient E un $\mathbb{A}$–module.
Soit H un sous–module de E de projection canonique associée π.
On a alors des bijections naturelles, réciproque l'une de l'autre, entre l'ensemble U des sous modules de E contenant H et l'ensemble V des sous–modules de E/H. Ces bijections données par :

$$(F \in V) \mapsto (F/H = \pi(F) \in V) \quad et \quad (K \in V) \mapsto (\pi^{-1}(K) \in U)$$

Corollaire 1.5.5.1
Soient E un $\mathbb{A}$–module.
Soit H un sous–module de E et F un sous–module de E contenant H.
Alors :

$$E/F \cong (E/H)/(F/H)$$

Proposition 1.5.6 (Sous–module engendré par une partie)
Soit E un $\mathbb{A}$–module
Soit $S \subset E$.
Alors l'intersection de tous les sous–modules de E contenant S est le plus petit sous–module de E contenant S. On l'appelle sous–module engendré par S.
Il est de plus égal à :

$$\left\{ \sum_{i=1}^{n} \lambda_i s_i \;\middle|\; n \geq 1, (\lambda_i)_i \in \mathbb{A}^n, (s_i)_i \in S^n \right\}$$

En particulier, le sous–module engendré par la réunion de deux parties est égal à leur somme.

✍ On notera cet ensemble $\langle S \rangle_{\mathbb{A}}$, voire $\langle S \rangle$ si l'on a pas froid aux yeux.

Proposition 1.5.7 (Produit de modules)
Soit I un ensemble et soit $(E_i)_{i \in I}$ une famille de $\mathbb{A}$–modules à gauche.
Alors le produit (cartésien) E des E_i est muni d'une structure de $\mathbb{A}$–module à gauche via les opérations suivantes :

(i) $\forall x, y \in E$, $x + y := (x_i + y_i)_{i \in I}$;

(ii) $\forall x \in E, \forall \lambda \in \mathbb{A}$, $\lambda.x := (\lambda.x_i)_{i \in I}$.

On a le même résultat pour une famille de modules à droite.

☞On rappelle que l'on a :

$$\prod_{i \in I} E_i = \left\{ x : I \to \bigcup_{i \in I} E_i \;\middle|\; \forall i \in I,\ x(i) \in E_i \right\}$$

Proposition 1.5.8
Soit I un ensemble et soit $(E_i)_{i\in I}$ une famille de $\mathbb{A}$–modules à gauche.
Alors les projections p_j et les applications u_j définies ci–après sont $\mathbb{A}$–linéaires pour $j \in I$:

$$p_j \,:\, \prod_{i\in I} E_i \to E_j \qquad\qquad u_j \,:\, E_j \to \prod_{i\in I} E_i$$
$$(x_i)_{i\in I} \mapsto x_j \qquad\qquad x \mapsto (\delta_{i,j}.x)_{i\in I}$$

On a le même résultat pour une famille de modules à droite.

Définition 1.5.4 (Somme directe)
Soit I un ensemble et soit $(E_i)_{i\in I}$ une famille de $\mathbb{A}$–modules.
On appelle somme directe de $(E_i)_{i\in I}$ l'ensemble :

$$\bigoplus_{i\in I} E_i := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} E_i \,\middle|\, \mathrm{card}\left(\{i\in I \,|\, x_i \neq 0\}\right) < \infty \right\}$$

Proposition 1.5.9
Soit I un ensemble et soit $(E_i)_{i\in I}$ une famille de $\mathbb{A}$–modules.
Alors :

(i) $\bigoplus_{i\in I} E_i$ *est un sous–module de* $\prod_{i\in I} E_i$ *;*
(ii) $\bigoplus_{i\in I} E_i$ *est le sous–module engendré par* $\cup_{j\in I}\,\mathrm{Im}(u_j)$ *;*
(iii) Si les E_i sont tous égaux à un même module E, alors :

$$\prod_{i\in I} E_i = E^I$$

On a de plus que :

$$\bigoplus_{i\in I} E_i = E^{(I)} := \{f : I \to E \,|\, \mathrm{card}\left(\mathrm{supp}(f)\right) < \infty\}$$

(iv) Si $\mathrm{card}(I) < \infty$*, alors :*

$$\bigoplus_{i\in I} E_i = \prod_{i\in I} E_i = E^I$$

Exemple : Soit $\mathbb{A}$ un anneau. $\mathbb{A}^{\mathbb{N}}$ est alors l'ensemble des suites d'éléments de $\mathbb{A}$, tandis que $\mathbb{A}^{(\mathbb{N})}$ est l'ensemble des suites d'éléments de $\mathbb{A}$ nulles à partir d'un certain rang.

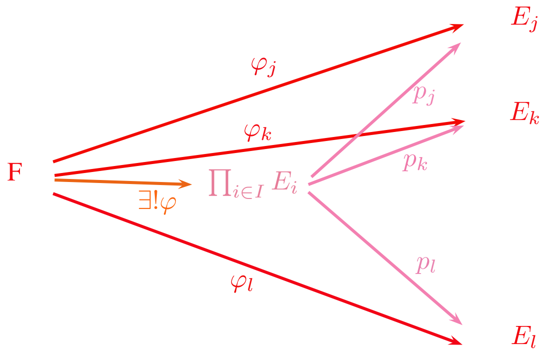
Proposition 1.5.10 (Propriété universelle du produit)
Soit I un ensemble et soit $(E_i)_{i\in I}$ une famille de $\mathbb{A}$–modules.
Soit F un $\mathbb{A}$–module.
Soit $(\varphi_i)_{i\in I}$ une famille d'applications telle que $\forall i \in I,\ \varphi_i \in \mathrm{Hom}_{\mathbb{A}}(F, E_i)$.
Alors :

$$\exists! \varphi \in \mathrm{Hom}_{\mathbb{A}}\left(F, \prod_{i\in I} E_i\right), \quad \forall_i \in I,\ p_i \circ \varphi = \varphi_i$$

De fait, on a :

$$\forall x \in F,\ \varphi(x) = (\varphi_i(x))_{i\in I}$$

✌ Diagrammons ...



Corollaire 1.5.10.1
Soit I un ensemble et soit $(E_i)_{i\in I}$ une famille de $\mathbb{A}$–modules.
Soit F un $\mathbb{A}$–module.
Alors :

$$\mathrm{Hom}_{\mathbb{A}}\left(F, \prod_{i\in I} E_i\right) \cong \prod_{i\in I} \mathrm{Hom}_{\mathbb{A}}(F, E_i)$$

Et ce via l'isomorphisme de groupes $\varphi \mapsto (p_i \circ \varphi)_{i\in I}$.

✘ Il n'existe pas de description simple de $\mathrm{Hom}_{\mathbb{A}}\left(\prod_{i\in I} E_i, F\right)$ si I est infini. Par exemple, $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^{\mathbb{N}}, \mathbb{R})$ contient des éléments non–descriptibles : en particulier, il existe une forme linéaire qui envoie chaque suite de la forme $(0, \ldots, 0, 1, 0\ldots)$ sur 1.

Proposition 1.5.11
Soit I un ensemble et soit $(E_i)_{i\in I}$ une famille de $\mathbb{A}$–modules.
Soit F un $\mathbb{A}$–module.
Soit $(\varphi_i)_{i\in I}$ une famille d'applications telle que $\forall i \in I$, $\varphi_i \in \mathrm{Hom}_{\mathbb{A}}(E_i, F)$.
Alors :

$$\exists! \varphi \in \mathrm{Hom}_{\mathbb{A}}\left(\bigoplus_{i\in I} E_i, F\right), \quad \forall_i \in I,\ \varphi \circ u_i = \varphi_i$$

De plus, φ est alors donnée par :

$$\forall (x_i)_{i\in I} \in \bigoplus_{i\in I} E_i, \quad \varphi\left((x_i)_{i\in I}\right) = \sum_{i\in I} \varphi_i(x_i)$$

Rappelons que cette somme est bien définie car la famille $(x_i)_{i\in I}$ est presque nulle.

Corollaire 1.5.11.1
Soit I un ensemble et soit $(E_i)_{i\in I}$ une famille de $\mathbb{A}$–modules.
Soit F un $\mathbb{A}$–module.
Alors :

$$\mathrm{Hom}_{\mathbb{A}}\left(\bigoplus_{i\in I} E_i, F\right) \cong \prod_{i\in I} \mathrm{Hom}_{\mathbb{A}}(E_i, F)$$

Et ce via l'isomorphisme de groupes $\varphi \mapsto (\varphi \circ u_i)_{i\in I}$.

Proposition 1.5.12
Soit E un $\mathbb{A}$–module.
Soient F et G deux sous–modules de E.
On a alors équivalence entre les propriétés suivantes :

(i) $((x, y) \in F \oplus G) \mapsto (x + y \in E)$ *est un isomorphisme ;*
(ii) $G \cap G = \{0\}$ *et* $F + G = E$ *;*
(iii) la composée suivante est un isomorphisme :

$$G \hookrightarrow E \xrightarrow{\pi} E/F \tag{1.3}$$

Où "$\hookrightarrow$" représente le morphisme d'inclusion.

Lorsque c'est le cas, on dit que F et G sont supplémentaires, ou que E est somme directe de F et G.

✘ Il n'y a pas nécessairement existence du supplémentaire. Par exemple, $2\mathbb{Z}$ n'en possède aucun dans $\mathbb{Z}$.

Corollaire 1.5.12.1
Soit E un $\mathbb{A}$–module.
Soient F et G deux sous–modules de E.
Alors si F et G sont supplémentaires, il existe une "projection[11]" sur G parallèlement à F, i.e une application $p_G : E \to G$ vérifiant :

11. À ne pas confondre avec les projecteurs, dont nous parlerons plus tard ...

(i) $\mathrm{Ker}(p_G) = F$;

(ii) $p_{G|_G} = \mathrm{id}_G$.

Cette application passe alors au quotient en une application de E/F dans G qui est l'inverse de l'isomorphisme (1.3).

☞ Notons que de fait p_G est $\mathbb{A}$–linéaire car elle l'est sur deux supplémentaires.

Dans ce cadre, on peut définir une application composée s comme suit :

$$\begin{aligned} s \,:\, E/F &\cong G \hookrightarrow E \\ z + F &\mapsto p_G(z) \mapsto p_G(z) \end{aligned}$$

s est alors une *section linéaire* de $\pi : E \to E/F$, i.e une application vérifiant :

$$\pi \circ s = \mathrm{id}_{E/F} \quad \text{i.e} \quad \forall \xi \in E/F,\ s(\xi) \in \overline{\xi}$$

Au final, on obtient que l'ensemble des supplémentaires de F dans E est équipotent à l'ensemble des sections linéaires de la projection canonique.

✘ l'application $f : \mathbb{Z}/2\mathbb{Z}$ définie par $f(\overline{0}) = 0$, $f(\overline{1}) = 1$ est une section *non $\mathbb{Z}$–linéaire* de la projection canonique.

Définition 1.5.5 (Projecteur)
Soit E un $\mathbb{A}$–module.
On appelle projecteur de E toute application $p \in \mathrm{Hom}_{\mathbb{A}}$ vérifiant :

$$p \circ p = p$$

Dans le cas où E est somme directe de deux sous–modules F et G, l'endomorphisme q_G suivant est un projecteur :

$$q_G \,:\, E \xrightarrow{p_G} G \hookrightarrow E$$

On obtient ainsi une bijection entre l'ensemble des décompositions de E en somme directe de deux sous–modules et les projecteurs de E, via le mécanisme suivant :

$$(F, G \subset E) \mapsto q_G \quad \text{et} \quad p \mapsto (\mathrm{Ker}(p), \mathrm{Im}(p))$$

1.6 Bases

Dans tout ce paragraphe, on se donne un anneau $(\mathbb{A}, +, \times)$.

Définition 1.6.1 (Module libre standard, base canonique)
Soit I un ensemble.
Alors :

(i) $\mathbb{A}^{(I)}$ *est appelé module libre standard de base I ;*

(ii) la famille $(e_i)_{i\in I} := ((\delta_{i,j})_{j\in I})_{i\in I}$ est appelée base canonique de $\mathbb{A}^{(I)}$.

Exemple : Si $I = \mathbb{N}$, on a :

$$\forall n \geq 0, \quad e_n = (0, 0, \ldots, 0, \underbrace{1_{\mathbb{A}}}_{n}, 0, \ldots)$$

Remarques :

1. Si $\mathbb{A}$ est non trivial, l'application $i \mapsto e_i$ est injective.
2. Si $x = (x_i)_i \in \mathbb{A}^{(I)}$, alors :
$$x = \sum_{i \in I} x_i e_i$$
Notons que cette somme est bien définie car finie.

Proposition 1.6.1 (Propriété universelle du module libre standard)
Soit E un $\mathbb{A}$–module et soit I un ensemble.
Soit $\underline{v} = (v_i)_{i \in I} \in E^I$.
Alors :
$$\exists ! \varphi_{\underline{v}} \in \mathrm{Hom}_{\mathbb{A}}\left(\mathbb{A}^{(I)}, E\right), \quad \forall i \in I,\ \varphi_{\underline{v}}(e_i) = v_i$$
Ce qui implique que pour tout $(\lambda_i)_i \in \mathbb{A}^{(I)}$, on a :
$$\varphi_{\underline{v}}\left((\lambda_i)_i\right) = \sum_{i \in I} \lambda_i v_i$$
De plus, :
$$\mathrm{Im}(\varphi_{\underline{v}}) = \langle v_i \mid i \in I \rangle \quad et \quad \mathrm{Ker}(\varphi_{\underline{v}}) = \left\{ (\lambda_i)_i \in \mathbb{A}^{(I)} \;\middle|\; \sum_{i \in I} \lambda_i v_i = 0 \right\}$$

Corollaire 1.6.1.1
Soit E un $\mathbb{A}$–module et soit I un ensemble.
Alors :
$$\mathrm{Hom}_{\mathbb{A}}\left(\mathbb{A}^{(I)}, E\right) \cong E^I$$
Via l'isomorphisme de groupes (et de $\mathbb{A}$ module si $\mathbb{A}$ est commutatif) $f \mapsto (f(e_i))_i$.

Définition 1.6.2 (Familles libre et génératrice, base, module libre)
Soit E un $\mathbb{A}$–module à gauche[12] *et soit I un ensemble.*
Soit $\underline{v} = (v_i)_{i \in I} \in E^I$, d'application associée $\varphi_{\underline{v}}$ (via la proposition 1.6.1).
Alors :

(i) on dit que $\underline{v}$ est une famille $\mathbb{A}$–libre dans E si l'une[13] *des conditions équivalentes suivantes est vérifiée :*
  (a) $\varphi_{\underline{v}}$ est injective ;
  (b) pour tout $(\lambda_i)_i \in \mathbb{A}^{(I)}$, on a l'implication :
$$\left(\sum_{i \in I} \lambda_i v_i = 0\right) \Rightarrow (\forall i \in I,\ \lambda_i = 0)$$

(ii) on dit que $\underline{v}$ est une famille $\mathbb{A}$–génératrice de E si l'une des conditions équivalentes suivantes est vérifiée :
  (a) $\varphi_{\underline{v}}$ est surjective ;
  (b) $\langle (v_i)_i \rangle = E$.

(iii) on dit que $\underline{v}$ est une $\mathbb{A}$–base de E si l'une des conditions équivalentes suivantes est vérifiée :
  1. $\varphi_{\underline{v}}$ est bijective ;
  2. $\underline{v}$ est libre et génératrice.

On dit que E est un $\mathbb{A}$–module libre si il admet une base.

Remarques :

1. E est un module libre $\Leftrightarrow E \cong \mathbb{A}^{(I)}$.
2. La base canonique $\underline{e}$ est une base du module libre standard et $\varphi_{\underline{e}} : \mathbb{A}^{(I)} \to \mathbb{A}^{(I)}$ est l'application identité.
3. Une famille est libre si et seulement chacune de ses sous–familles finies l'est.
4. Une famille libre est une base du sous–module qu'elle engendre (qui est donc libre).

12. Par soucis de concision, nous nous limiterons au cas des modules à gauche. C'est politique.
13. …et si vous arrêtiez de m'ennuyer avec ça, hein ?

Exemples :

1. $\mathbb{A}$ est un $\mathbb{A}$–module libre, de base $(1_{\mathbb{A}})$.
2. $()$ est libre, et $\langle () \rangle = \{0\}$.
3. $(X^n)_n$ est une $\mathbb{R}$–base de $\mathbb{R}[X]$ mais pas de $\mathbb{R}[[X]]$.
4. Dans le $\mathbb{Z}$–module $\mathbb{Z}^{\mathbb{N}}$, la famille des $e_n := (0, 0, \ldots, 0, \underbrace{1}_{n}, 0, \ldots)$, $n \geq 0$ est libre mais n'est pas une base. En effet, $\langle (e_n)_n \rangle = \mathbb{Z}^{(\mathbb{N})}$.
5. $\mathbb{Z}/2\mathbb{Z}$ n'est pas un $\mathbb{Z}$–module libre car il ne contient aucune famille $\mathbb{Z}$–libre non vide.
6. $\mathbb{Q}$ n'est pas un $\mathbb{Z}$–module libre car tout famille $\mathbb{Z}$–libre y a au plus un élément.
7. Tout $\{0\}$–module est libre, car toute famille d'éléments d'un tel module en forme une $\{0\}$–base.

Proposition 1.6.2 (Partie libre, partie génératrice)
Soit E un $\mathbb{A}$–module et soit I un ensemble.
Soit $\underline{v} = (v_i)_{i \in I} \in E^I$.
Alors :

(i) la propriété "$\underline{v}$ est génératrice" ne dépend que du sous–ensemble $\{v_i \,|\, i \in I\} \subset E$, ce qui n'est pas le cas de la propriété "$\underline{v}$ est libre". De fait, on dit que $S \subset E$ est génératrice si la famille $\{x \,|\, x \in S\}$ l'est[14] *;*

(ii) si $S \subset E$, on peut toujours l'indexer sans répétition, i.e la voir comme l'image d'une application injective *de I dans E. Si la famille ainsi construite est libre, on dit que S est une partie libre de E, ce qui signifie que S est libre si et seulement si pour tout $n \in \mathbb{N}$, pour toute famille $s_1 \ldots s_n$ d'éléments deux à deux distincts de S, pour tout $(\lambda_i)_i \in \mathbb{A}^n$ on a l'implication :*

$$\left(\sum_{i \in I} \lambda_i s_i = 0 \right) \Rightarrow (\forall i \in I,\ \lambda_i = 0)$$

Corollaire 1.6.2.1
Soit E un $\mathbb{A}$–module et soit I un ensemble.
Soit $\underline{v} = (v_i)_{i \in I} \in E^I$.
Alors :

$$\underline{v} \textit{ est libre} \quad \Leftrightarrow \quad \mathbb{A} = \{0\} \quad \textit{ou } \{v_i \,|\, i \in I\} \textit{ est une partie libre } \text{et } i \mapsto v_i \textit{ est injective}$$

Définition 1.6.3 (Partie libre maximale, génératrice minimale)
Soit E un $\mathbb{A}$–module.
Soit $S \subset E$.
Alors :

(i) on dit que S est libre maximale si :
   (a) S est libre ;
   (b) $\forall x \notin S$, $S \cup \{x\}$ n'est pas libre ;

(ii) on dit que S est génératrice minimale si :
   (a) S est génératrice ;
   (b) $\forall x \in S$, $S \setminus \{x\}$ n'est pas génératrice.

Exemple :

1. Les familles (1) et $(1, 1)$ engendrent le même espace mais seule (1) y est libre.
2. $\{2\}$ est libre maximale dans le $\mathbb{Z}$–module $\mathbb{Z}$ mais n'en forme pas une base.
3. $\{2, 3\}$ est génératrice minimale dans le $\mathbb{Z}$–module $\mathbb{Z}$ mais n'en forme pas une base.

Lemme 1.6.1
Soit E un $\mathbb{A}$–module.
Soient L une partie libre de E et $X \subset E$ telles que $L \subset X$.
Alors l'ensemble $\{L' \subset E \text{ libres} \,|\, L \subset L' \subset X\}$ est inductif.

14. Les notions de famille et de partie génératrice sont donc confondues : nous identifierons donc à l'avenir ces deux types d'objets.

Lemme 1.6.2
Soit $\mathbb{K}$ un anneau à division.
Soit E un $\mathbb{K}$–e.v (à gauche).
Soit L une partie libre de E et soit $x \in E$.
Si $x \notin \langle L \rangle$ alors $L \cup \{x\}$ est libre.

✗ Ce résultat est faux sur un anneau quelconque. Prendre par exemple le $\mathbb{Z}$–module $\mathbb{Z}$, la famille $L = \{2\}$ et $x = 1$.
DÉMONSTRATION : Si il existe une famille $\lambda_1 \dots \lambda_n$ de scalaires, $\lambda \in \mathbb{K}^*$ et $x_1 \dots x_n \in \langle L \rangle$ tels que :

$$\sum_{i=1}^{n} \lambda_i x_i + \lambda x = 0$$

Alors $x \in \langle x_1 \dots x_n \rangle \subset \langle L \rangle$ ce qui est absurde. D'où le résultat.

Théorème 1.6.3 (Base incomplète)
Soit $\mathbb{K}$ un anneau à division.
Soit E un $\mathbb{K}$–e.v.
Soient L une partie libre de E et G une partie génératrice de E telles que $L \subset G$.
Alors il existe une base B de E telle que :

$$L \subset B \subset G$$

DÉMONSTRATION : D'après le lemme de Zorn (lemme 1.4.1) et le lemme 1.6.1, il existe une partie libre maximale B contenant L et inclue dans G. Il ne nous reste plus qu'à démontrer que $\langle B \rangle = G$.

Soit $x \in G$. Alors, si $x \in B$, $x \in \langle B \rangle$. Sinon, $B \subsetneq B \cup \{x\} \subset G$. Or $B \cup \{x\}$ est non libre car B est maximale, donc le lemme 1.6.2 entraîne que $x \in \langle B \rangle$. D'où le résultat.

Corollaire 1.6.3.1
Soit $\mathbb{K}$ un anneau à division.
Alors tout $\mathbb{K}$–e.v admet une base.

DÉMONSTRATION : Prendre $L = \emptyset$ et $G = E$ dans le théorème 1.6.3.

Corollaire 1.6.3.2
Tout $\mathbb{A}$–module admet une partie libre maximale.

Corollaire 1.6.3.3
Sur un anneau à division, toute partie libre maximale est une base.

Proposition 1.6.4
Soient E, F deux $\mathbb{A}$–modules.
Soit $\varphi \in \mathrm{Hom}_{\mathbb{A}}(E, F)$ une application surjective.
Alors si F est un module libre, φ admet une section (i.e un inverse à droite) $\mathbb{A}$–linéaire, i.e :

$$\exists s \in \mathrm{Hom}_{\mathbb{A}}(F, E),\ \varphi \circ s = \mathrm{id}_F$$

DÉMONSTRATION : Soit $(e_i)_{i \in I}$ une base de F. Comme φ est surjective, l'axiome du choix entraîne qu'il existe une famille $(v_i)_i \in E^I$ telle que $\forall i \in I, \varphi(v_i) = e_i$.

D'après la proposition 1.6.1, il existe $s \in \mathrm{Hom}_{\mathbb{A}}(F, E)$ telle que $\forall i \in I, s(e_i) = v_i$, ce qui signifie que $\varphi \circ s$ et id_F coïncident sur une famille génératrice donc sont égales.

Corollaire 1.6.4.1
Soit E un $\mathbb{A}$–module.
Soit H un sous–module de E.
Si E/H est libre, alors H a un supplémentaire dans E et donc :

$$E \cong H \oplus E/H$$

Corollaire 1.6.4.2
Soit $\mathbb{K}$ un anneau à division. Alors :

(i) tout s–e.v d'un $\mathbb{K}$–e.v admet un supplémentaire ;

(ii) tout application $\mathbb{K}$–linéaire surjective admet une section ;

(iii) tout application $\mathbb{K}$–linéaire injective admet une rétraction (i.e un inverse à gauche) ;

✘ Gaffe aux hypothèses[15] !

1. La projection canonique $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ est surjective mais n'a pas de section $\mathbb{Z}$–linéaire.
2. $2\mathbb{Z} \hookrightarrow \mathbb{Z}$ est $\mathbb{Z}$–linéaire injective mais n'a pas de rétraction.
3. $2\mathbb{Z}$ n'a pas de supplémentaire dans $\mathbb{Z}$ donc $\mathbb{Z}$ n'est *pas* isomorphe à $2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

☞ Notons les deux choses suivantes ($\mathbb{A}$ est ici supposé non trivial) :

1. Si un $\mathbb{A}$–module admet une base infinie, toutes ses bases le sont.
2. Il existe un anneau $\mathbb{A}$ (non commutatif) tel que le $\mathbb{A}$–module $\mathbb{A}$ admette une base à deux éléments, en plus de sa base usuelle (à un élément !) $(1_{\mathbb{A}})$ ... Ce qui signifie que :
$$\mathbb{A} \cong \mathbb{A} \oplus \mathbb{A} \quad \text{(en tant que } \mathbb{A}\text{–module)}$$
Ce qui entraîne que :
$$\forall n \geq 1, \quad \mathbb{A} \cong \mathbb{A}^n$$

Proposition 1.6.5
Soit $\mathbb{K}$ un anneau à division.
Soit E un $\mathbb{K}$–e.v.
Soit $(e_1 \dots e_p)$ une famille libre (finie) dans E.
Soit $(v_1 \dots v_n)$ une famille génératrice (finie) de E.
Alors :
$$p \leq n$$

Démonstration : Démontrons par récurrence sur $p \geq 0$, à $n \geq 0$ fixé que :

$\forall p \geq 0$, $\forall E$ $\mathbb{K}$–e.v, $\forall (e_1 \dots e_p)$ famille libre dans E, $\forall (v_1 \dots v_n)$ famille génératrice de E, $p \geq n$

- Si $p = 0$, le résultat est trivial.
- Supposons la propriété validée au rang $p-1$ ($p \geq 0$). Soient E un $\mathbb{K}$–e.v, $(e_1 \dots e_p)$ une famille libre (finie) dans E et $(v_1 \dots v_n)$ une famille génératrice (finie) de E. Alors :
$$F := \langle e_1 \dots e_{p-1} \rangle \subsetneq E \text{ car } e_p \notin F$$
De facto, l'un des v_j, par exemple v_n, n'est pas dans F. Donc, d'après le lemme 1.6.2, la famille $(e_1, \dots, e_{p-1}, v_n)$ est libre. Par conséquent, la famille $(\overline{e_1}, \dots, \overline{e_{p-1}})$ est libre dans le quotient $E/\langle v_n \rangle$ et $(\overline{v_1}, \dots, \overline{v_n})$ y est génératrice, donc c'est également le cas de la famille $(\overline{v_1}, \dots, \overline{v_{n-1}})$ car $\overline{v_n} = \overline{0}$. Si on applique l'hypothèse de récurrence aux familles $(\overline{e_1}, \dots, \overline{e_{p-1}})$ et $(\overline{v_1}, \dots, \overline{v_{n-1}})$ dans l'espace $E/\langle v_n \rangle$, on obtient que $p-1 \leq n-1$ donc $p \leq n$. Ce qui termine la preuve.

Corollaire 1.6.5.1 (Dimension d'un espace vectoriel)
Si un espace vectoriel *E admet une base finie, toutes ses bases ont le même cardinal, appelé dimension de E et notée* $\dim(E)$.

Corollaire 1.6.5.2
Soit $\mathbb{K}$ un anneau à division.
Soient $m, n \in \mathbb{N}$. Alors :
$$\mathbb{K}^m \cong \mathbb{K}^n \Leftrightarrow m = n$$

Corollaire 1.6.5.3 (Rang d'un module libre)
Soit $\mathbb{A}$ un anneau commutatif non trivial.
Soit E un $\mathbb{A}$–module libre.
Alors toutes les bases de E ont même cardinal, appelé rang de E et noté $\mathrm{rg}(E)$.

15. Si vous me passez l'expression.

DÉMONSTRATION : Si $\mathbb{A}$ est un corps, on montre que :

$$\left(\mathbb{A}^{(I)} \cong \mathbb{A}^{(J)}\right) \Rightarrow (\mathrm{card}(I) = \mathrm{card}(J))$$

Sinon, on se donne un idéal maximal M de $\mathbb{A}$ (l'existence nous en est donnée par la proposition 1.4.1). On pose $\mathbb{K} = \mathbb{A}/M$, qui forme alors un corps. Si on pose $ME = \{mx \,|\, m \in M,\, x \in E\}$, on peut montrer que E/ME est un espace vectoriel sur $\mathbb{K}$ (en fait, si M est un idéal quelconque, E/ME est un $\mathbb{A}/M$–module).

De plus, $\mathbb{A}^{(I)}/M\mathbb{A}^{(I)} \cong \mathbb{K}^{(I)}$ pour tout ensemble I via $(\lambda_i)_i \mapsto (\lambda_i.M)_i$ et la proposition 1.5.4. En conclusion, comme si $\mathbb{A}^{(I)} \cong \mathbb{A}^{(J)}$ alors $\mathbb{A}^{(I)}/M\mathbb{A}^{(I)} \cong \mathbb{A}^{(J)}/M\mathbb{A}^{(J)}$, on a que $\mathbb{K}^{(I)} \cong \mathbb{K}^{(J)}$ ce qui implique $\mathrm{card}(I) = \mathrm{card}(J)$. D'où le résultat.

1.7 Algèbre linéaire dans les modules libres de rang fini

Dans tout ce paragraphe, $\mathbb{A}$ désigne un anneau *commutatif* non trivial.

Soient E, F deux $\mathbb{A}$–modules libres de rangs (finis) respectifs n et p et de bases respectives $\mathcal{B}_1$ et $\mathcal{B}_2$.
Si $u \in \mathrm{Hom}_{\mathbb{A}}(E,F)$, on définit sa matrice $\mathrm{mat}_{\mathcal{B}_1,\mathcal{B}_2}(u) \in \mathcal{M}_{p,n}(\mathbb{A})$ comme dans le cas d'un corps.

On obtient alors un isomorphisme de $\mathbb{A}$–modules :

$$\begin{aligned}\mathrm{Hom}_{\mathbb{A}}(E,F) &\to \mathcal{M}_{p,n}(\mathbb{A})\\ u &\mapsto \mathrm{mat}_{\mathcal{B}_1,\mathcal{B}_2}(u)\end{aligned}$$

Ce qui implique que $\mathrm{Hom}_{\mathbb{A}}(E,F)$ est un $\mathbb{A}$–module[16] libre de rang $p \times n$. En particulier :

$$\mathrm{End}_{\mathbb{A}}(E) \cong \mathcal{M}_n(\mathbb{A})$$

La plupart des us et coutumes de l'algèbre linéaire "classique" restent valable dans ce cadre.

- La composition des applications linéaires correspond au produit matriciel. On a même un isomorphisme de groupes :
$$(\mathrm{Aut}_{\mathbb{A}}, \circ) \cong (G\ell_n(\mathbb{A}), \times)$$
- *Changement de base.* Si $\mathcal{B}$ et $\mathcal{B}'$ sont deux bases de E, on appelle *matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$* la matrice :
$$P_{\mathcal{B}\to\mathcal{B}'} := \mathrm{mat}_{\mathcal{B}',\mathcal{B}}(\mathrm{id}_E) \in G\ell_n(\mathbb{A})$$
De plus, si $u \in \mathrm{Hom}_{\mathbb{A}}(E,F)$ et que $\mathcal{B}_1, \mathcal{B}_1'$ (resp. $\mathcal{B}_2, \mathcal{B}_2'$) sont deux bases de E (resp. F) et si on pose $M = \mathrm{mat}_{\mathcal{B}_1,\mathcal{B}_2}(u)$ et $M' = \mathrm{mat}_{\mathcal{B}_1',\mathcal{B}_2'}(u)$ on a :
$$M' = \left(P_{\mathcal{B}_1\to\mathcal{B}_1'}\right)^{-1} M P_{\mathcal{B}_2\to\mathcal{B}_2'}$$
- ✘ La notion de rang d'une application linéaire n'a *aucun sens* dans ce cadre : $\mathrm{Im}(u)$ n'est *pas* a priori un sous–module libre de F !
- *Déterminant.* Si $U = (u_{i,j})_{i,j} \in G\ell_n(\mathbb{A})$, on définit le déterminant de U via la formule :
$$\det(U) := \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} u_{i,\sigma(i)}$$
On peut aussi le faire par récurrence et développements selon la première ligne, mais ce n'est pas très drôle[17]. Ou on peut définir det comme la seule forme n–linéaire (en les colonnes) alternée vérifiant $\det(I_n) = 1$, ce qui est assez sympathique. On montre que le déterminant est invariant par changement de base, ce qui permet de définir le déterminant d'un endomorphisme.
- Soient $U, V \in \mathcal{M}_n(\mathbb{A})$. Alors :
  (i) $\det(U) = \det({}^tU)$;
  (ii) U est inversible $\Leftrightarrow \det(U) \in \mathbb{A}^\times \Leftrightarrow U$ est inversible à gauche $\Leftrightarrow U$ est inversible à droite ;

16. Rappelons que ceci est faux en général si $\mathbb{A}$ n'est pas commutatif.
17. Sauf si, bien sur, vous êtes informaticien.

(iii) $\det(UV) = \det(U)\det(V)$, ce qui entraîne que si $U \in G\ell_n(\mathbb{A})$, $\det(U^{-1}) = \det(U)^{-1}$;

(iv) $U{}^t\mathrm{Com}(U) ={}^t \mathrm{Com}(U)U = \det(U)I_n$.

– On généralise également les formules classiques de l'algèbre linéaire, telles celles de Cramer.

Proposition 1.7.1
Soit E un $\mathbb{A}$–module libre de rang fini.
Soit $u \in \mathrm{End}_{\mathbb{A}}(E)$. Alors on a équivalence entre les propriétés suivantes :

(i) $u \in \mathrm{Aut}_{\mathbb{A}}(E)$ *;*

(ii) $\det(u) \in \mathbb{A}^\times$ *;*

(iii) u est inversible à gauche dans $\mathrm{End}_{\mathbb{A}}(E)$ *;*

(iv) u est inversible à droite dans $\mathrm{End}_{\mathbb{A}}(E)$ *;*

(v) u est ***surjectif****.*

✘ L'injectivité de u n'est pas suffisante ici ! Par exemple, $u : x \mapsto 2x$ est un endomorphisme $\mathbb{Z}$–linéaire injectif du $\mathbb{Z}$–module $\mathbb{Z}$ mais $\det(u) = 2 \notin \mathbb{Z}^\times = \{-1, 1\}$ ...

Proposition 1.7.2
Soit E un $\mathbb{A}$–module libre de rang fini.
Soit $u \in \mathrm{End}_{\mathbb{A}}(E)$. Alors on a équivalence entre les propriétés suivantes :

(i) u est injectif;

(ii) $\det(u)$ *est régulier dans* $\mathbb{A}$.

Proposition 1.7.3 (Polynômes en un endomorphisme)
Soit E un $\mathbb{A}$–module.
Soit $u \in End_{\mathbb{A}}(E)$.
Soit $P = \sum_{i=0}^d a_i T^i \in \mathbb{A}[T]$.
Alors on a que :

$$P(u) := \sum_{i=0}^{d} a_i u^i \in \mathrm{End}_{\mathbb{A}}(E)$$

Où $u^i = \underbrace{u \circ \ldots \circ u}_{i fois}$, *avec la convention que* $u^0 = \mathrm{id}_E$. *On définit de même un polynôme en une matrice.*

✘ Attention :

$$P(u) = a_0 \mathrm{id}_E + \ldots + a_d u^d \text{ et non } a_0 + \ldots + a_d u^d$$

✍ Pour $u \in \mathrm{End}_{\mathbb{A}}$, l'application suivante est un morphisme d'anneaux :

$$\begin{aligned} \mathbb{A}[T] &\to \mathrm{End}_{\mathbb{A}}(E) \\ P &\mapsto P(u) \end{aligned}$$

Proposition 1.7.4 (Changement d'anneau)
Soit $\mathbb{B}$ un autre anneau commutatif non trivial.
Soit $\varphi : \mathbb{A} \to \mathbb{B}$ un morphisme d'anneaux.
Pour $U = (u_{i,j})_{i,j} \in \mathcal{M}_n(\mathbb{A})$, on définit la matrice :

$$U^\varphi = \left(\varphi(u_{i,j})\right)_{i,j} \in \mathcal{M}_n(\mathbb{B})$$

Alors :

$$\begin{aligned} \mathcal{M}_n(\mathbb{A}) &\to \mathcal{M}_n(\mathbb{B}) \\ U &\mapsto U^\varphi \quad \textit{est un morphisme d'anneaux.} \end{aligned}$$

De même :

$$\begin{aligned} \mathbb{A}[T] &\to \mathbb{B}[T] \\ P = \sum_{i=0}^{d} a_i T^i &\mapsto P^\varphi := \sum_{i=0}^{d} \varphi(a_i) T^i \quad \textit{est un morphisme d'anneaux.} \end{aligned}$$

On a de plus que, si $(P, U) \in \mathbb{A}[T] \times \mathcal{M}_n(\mathbb{A})$:

(i) $\det(U^\varphi) = \varphi(\det(U))$ *;*

(ii) $(P(U))^\varphi = P^\varphi(U^\varphi)$.

Exercice : Expliciter les U^φ et P^φ lorsque :

1. $\varphi = \mathbb{Z} \hookrightarrow \mathbb{Q}$;
2. φ est la projection canonique $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$;
3. φ est la conjugaison complexe.

Définition 1.7.1 (Polynôme caractéristique)
Soit $U \in \mathcal{M}_n(\mathbb{A})$.
On appelle polynôme caractéristique de U le polynôme :

$$P_U := \det(\underbrace{U - TI_n}_{\in \mathcal{M}_n(\mathbb{A}[T])}) \in \mathbb{A}[T]$$

Théorème 1.7.5 (Cayley–Hamilton)
Soit $U \in \mathcal{M}_n(\mathbb{A})$.
Alors :

$$P_U(U) = 0_{\mathcal{M}_n(\mathbb{A})}$$

DÉMONSTRATION :

- On admet le résultat si $\mathbb{A}$ est un corps (se reporter à un cours d'algèbre linéaire[18]).
- Si $\mathbb{A}$ est intègre, $\mathbb{A}$ s'injecte via un morphisme φ dans son corps des fractions $\mathbb{K}$. Alors :

  $$(P_U(U))^\varphi = P_{U^\varphi}(\underbrace{U^\varphi}_{\in \mathcal{M}_n(\mathbb{K})}) = 0$$

  Donc $P_U(U) = 0$ par injectivité de de φ.
- Si $\mathbb{A}$ est un anneau quelconque, appelons $u_{i,j}$ les coefficients de U, donnons nous n^2 indéterminées $(V_{i,j})_{1 \leq i,j \leq n}$ et posons $\mathcal{R} = \mathbb{Z}[(V_{i,j})_{i,j}]$. Posons enfin $V = (V_{i,j})_{i,j} \in \mathcal{M}_n(\mathcal{R})$. On a de facto un morphisme d'anneaux, appelé *morphisme d'évaluation* :

  $$\begin{aligned} \varphi : \mathcal{R} &\to \mathbb{A} \\ V_{i,j} &\mapsto u_{i,j} \\ x \in \mathbb{Z} &\mapsto x.1_{\mathbb{A}} \end{aligned}$$

  Par construction, on a alors que :

  $$U = V^\varphi$$

  Donc :

  $$P_U(U) = P_{V^\varphi}(V^\varphi) = (P_V(V))^\varphi = 0 \text{ car } \mathcal{R} \text{ est intègre.}$$

18. Voire d'algèbre linéaire *numérique* ...

Chapitre 2

Anneaux principaux et euclidiens

Dans tout ce chapitre et sauf mention du contraire, les anneaux seront supposés ***commutatifs***.

2.1 Divisibilité

Dans tout ce paragraphe, $\mathbb{A}$ désigne un anneau ***intègre***.

Définition 2.1.1 (Divisibilité)
Soient $a, b \in \mathbb{A}$.
Alors on dit que a divise b dans $\mathbb{A}$ si (définitions équivalentes) :

(i) $\exists c \in \mathbb{A},\ b = ac$;

(ii) $(b) \subset (a)$.

✍ On note alors $a|b$. Pour $a \in \mathbb{A}$, on pose :

$$\mathrm{Div}_{\mathbb{A}}(a) = \{b \in \mathbb{A} \mid b|a\}$$

Définition 2.1.2 (Éléments associés)
Soient $a, b \in \mathbb{A}$.
Alors a et b sont dits associés dans $\mathbb{A}$ si (définitions équivalentes) :

(i) $a|b$ *et* $b|a$;

(ii) $\exists c \in \mathbb{A}^\times,\ b = ac$ *(et donc a fortiori* $a = bc^{-1}$*)* ;

(iii) $(a) = (b)$.

✍ La relation d'association est une relation d'équivalence que nous noterons désormais "$\sim$", comme dans "relation d'équivalence".

En outre, $\mathbb{A}/\sim$ s'identifie à l'ensemble des idéaux principaux de $\mathbb{A}$ via $\overline{a} \mapsto (a)$. La multiplication dans $\mathbb{A}/\sim$ s'identifie au produit d'idéaux défini de la façon suivante : si I et J sont deux idéaux de $\mathbb{A}$, on pose

$$I.J = \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; n \geq 1,\ (a_i)_i \in I^n,\ (b_i)_i \in J^n \right\}$$

Définition 2.1.3 (Plus grand commun diviseur)
Soient I un ensemble et $(a_i)_i \in \mathbb{A}^I$.
Soit $c \in \mathbb{A}$.
Alors on dit que c est un plus grand commun diviseur (pgcd) de $(a_i)_i$ si (définitions équivalentes) :

(i)
$$\mathrm{Div}_{\mathbb{A}}(c) = \bigcap_{i \in I} \mathrm{Div}_{\mathbb{A}}(a_i)$$

(ii) (c) *est le plus petit idéal principal contenant tous les* a_i ;

(iii) (c) *est le plus petit idéal principal contenant l'idéal* $\sum_i (a_i)$.

Définition 2.1.4 (Plus petit commun multiple)
Soient I un ensemble et $(a_i)_i \in \mathbb{A}^I$.
Soit $c \in \mathbb{A}$.
Alors on dit que c est un plus petit commun multiple (ppcm) de $(a_i)_i$ si (définitions équivalentes) :

(i) l'ensemble des multiples de c est égal à l'intersection des ensembles des multiples des a_i ;

(ii)
$$(c) = \bigcap_{i \in I} (a_i)$$

✘ On n'a pas nécessairement existence d'un pgcd (resp. ppcm). De plus, si "le" pgcd (resp. ppcm) existe, il est unique ***à association près***. Malgré tout, on notera souvent (par abus) "$d = \text{pgcd}(a, b)$" (resp. "$d = \text{ppcm}(a, b)$").

Exemple : Dans $\mathbb{Z}$, $1 = \text{pgcd}(2, 3)$ et $-1 = \text{pgcd}(2, 3)$ sans que l'on ait $1 = -1$!

Proposition 2.1.1
Soient $a, b \in \mathbb{A}$.
Alors :

(i) a et b ont un ppcm $\Leftrightarrow$ l'idéal $(a) \cap (b)$ est principal ;

(ii) a et b ont un pgcd $\Leftrightarrow$ il existe un plus petit principal contenant (a, b) ;

(iii) Si *(a, b) est principal,* alors *a et b ont un pgcd. La réciproque est* fausse *;*

(iv) (a, b) est principal $\Leftrightarrow$ a et b ont un pgcd d et *$\exists u, v \in \mathbb{A},\ d = ua + vb$.*

Exemples :

1. Dans $\mathbb{R}[X, Y]$, X et Y ont 1 pour pgcd mais (X, Y) n'est pas principal car $\nexists U, V \in \mathbb{R}[X, Y], UX + VY = 1$.
2. Dans $\mathbb{Z}[X]$, $1 = \text{pgcd}(X, 2)$ mais $(2, X)$ n'est pas principal car sinon il contiendrait 1 et donc l'anneau tout entier, alors qu'il est en fait égal à l'ensemble des polynômes à coefficient constant pair.

Définition 2.1.5 (Éléments premiers entre eux, étrangers)
Soient $a, b \in \mathbb{A}$.
Alors :

(i) a et b sont dits premiers entre eux si 1 est un pgcd de a et b, i.e si tout diviseur commum de a et b est inversible ;

(ii) a et b sont dits étrangers si $(a, b) = \mathbb{A}$, i.e si $\exists u, v \in \mathbb{A},\ ua + vb = 1$;

Proposition 2.1.2
Deux éléments étrangers sont premiers entre eux.

✘ La réciproque et fausse : s'intéresser au cas de 2 et X dans $\mathbb{Z}[X]$.

Définition 2.1.6 (Élément irréductible)
Soit $p \in \mathbb{A}$.
Alors p est dit irréductible si :

(i) $p \neq 0$;

(ii) $p \notin \mathbb{A}^\times$;

(iii) les seuls (à association près) diviseurs de p sont 1 et p.

Remarque Si p est irréductible et $a \in \mathbb{A}$ alors soit $p|a$ et alors $\text{pgcd}(a, p) = 1$, soit $p \nmid a$ et donc a et p sont premiers entre eux.

Exemples :

1. Les irréductibles de $\mathbb{Z}$ sont les nombres premiers (positifs et négatifs).
2. 2 et X sont irréductibles dans $\mathbb{Z}[X]$.

2.2 Généralités sur les anneaux principaux et euclidiens

Définition 2.2.1 (Anneau principal)
Un anneau $\mathbb{A}$ est dit principal si :

(i) *$\mathbb{A}$ est intègre ;*

(ii) *tout idéal de $\mathbb{A}$ est principal.*

Exemples :

1. Un corps est un anneau principal.
2. $\mathbb{Z}$ est principal.
3. Si $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ est principal. La réciproque est vraie (nous en parlerons un peu plus loin).
4. L'anneau $\mathbb{A}[X,Y]$ n'est *jamais* principal, quelle que soit la nature/religion/orientation politique/boisson préfére de $\mathbb{A}$. En effet, l'idéal (X,Y) ne sera *jamais* principal. Même si on insiste.
5. $\mathbb{Z}[X]$ n'est pas principal, et c'est encore la faute de $(2,X)$.

Proposition 2.2.1
Dans un anneau principal $\mathbb{A}$, toute famille $(a_i)_i$ admet un pgcd et un ppcm. De plus :

(i) *tout générateur de l'idéal $\cap_i(a_i)$ est un ppcm de $(a_i)_i$;*

(ii) *tout générateur de l'idéal $((a_i)_i)$ est un pgcd de $(a_i)_i$.*

Corollaire 2.2.1.1 (Identité de Bézout)
Soit $\mathbb{A}$ un anneau principal.
Soient $a, b \in \mathbb{A}$ et soit $d = \mathrm{pgcd}(a,b)$.
Alors :

$$\exists u, v \in \mathbb{A},\ d = ua + bv$$

Corollaire 2.2.1.2
Dans un anneau principal, deux éléments premiers entre eux sont étrangers.

Définition 2.2.2 (Jauge euclidienne)
Soit $\mathbb{A}$ un anneau intègre.
Une jauge euclidienne (ou stathme euclidien) sur $\mathbb{A}$ est une application $\delta : \mathbb{A} \to \mathbb{N}$ telle que :

(i) Croissance. *Si $a|b$ avec $(a,b) \in \mathbb{A} \times \mathbb{A}^*$, alors $\delta(a) \leq \delta(b)$.*

(ii) Division euclidienne. *Si $(a,b) \in \mathbb{A} \times \mathbb{A}^*$, alors :*

$$\exists r, q \in \mathbb{A},\ a = bq + r,\ \delta(r) < \delta(q)$$

☞ Si un anneau $\mathbb{A}$ admet une jauge, il est dit *euclidien.*

Remarques :

1. Si $\mathbb{A}$ est euclidien, il admet un élément de jauge minimale, qui est nécessairement 0 (par propriété de division euclidienne).
2. Si il existe $\eta : \mathbb{A} \to \mathbb{N}$ vérifiant la propriété de division euclidienne, alors $\mathbb{A}$ est euclidien via la jauge :
$$\delta : a \mapsto \min_{x \in \mathbb{A}^*} \eta(x)$$

Exemples :

1. $\mathbb{Z}$ est euclidien, via la jauge $|.|$.
2. Si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[X]$ est euclidien via la jauge :
$$\delta : P \mapsto \begin{cases} \deg(P)+1 & \text{si } P \neq 0 \\ 0 & \text{si } P = 0 \end{cases}$$
3. L'anneau $\mathbb{Z}[i]$ des entiers de Gauss est euclidien, de jauge $\delta : z \mapsto |z|^2$.

Proposition 2.2.2
Tout anneau euclidien est principal.

☞ Plus précisément, si $\mathcal{I}$ est un idéal d'un anneau euclidien $\mathbb{A}$, alors $\mathcal{I} = \{0\}$ ou bien $\mathcal{I} = (\alpha)$, avec α de jauge minimal *dans* $\mathbb{A}^*$.

Algorithme 2.2.1 (Euclide étendu)
Soit $\mathbb{A}$ un anneau euclidien de jauge δ.
Soient $a, b \in \mathbb{A}$.
On souhaite calculer $(u, v) \in \mathbb{A}^2$ tels que $ua + vb = \operatorname{pgcd}(a, b)$.

- *Si $b = 0$, $\operatorname{pgcd}(a, b) = a$ et donc on renvoie $(u, v) = (1, 0)$.*
- *Sinon, par division euclidienne, on peut écrire :*

$$a = bq + r,\ \delta(r) < \delta(b)$$

On en déduit que les idéaux (a, b) et (b, r) sont égaux et donc que $d := \operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, r)$.
Plus précisément, si on a trouvé (s, t) tels que $d = sb + tr$, alors :

$$d = sb + t(a - bq) = ta + (s - tq)b$$

Et donc on renvoie $(u, v) = (t, s - tq)$.

Proposition 2.2.3 (Lemme Chinois)
Soit $\mathbb{A}$ un anneau (commutatif).
Soient I, J deux idéaux étrangers de $\mathbb{A}$, i.e tels que :

$$I + J = \mathbb{A}$$

Alors :
(i) $I \cap J = I.J$;
(ii) on a un isomorphisme d'anneaux :

$$\begin{aligned} \mathbb{A}/I.J &\to (\mathbb{A}/I) \times (\mathbb{A}/J) \\ x \bmod I.J &\mapsto (x \bmod I, x \bmod J) \end{aligned}$$

Démonstration : I et J sont étrangers donc il existe $(\alpha, \beta) \in I \times J$ tels que :

$$1 = \alpha + \beta$$

L'inclusion $I.J \subset I \cap J$ découlant immédiatement de la structure d'idéal de I et J, il nous reste à montrer que $I \cap J \subset I.J$. Or, si $x \in I \cap J$, on a :

$$x = 1x = \underbrace{\alpha x}_{\in I.J} + \underbrace{x\beta}_{\in I.J} \in I.J$$

D'où le point (i).
Posons à présent :

$$\begin{aligned} \varphi : \mathbb{A} &\to (\mathbb{A}/I) \times (\mathbb{A}/J) \\ x &\mapsto (x \bmod I, x \bmod J) \end{aligned}$$

L'application φ est un morphisme d'anneaux par définition de la loi quotient. De plus :

$$\operatorname{Ker}(\varphi) = I \cap J = I.J$$

Ce qui implique que :

$$\mathbb{A}/I.J \cong \operatorname{Im}(\varphi)$$

Or, comme $\varphi(\alpha) = (0, 1)$ et $\varphi(\beta) = (1, 0)$, on a que :

$$\forall (x, y) \in (\mathbb{A}/I) \times (\mathbb{A}/J),\ \varphi(x\beta + y\alpha) = (x, y)$$

Donc φ est surjective, d'où le résultat.

Corollaire 2.2.3.1
Soit $\mathbb{A}$ un anneau principal.
Soient $a, b \in \mathbb{A}$ premiers entre eux.
Alors :

$$\mathbb{A}/(a,b) \cong (\mathbb{A}/(a)) \times (\mathbb{A}/(b))$$

Via l'isomorphisme d'anneaux $x \bmod ab \mapsto (x \bmod a, x \bmod b)$.

Proposition 2.2.4
Soit $\mathbb{A}$ un anneau principal.
Soit $p \in \mathbb{A}^*$.
On a alors équivalence entre les propriétés suivantes :

(i) p *est irréductible ;*

(ii) (p) *est premier (on dit que p est un* élément premier *de $\mathbb{A}$;*

(iii) (p) *est maximal.*

Démonstration :

$(iii) \Rightarrow (ii)$ Trivial.

$(ii) \Rightarrow (i)$ Vrai dans tout anneau intègre.

$(i) \Rightarrow (iii)$ Remarquons que $(p) \subsetneq \mathbb{A}$ car $p \notin \mathbb{A}^\times$. Soit $\mathcal{I}$ un idéal contenant (p). Comme $\mathcal{I}$ est principal, $\exists \alpha \in \mathbb{A}$, $\mathcal{I} = (\alpha)$. Comme $p \in \mathcal{I}$, $\alpha | p$ donc soit $\alpha \in \mathbb{A}^\times$ et donc $\mathcal{I} = \mathbb{A}$, soit $\alpha \sim p$ et alors $\mathcal{I} = (p)$. Donc (p) est maximal, ce qui conclut la preuve.

Remarques :

1. Les idéaux premiers de $\mathbb{A}$ sont donc (0) et les (p), avec p irréductible, ces derniers étant maximaux.
2. (0) n'est maximal que si $\mathbb{A}$ est un corps.
3. En général, un élément irréductible n'est pas premier.

Corollaire 2.2.4.1
Soit $\mathbb{A}$ un anneau principal.
Soit $p \in \mathbb{A}^*$ un élément irréductible.
Alors $\forall x, y \in \mathbb{A}$, si $p|xy$ on a nécessairement $p|x$ ou $p|y$.

Proposition 2.2.5 (Un anneau principal est factoriel)
Soit $\mathbb{A}$ un anneau principal.
Soit $z \in \mathbb{A}^*$.
Alors :

(i) il existe $\varepsilon \in \mathbb{A}^\times$, $n \in \mathbb{N}$ et une famille d'irréductibles $p_1, \dots p_n$ tels que :

$$z = \varepsilon \prod_{i=1}^{n} p_i$$

(ii) cette décomposition est unique au sens suivant : si on peut écrire deux décompositions $\varepsilon p_1 \dots p_n$ et $\eta q_1 \dots q_m$ de z, alors $m = n$ et (quitte à réordonner) $\forall 1 \leq i \leq n, p_i \sim q_i$.

Un anneau vérifiant (i) et (ii) est dit factoriel.

Démonstration :

(i) Supposons z "non décomposable". Alors z ne peut être ni inversible ni irréductible, et donc $\exists z_1, z_2 \notin \mathbb{A}^\times$ tels que $z = z_1 z_2$ et dont l'un des deux au moins est "non décomposable". En itérant ce procédé via l'axiome du choix on obtient une suite $(z_n)_n$ telle que $\forall n \geq 0, z_{n+1} | z_n$ et $z_{n+1} \not\sim z_n$ (avec $z_0 = z$), ce qui engendre une suite strictement croissante d'idéaux $I_n := (z_n)$. Or, si on pose :

$$J = \bigcup_{n \geq 0} I_n$$

J est un idéal donc $\exists \alpha \in \mathbb{A}$, $J = (\alpha)$ (par principalité), ce qui implique l'existence d'un n tel que $\alpha \in I_n$, d'où :

$$(\alpha) \subset I_n \subsetneq I_{n+1} \subset J = (\alpha)$$

Ce qui est impossible.

(*ii*) Quitte à simplifier, supposons que $\eta = 1$. Si l'on suppose que $\forall i, j,\ p_i \not\sim q_j$, alors si $n > 0$ on a :

$$p_1 | \prod_{j=1}^{m} q_j$$

Et donc, d'après le corollaire 2.2.4.1, p_1 divise l'un des q_j, ce qui est impossible. Donc $n = m = 0$ et $\varepsilon = 1$. D'où le résultat.

Remarques :

1. On peut démontrer que si $\mathbb{A}$ est factoriel, alors $\mathbb{A}[X]$ l'est également, et donc tous les $\mathbb{A}[X_1, \ldots, X_n]$ seront factoriels. Cependant, $\mathbb{A}[X]$ n'est principal que si $\mathbb{A}$ est un corps.
2. On déduit de la proposition 2.2.5 que si $\mathbb{A}$ est principal mais n'est pas un corps, il contient au moins un irréductible.
3. Si $\mathbb{A}$ est euclidien, on peut démontrer (*i*) sans avoir recours à l'axiome du choix, via un récurrence sur la jauge.

Définition 2.2.3 (Système représentatif des irréductibles d'un anneau principal)
Soit $\mathbb{A}$ un anneau principal.
Soit $\mathcal{P}$ l'ensemble des idéaux premiers de $\mathbb{A}$.
On appelle système représentatif des irréductibles de $\mathbb{A}$ tout ensemble $\Sigma \subset \mathbb{A}$ composé exclusivement de générateurs d'éléments de $\mathcal{P}$ vérifiant que pour tout $\mathcal{I} \in \mathcal{P}$, Σ ne contienne qu'un et un seul générateur de $\mathcal{I}$.

Exemples :

1. Un système représentatif des irréductibles de $\mathbb{Z}$ est l'ensemble des nombres premiers positifs.
2. Si $\mathbb{K}$ est un corps, un système représentatif des irréductibles de $\mathbb{K}[X]$ est l'ensemble des polynômes irréductibles unitaires.

Proposition 2.2.6
Soit $\mathbb{A}$ un anneau principal.
Soit Σ un système représentatif des irréductibles de $\mathbb{A}$.
Alors tout élément $z \neq 0$ s'écrit de façon unique *sous la forme :*

$$z = \varepsilon(z) \sum_{p \in \Sigma} p^{e_p(z)}$$

Avec $\varepsilon(z) \in \mathbb{A}^\times$ et les $e_p(z) \in \mathbb{N}$ presque tous nuls.

Corollaire 2.2.6.1
Soit $\mathbb{A}$ un anneau principal.
Soit Σ un système représentatif des irréductibles de $\mathbb{A}$.
Alors $\forall z, z' \in \mathbb{A}^*$, on a :

$$z | z' \Leftrightarrow \forall p \in \Sigma,\ e_p(z) \leq e_p(z')$$

Corollaire 2.2.6.2
Soit $\mathbb{A}$ un anneau principal.
Soit Σ un système représentatif des irréductibles de $\mathbb{A}$.
Soient $a, b \in \mathbb{A}^*$.
Alors :

(*i*) $\forall p \in \Sigma,\ e_p(\mathrm{pgcd}(a, b)) = \min(e_p(a), e_p(b))$;
(*ii*) $\forall p \in \Sigma,\ e_p(\mathrm{ppcm}(a, b)) = \max(e_p(a), e_p(b))$;

Corollaire 2.2.6.3
Soit $\mathbb{A}$ un anneau principal.
Soit Σ un système représentatif des irréductibles de $\mathbb{A}$.
Soit $\mathbb{K}$ le corps des fractions de $\mathbb{A}$.
Alors tout élément $z \in \mathbb{K}^*$ s'écrit de façon unique *sous la forme :*

$$z = \varepsilon(z) \sum_{p \in \Sigma} p^{e_p(z)}$$

Avec $\varepsilon(z) \in \mathbb{A}^\times$ et les $e_p(z) \in \mathbb{Z}$ presque tous nuls.

☞ En particulier, on a un isomorphisme de groupes :

$$\mathbb{K}^* \cong \mathbb{A}^\times \times \mathbb{Z}^{(\Sigma)}$$

Via $z \mapsto (\varepsilon(z), (e_p(z))_{p\in\Sigma}$.

2.3 Opérations élémentaires sur les matrices

Dans tout ce paragraphe, $\mathbb{A}$ désigne un anneau (commutatif).

Définition 2.3.1 (Groupe spécial linéaire)
Soit $n \geq 0$. On appelle groupe spécial linéaire d'ordre n le sous groupe $S\ell_n(\mathbb{A})$ de $G\ell_n(\mathbb{A})$ égal au noyau de l'application $\det : G\ell_n(\mathbb{A}) \to \mathbb{A}^\times$.

☞ Plus explicitement, on a :

$$S\ell_n(\mathbb{A}) = \{M \in G\ell_n(\mathbb{A}) \mid \det(M) = 1_{\mathbb{A}}\}$$

Fixons nous à présent deux entiers n et p.

Définition 2.3.2 (Matrices élémentaires)
Pour $1 \leq i, j \leq n$, on pose :

$$e_{i,j} = (\delta_{i,k}\delta_{j,l})_{k,l} \in \mathcal{M}_n(\mathbb{A})$$

La famille $(e_{i,})_{i,j}$ forme alors une $\mathbb{A}$–base de $\mathcal{M}_n(\mathbb{A})$. De plus, si $i \neq j$ et $a \in \mathbb{A}$, on définit la (i,j)–ième matrice élémentaire d'ordre n en a par :

$$E_{i,j}(a) = I_n + ae_{i,j}$$

On note $E_n(\mathbb{A})$ le sous–groupe de $S\ell_n(\mathbb{A})$ engendré par ces matrices.

Proposition 2.3.1
Soient $1 \leq i \neq j \leq n$ et $a, b \in \mathbb{A}$.
Alors :
- *(i)* $E_{i,j}(a)E_{i,j}(b) = E_{i,j}(a+b)$;
- *(ii)* $E_{i,j}(0) = I_n$.

Ainsi, $E_{i,j} : x \mapsto E_{i,j}(x)$ est un morphisme de groupes de $(\mathbb{A}, +)$ dans $(S\ell_n(\mathbb{A}), \times)$.

Proposition 2.3.2 (Opérations élémentaires)
Soit $M \in \mathcal{M}_{n,p}(\mathbb{A})$.
- *(i) Multiplier M à droite par la (i,j)–ième matrice élémentaire d'ordre p en $a \in \mathbb{A}$ revient à effectuer l'opération $C_j \leftarrow C_j + aC_i$.*
- *(ii) Multiplier M à gauche par la (i,j)–ième matrice élémentaire d'ordre n en $a \in \mathbb{A}$ revient à effectuer l'opération $L_j \leftarrow L_j + aL_i$.*

Définition 2.3.3 (Équivalences matricielles)
Soient $M, N \in \mathcal{M}_n(\mathbb{A})$.
- *(i) on dit que M et N sont (G–)équivalentes, ce que l'on note $M \overset{\mathrm{G}}{\sim} N$ si :*

$$\exists P \in G\ell_n(\mathbb{A}), Q \in G\ell_p(\mathbb{A}), \quad N = PMQ$$

- *(ii) on dit que M et N sont S–équivalentes, ce que l'on note $M \overset{\mathrm{S}}{\sim} N$ si :*

$$\exists P \in S\ell_n(\mathbb{A}), Q \in S\ell_p(\mathbb{A}), \quad N = PMQ$$

- *(iii) on dit que M et N sont E–équivalentes, ce que l'on note $M \overset{\mathrm{E}}{\sim} N$ si :*

$$\exists P \in E_n(\mathbb{A}), Q \in E_p(\mathbb{A}), \quad N = PMQ$$

☞ $M \overset{\mathrm{E}}{\sim} N \Leftrightarrow N$ s'obtient à partir de M via les opérations élémentaires de la proposition 2.3.2.

Interprétation en termes d'actions de groupes : Le groupe $G\ell_n(\mathbb{A}) \times G\ell_p(\mathbb{A})$ agit à gauche sur $\mathcal{M}_{n,p}(\mathbb{A})$ via :

$$(P, Q).M := PMQ^{-1}$$

Les orbites pour cette action de groupes correspondent aux classes d'équivalences pour la relation $\overset{\mathrm{G}}{\sim}$. On peut similairement décrire les classes modulo $\overset{\mathrm{S}}{\sim}$ et $\overset{\mathrm{E}}{\sim}$.

Proposition 2.3.3 (Forme normale de Smith)
Soit $\mathbb{A}$ un anneau principal.
Soit $M \in \mathcal{M}_{n,p}(\mathbb{A})$.
Alors il existe $d_1, \ldots, d_r \in \mathbb{A}^*$ tels que :

(i) $\forall 1 \leq i \leq r-1,\ d_i | d_{i+1}$;

(ii)

$$M \overset{\mathrm{S}}{\sim} \mathrm{diag}_{n,p}(d_1, \ldots, d_r) := \begin{pmatrix} d_1 & 0 & \ldots & 0 & \\ 0 & d_2 & \ddots & \vdots & (0) \\ \vdots & \ddots & \ddots & 0 & \\ 0 & \ldots & 0 & d_r & \\ & & & & (0) \\ & (0) & & & \end{pmatrix}$$

De plus, si $\mathbb{A}$ est euclidien, on a même $M \overset{\mathrm{E}}{\sim} \mathrm{diag}_{n,p}(d_1, \ldots, d_r)$.

(iii) Unicité. *Si $\mathrm{diag}_{n,p}(d_1, \ldots, d_r)$ et $\mathrm{diag}_{n,p}(c_1, \ldots, c_s)$ vérifient la condition (i) et sont équivalentes, alors :*
– $r = s$;
– $\forall 1 \leq i \leq r,\ d_i \sim c_i$.
Autrement dit, la suite $(d_1) \supset (d_2) \supset \ldots \supset (dr)$ ne dépend que de M.

La matrice $\mathrm{diag}_{n,p}(d_1, \ldots, d_r)$ est appelée forme normale de Smith de la matrice M.

DÉMONSTRATION :

– *"Taille" d'un élément.* Soit $a \in \mathbb{A}^*$. On définit la "taille" $\omega(a)$ de a comme étant le nombre de facteurs irréductibles de a si $\mathbb{A}$ n'est pas euclidien, et on pose $\omega(a) = \delta(a)$ si $\mathbb{A}$ est euclidien de jauge δ.
Si $M = (m_{i,j})_{i,j} \in \mathcal{M}_{n,p}(\mathbb{A})$, on pose :

$$\mu(M) = \min\{\omega(m_{i,j}) \,|\, 1 \leq i \leq n,\ 1 \leq j \leq p,\ m_{i,j} \neq 0\}$$

– *Procédures de transformation des matrices.*

1. Soient $a, b \in \mathbb{A}$. Alors :

$$\begin{aligned} (a \quad b) &\overset{\mathrm{E}}{\sim} (a \quad a+b) && C_2 \leftarrow C_1 + C_2 \\ &\overset{\mathrm{E}}{\sim} (-b \quad a+b) && C_1 \leftarrow C_1 - C_2 \\ &\overset{\mathrm{E}}{\sim} (-b \quad a) && C_1 \leftarrow C_1 + C_2 \end{aligned}$$

   Il nous est donc possible d'échanger (au signe près) deux colonnes d'une matrice. On procède de même pour les lignes. Ainsi, tout coefficient de M peut être placé (au signe près) en position $(1,1)$ sans changer la classe modulo $\overset{\mathrm{E}}{\sim}$ de M ni $\mu(M)$.

2. Soient $a, b \in \mathbb{A}$. Alors :

$$(a \quad ba) \overset{\mathrm{E}}{\sim} (a \quad 0) \qquad\qquad C_2 \leftarrow C_2 - qC_1$$

   Ainsi, si un coefficient de M divise un de ses camarades de la même ligne, on peut remplacer ce dernier par 0 en ne modifiant que les éléments de sa colonne.

3. Soient $a, b \in \mathbb{A}$ tels que $b \nmid a$ et $ab \neq 0$.

– *Cas non euclidien.* On pose $d = pgcd(a,b) =: ua + vb$ et $a =: da'$, $b =: db'$. Alors $ua' + vb' = 1$ et $ab' = ba' = \frac{ab}{d}$ d'où :

$$\begin{pmatrix} a & b \end{pmatrix} \underbrace{\begin{pmatrix} u & -b' \\ v & a' \end{pmatrix}}_{\in S\ell_2(\mathbb{A})} = \begin{pmatrix} d & 0 \end{pmatrix}$$

Donc $\begin{pmatrix} a & b \end{pmatrix} \overset{\mathrm{S}}{\sim} \begin{pmatrix} d & 0 \end{pmatrix}$. De plus, comme $d|a$ et $d \not\sim a$, on a $\omega(d) < \omega(a)$.

– *Cas euclidien.* Par division euclidienne, $\exists q, r \in \mathbb{A}$, $b = aq + r$ avec $\delta(r) < \delta(a)$. Ainsi :

$$\begin{pmatrix} a & b \end{pmatrix} \underbrace{\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}}_{=E_{1,2}(-q)} = \begin{pmatrix} a & r \end{pmatrix}$$

Donc $\begin{pmatrix} a & b \end{pmatrix} \overset{\mathrm{E}}{\sim} \begin{pmatrix} a & r \end{pmatrix}$ avec $\omega(r) < \omega(a)$.

– *Existence de la forme normale de Smith.* On le fait par récurrence sur $\max(n,p)$.
  – Si $\max(n,p) \leq 1$, la propriété est triviale.
  – Si on suppose la propriété valide pour toutes les matrices de $\mathcal{M}_{n',p'}(\mathbb{A})$, avec $\max(n',p') \leq \max(n,p)$, alors on démontre par récurrence sur $\mu(M)$ qu'il existe une matrice N telle que N soit une matrice de Smith *ou* vérifie $\mu(N) < \mu(M)$ satisfaisant à la condition $M \overset{\mathrm{S}}{\sim} N$ ($M \overset{\mathrm{E}}{\sim} N$ dans le cas euclidien). On applique à cet effet l'algorithme suivant :
    – On part de $M = (m_{i,j})_{i,j} \in \mathcal{M}_{n,p}(\mathbb{A})^*$. Quitte à appliquer la procédure 1, on peut supposer que $m_{1,1} \neq 0$ et que $\omega(m_{1,1}) = \mu(M)$.
    – *Cas 1 : il existe $\ell > 1$ tel que $m_{1,1} \nmid m_{1,\ell}$ ou $m_{1,1} \nmid m_{\ell,1}$.* Alors via la procédure 3, M est E ou S–équivalente à une matrice N vérifiant $\mu(N) < \mu(M)$, d'où le résultat.
    – *Cas 2 : $m_{1,1}$ divise sa ligne et sa colonne.* On applique alors la procédure 2 à tous les $m_{1,\ell}$, ce qui nous permet de remplacer la première ligne de M par $\begin{pmatrix} m_{1,} & 0 & \dots & 0 \end{pmatrix}$ sans modifier sa première colonne. En appliquant la même procédure aux colonnes de M on obtient une matrice de la forme :

$$\begin{pmatrix} m_{1,1} & 0 & \dots & \dots & 0 \\ 0 & & & & \\ \vdots & & M_1 & & \\ 0 & & & & \end{pmatrix}$$

Par hypothèse de récurrence, on a alors $M_1 = P_1 D_1 Q_1$ avec $(P_1, Q_1) \in S\ell_{n-1}(\mathbb{A}) \times S\ell_{p-1}(\mathbb{A})$ ou $E_{n-1}(\mathbb{A}) \times E_{p-1}(\mathbb{A})$ et D_1 une matrice de Smith $\mathrm{diag}_{n-1,p-1}(d_2, \dots, d_r)$. D'où $M = PDQ$, avec :

$$P = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & & & & \\ \vdots & & P_1 & & \\ 0 & & & & \end{pmatrix}, \ Q = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & & & & \\ \vdots & & Q_1 & & \\ 0 & & & & \end{pmatrix} \text{ et } D = \mathrm{diag}_{n,p}(m_{1,1}, d_2, \dots, d_r)$$

Si $m_{1,1}|d_2$, D est une matrice de Smith et on a (enfin !) fini. Sinon, on remarque que :

$$\begin{pmatrix} m_{1,1} & 0 \\ 0 & d_2 \end{pmatrix} \overset{\mathrm{E}}{\sim} \begin{pmatrix} m_{1,1} & d_2 \\ 0 & d_2 \end{pmatrix} \qquad L_1 \leftarrow L_1 + L_2$$

On peut alors appliquer la procédure 3 à cette matrice car $m_{1,1} \nmid d_2$, ce qui termine l'algorithme.

– *Unicité.* Soit $r \in \mathbb{N}$. On appelle $I_r(M)$ l'idéal de $\mathbb{A}$ engendré par les mineurs d'ordre r de M (i.e par les déterminants des sous–matrices de taille $r \times r$ de M). On peut alors démontrer que :

1. $I_{r+1}(M) \subset I_r(M)$;
2. si $N \in \mathcal{M}_{p,q}(\mathbb{A})$, alors $I_r(MN) \subset I_r(M).I_r(N) \subset I_r(M) \cap I_r(N)$;
3. si $(P,Q) \in G\ell_n(\mathbb{A}) \times G\ell_q(\mathbb{A})$, alors $I_r(PMQ) = I_r(M)$;

4. Si $D = \mathrm{diag}_{p,q}(d_1, \dots d_n)$ est une matrice de Smith, alors $I_r(D) = (d1 \dots d_n)\mathbb{A}$ si $r \leq n$ et $I_r(D) = 0$ si $r > n$.

On en déduit que $\forall t \leq \min(r, s)$, $d_1 \dots d_t\mathbb{A} = c_1 \dots c_t\mathbb{A}$ donc $d_1 \dots d_t \sim c_1 \dots c_t$ et donc $\forall 1 \leq i \leq t$, $d_i \sim c_i$ et $r = s$.

Proposition 2.3.4
Soir $\mathbb{A}$ un anneau principal.
Soient E et F deux $\mathbb{A}$–modules libres de rangs (finis) respectifs p et n.
Soit $u \in \mathrm{Hom}_{\mathbb{A}}(E, F)$.
Alors il existe une base $\mathcal{B}$ de E et une base $\mathcal{B}'$ de F telles que $\mathrm{mat}_{\mathcal{B},\mathcal{B}'}(u)$ soit une matrice de Smith, i.e telles que $\mathrm{mat}_{\mathcal{B},\mathcal{B}'}(u) = \mathrm{diag}_{n,p}(d_1, \dots d_r)$ avec les idéaux $(d_1) \supset \dots \supset (d_r)$ ne dépendanr que de u.
De plus :

(i) *u est injective $\Leftrightarrow r = p$;*

(i) *u est surjective $\Leftrightarrow r = n$ et $\forall 1 \leq i \leq n$, $d_i \in \mathbb{A}^{\times}$.*

2.4 Modules de type fini

Dans tout ce paragraphe, $\mathbb{A}$ désigne un anneau (commutatif).

Définition 2.4.1 (Module de type fini)
Un $\mathbb{A}$–module est dit de type fini s'il admet une partie génératrice finie.

Remarques :

1. Tout quotient d'un module de type fini est de type fini.
2. Sur un corps $\mathbb{K}$, les notions de module de type fini et d'espace vectoriel de dimension finie coïncident.
3. ✘ Les sous–modules d'un module de type fini ne sont ***pas*** nécessairement de type fini.

Proposition 2.4.1
Soient M et N deux $\mathbb{A}$–modules.
Alors :

(i) *M et N sont de type fini $\Leftrightarrow M \times N$ est de type fini ;*

(ii) *M est de type fini $\Leftrightarrow$ il existe $n \in \mathbb{N}$ tel que M soit isomorphe à un quotient de $\mathbb{A}^n$;*

(iii) *Si N est un sous–module de M tel que N et M/N soient de type fini, alors M est de type fini.*

Proposition 2.4.2
Soit $\mathbb{A}$ un anneau principal.
Soit E un $\mathbb{A}$–module libre de rang fini n.
Alors tout sous–module de E est libre de rang inférieur ou égal à n (et donc fini).

Démonstration : On peut supposer sans perdre de généralité que $E = \mathbb{A}^n$. On démontre ensuite la proposition par récurrence sur n.

- Si $n = 0$, le résultat est trivial.
- Si $n = 1$, un sous–$\mathbb{A}$–module de $\mathbb{A}$ (i.e un idéal de cet anneau) est soit trivial (donc de rang 0), soit engendré par un élément de $\mathbb{A}^*$ et donc isomorphe à $\mathbb{A}$ donc de rang 1.
- Si on suppose la propriété vraie au rang $n - 1 \geq 0$ et que l'on se donne un sous–module F de $\mathbb{A}^n$, alors on peut définir une application $p \in \mathrm{Hom}_{\mathbb{A}}(F, \mathbb{A})$ via $(x_i)_i \mapsto x_n$. $\mathrm{Im}(p)$ est alors un sous–module de $\mathbb{A}$ donc libre de rang inférieur ou égal à 1. De même, $\mathrm{Ker}(p)$ est un sous–module de $\mathbb{A}^{n-1} \times \{0\} \cong \mathbb{A}^{n-1}$ donc est libre de rang inférieur ou égal à $n - 1$. Comme $\mathrm{Im}(p)$ est libre, on a alors $F \cong \mathrm{Im}(p) \oplus \mathrm{Ker}(p)$, ce qui implique que F est libre de rang au pus n.

✌ On peut démontrer que tout sous–module d'un $\mathbb{A}$–module libre l'est, sans l'hypothèse de rang fini.

Corollaire 2.4.2.1
Soit $\mathbb{A}$ un anneau principal.
Alors tout sous–module d'un $\mathbb{A}$–module de type fini est de type fini.

Proposition 2.4.3 (Théorème de la base adaptée)
Soit $\mathbb{A}$ un anneau principal.
Soit M un $\mathbb{A}$–module libre de rang fini n.
Soit N un sous–module de M.
Alors il existe une base $(e_i)_{1\leq i\leq n}$ de M, un entier $r \leq n$ et $d_1, \ldots, d_r \in \mathbb{A}^*$ tels que :

(i) $\forall 1 \leq i \leq r-1,\ d_i | d_{i+1}$;

(ii) la famille $(d_i e_i)_{1\leq i\leq r}$ constitue une base de N.

De plus, la suite d'idéaux $(d_1) \supset \ldots \supset (d_r)$ ne dépend que de M et N (et pas de la base $(e_i)_i$).

✌ Sur un corps, on peut prendre tous les d_i égaux à 1.
DÉMONSTRATION : On applique la proposition 2.3.3 à l'inclusion $j : N \hookrightarrow M$. Ainsi, comme N est libre de rang $p-1 \leq n$, il existe une base $\underline{\varepsilon} = (\varepsilon_2, \ldots, \varepsilon_p)$ de N et une base $\underline{e} = (e_1, \ldots, e_n)$ de M et $d_1, \ldots, d_r \in \mathbb{A}^*$ tels que $\forall 1 \leq i \leq r$, $d_i | d_{i+1}$ et que $\mathrm{mat}_{\underline{\varepsilon},\underline{e}}(j) = \mathrm{diag}_{n,p}(d_1, \ldots, d_r)$. Comme de plus j est une injection, $r = p$ et donc $\underline{\varepsilon}$ est une base de N. Or, pour tout i, $j(\varepsilon_i) = d_i e_i$, d'où l'existence. L'indépendance de la suite $((d_i)_i$ de la base $\underline{e}$ est laissée en exercice.

☞ On a alors :

$$M/N \cong \left(\bigoplus_{i=1}^{r} \mathbb{A}/(d_i)\right) \oplus \mathbb{A}^{n-r}$$

Corollaire 2.4.3.1 (Facteurs invariants d'un module sur un anneau principal)
Soit $\mathbb{A}$ un anneau principal.
Soit M un $\mathbb{A}$–module de type fini.
Alors il existe $n \in \mathbb{N}$ et $d_1, \ldots, d_n \in \mathbb{A}$ tels que :

(i) $\forall 1 \leq i \leq n$, $d_i \notin \mathbb{A}^\times$ *(les d_i peuvent être nuls) ;*

(ii) $\forall 1 \leq i \leq n-1$, $d_i | d_{i+1}$;

(iii)

$$M \cong \bigoplus_{i=1}^{n} \mathbb{A}/(d_i)$$

Il y a de plus unicité au sens suivant : n et la suite d'idéaux $(d_1) \supset \ldots \supset (d_n)$ ne dépend que de M.

Dans ce cadre, quitte à réordonner les d_i de telle sorte que si $s := \mathrm{card}\{i \,|\, d_i \neq 0\}$ et si $r := n-s$ on ait $d_1, \ldots, d_r \neq 0$ et $\forall i > r$, $d_i = 0$, on a, comme $\mathbb{A}/\{0\} \cong \mathbb{A}$:

$$M \cong \mathbb{A}/(d_1) \oplus \ldots \oplus \mathbb{A}/(d_s) \oplus \mathbb{A}^r$$

Les éléments $d_1, \ldots, d_s$ sont appelés *facteurs invariants* du module M, et r est le cardinal de toute famille libre maximale de M.

Définition 2.4.2 (Torsion)
Soit $\mathbb{A}$ un anneau intègre.
Soit M un $\mathbb{A}$–module.
Alors :

(i) un élément $x \in M$ est dit de torsion si (x) n'est pas libre, i.e si :

$$\mathrm{Ann}(x) := \{a \in \mathbb{A} \,|\, ax = 0\} \neq \{0\}$$

(ii) l'ensemble des éléments de torsion de M est un sous–module de M, appelé sous–module de torsion de M et noté $T(M)$;

(iii) M est dit de torsion (resp. sans torsion) si $M = T(M)$ (resp. $T(M) = \{0\}$).

✍ Si $\mathbb{A}$ un anneau principal, on peut alors écrire :

$$M \cong \mathbb{A}/(d_1) \oplus \ldots \oplus \mathbb{A}/(d_s) \oplus \mathbb{A}^r$$

Avec la suite $((d_i))_i$ décroissante et sans terme nul ou égal à $\mathbb{A}$. On a de fait :

$$T(M) \cong \mathbb{A}/(d_1) \oplus \ldots \oplus \mathbb{A}/(d_s) \oplus \{0\}$$

Et ainsi :

$$\mathrm{Ann}(T(M)) = (d_s)$$

D'où :

$$M/T(M) \cong \mathbb{A}^r \text{ est libre de rang } r.$$

On en déduit la proposition suivante :

Proposition 2.4.4
Soit $\mathbb{A}$ un anneau principal.
Alors tout $\mathbb{A}$–module de type fini sans torsion est libre.

Exemples :

1. $\mathbb{Q}$ est un $\mathbb{Z}$–module sans torsion non libre et ne peut donc pas être de type fini.
2. $\mathbb{Z}[X]$ est un $\mathbb{Z}$–module libre sans torsion.
3. $(2, X)$ est un $\mathbb{Z}[X]$–module sans torsion, de type fini, mais non libre car $\mathbb{Z}[X]$ est non principal.

Décomposition primaire : Soit $\mathbb{A}$ un anneau principal et soit M un $\mathbb{A}$–module de type fini et de torsion. Alors on peut écrire $M \cong \mathbb{A}/(d_1) \oplus \ldots \oplus \mathbb{A}/(d_s)$ avec la suite $((d_i))_i$ décroissante et sans terme nul ou égal à $\mathbb{A}$.

Donnons nous un système représentatif Σ des irréductibles de $\mathbb{A}$. Alors, par factorialité de $\mathbb{A}$, il existe pour tout $1 \leq i \leq s$ un $\varepsilon_i \in \mathbb{A}^\times$ tel que :

$$d_i = \varepsilon_i \prod_{p \in \Sigma} p^{e_p(d_i)}$$

Ainsi, d'après le lemme chinois :

$$\mathbb{A}/(d_i) \cong \bigoplus_{p \in \Sigma} \mathbb{A}/(p^{e_p(d_i)}), \text{ les } \mathbb{A}/(p^{e_p(d_i)}) \text{ étant presque tous nuls.}$$

En regroupant, on obtient que :

$$M \cong \bigoplus_{p \in \Sigma} M_p \tag{2.1}$$

Où les M_p sont des sommes directes finies de $\mathbb{A}$–modules de la forme $\mathbb{A}/(p^{\text{truc}})$. Pour $p \in \Sigma$, M_p est appelé *composante p–primaire de M*. Par définition, il existe un $N \geq 1$ tel que $M_p = \mathrm{Ker}((x \in M) \mapsto x.p^N)$.

Exemple : On considère le $\mathbb{Z}$–module $M = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/45\mathbb{Z}$. On a alors, par lemme chinois :

$$M \cong \mathbb{Z}/8\mathbb{Z} \oplus (\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z})$$

Ainsi, en prenant comme système représentatif des irréductibles l'ensemble des nombres premiers positifs on a $M_2 \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, $M_3 \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$, $M_5 \cong \mathbb{Z}/5\mathbb{Z}$ et $M_p = \{0\}$ si p est premier strictement supérieur à 5.

En réordonnant, on trouve que les facteurs invariants de M sont 12 et 360. Ainsi :

$$M \cong \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/360\mathbb{Z}$$

2.5 Groupes abéliens de type fini

Proposition 2.5.1 (Théorème de structure des groupes abéliens de type fini)
Soit G un groupe abélien de type fini.
Alors il existe un unique $r \in \mathbb{N}$, appelé rang de G et une unique suite $(d_1, \dots d_s)$ d'entiers supérieurs ou égaux à 2 tels que :

(i) $\forall 1 \leq i \leq s-1,\ d_i | d_{i+1}$;

(ii)

$$G \cong \left(\bigoplus_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z} \right) \oplus \mathbb{Z}^r$$

☞ Ainsi G est fini si et seulement si son rang est nul.

2.6 Endomorphismes d'un espace vectoriel de dimension finie

Soit $\mathbb{A}$ un anneau (commutatif) et soit E un $\mathbb{A}[X]$–module. E est alors naturellement muni d'une structure de $\mathbb{A}$–module et $u : (\alpha \in \mathbb{A}) \mapsto \alpha X$ est $\mathbb{A}$–linéaire.

Réciproquement, si E est un $\mathbb{A}$–module et $u \in \mathrm{End}_{\mathbb{A}}(E)$, on peut munir E d'une structure de $\mathbb{A}[X]$–module via :

$$\begin{aligned} \mathbb{A}[X] \times E &\to E \\ (P, e) &\mapsto P.e := \underbrace{P(u)}_{\in \mathrm{End}_{\mathbb{A}}(E)} (e) \end{aligned}$$

En particulier, si $\lambda, e \in \mathbb{A}$ on a $\lambda.e = \lambda \times e$ et $X.e = u(e)$.

Ainsi, l'ensemble des $\mathbb{A}[X]$–modules est isomorphe [1] à l'ensemble des couples (E, u), où E est un $\mathbb{A}$–module et $u \in \mathrm{End}_{\mathbb{A}}(E)$. De fait, on se permettra à l'avenir de noter E_u le $\mathbb{A}[X]$–module associé au $\mathbb{A}$–module E et à l'endomorphisme u.

De plus, étant donnés deux couples (E, u) et (F, v) composés d'un $\mathbb{A}$–module et d'un endomorphisme de celui–ci et une application $f : E \to F$, alors f est $\mathbb{A}[X]$–linéaire de E_u dans F_v si et seulement si elle est $\mathbb{A}$–linéaire et vérifie $v \circ f = f \circ u$.

En particulier,

$$\mathrm{End}_{\mathbb{A}[X]}(E_u) = \{f \in \mathrm{End}_{\mathbb{A}}(E) \,|\, u \circ f = f \circ u\}$$

Remarquons en outre qu'un sous–$\mathbb{A}[X]$–module de E_u est un sous–$\mathbb{A}$–module de E stable par u.

Cas particulier : Soit $\lambda \in \mathbb{A}$. On considère $u \in End_{\mathbb{A}}(\mathbb{A})$ définit par $a \mapsto \lambda a$. Ainsi $\mathbb{A}$ est muni d'une structure de $\mathbb{A}[X]$–module $\mathbb{A}_u$ via :

$$\forall (P, t) \in \mathbb{A}[X] \times \mathbb{A},\ P.t := P(\lambda) \times t$$

On obtient ainsi une application $\mathbb{A}[X]$–linéaire :

$$\begin{aligned} \mathbb{A}[X] &\to \mathbb{A} \\ P &\mapsto P(\lambda).1_{\mathbb{A}} = P(\lambda) \end{aligned}$$

Cette application est surjective et de noyau $(X - \lambda)\mathbb{A}[X]$ donc induit un isomorphisme de $\mathbb{A}[X]$–modules :

$$\mathbb{A}[X]/(X - \lambda) \cong \mathbb{A}_u$$

$\boxed{\text{Dans la suite, } \mathbb{K} \text{ est un corps. Ainsi } \mathbb{K}[X] \text{ est principal.}}$

1. Via l'application qui à un $\mathbb{A}[X]$–module E fait correspondre le $\mathbb{A}$–module sous–jacent et la multiplication par X.

Soit E_u un $\mathbb{K}[X]$–module, i.e un $\mathbb{K}$–e.v E muni d'un endomorphisme u. Alors, pour $v \in E$, on peut définir une application $\mathbb{K}[X]$–linéaire :

$$\begin{aligned} \varphi_v : \mathbb{K}[X] &\to E_u \\ P &\mapsto P.v = P(u)(v) \end{aligned}$$

Ainsi, si $\lambda \in \mathbb{K}$ et $v \in E$, on a :

$$\begin{aligned} u(v) = \lambda v &\Leftrightarrow (u - \lambda \mathrm{id}_E) = 0 \\ &\Leftrightarrow (X - \lambda).v = 0 \\ &\Leftrightarrow \varphi_v(X - \lambda) = 0 \\ &\Leftrightarrow \varphi_v \text{ passe au quotient en } \overline{\varphi_v} : \mathbb{K}[X]/(X - \lambda) \text{ envoyant la classe de 1 sur } v. \end{aligned}$$

En conclusion, on a un isomorphisme :

$$\mathrm{Ker}(u - \lambda \mathrm{id}_E) \cong \mathrm{Hom}_{\mathbb{K}[X]}(D_\lambda, E_u)$$

Où $D_\lambda := (X - \lambda) \subset \mathbb{K}[X]$.

En particulier :

- λ est valeur propre de u si et seulement si $\mathrm{Hom}_{\mathbb{K}[X]}(D_\lambda, E_u) \neq \{0\}$;
- si E est de dimension finie, u est diagonalisable de valeurs propres (comptées avec leur ordre de multiplicité) $\lambda_1, \ldots, \lambda_n$ si et seulement si :

$$E_u \cong \bigoplus_{i=1}^{n} D_{\lambda_i}$$

Ainsi, les D_λ sont (à isomorphisme près) tous les $\mathbb{K}[X]$–modules qui sont de dimension 1 sur $\mathbb{K}$.

Définition 2.6.1 (Module cyclique)
Un $\mathbb{K}[X]$–module M est dit cyclique si il existe $P \in \mathbb{K}[X] \setminus \{0\}$ tel que :

$$M \cong \mathbb{K}[X]/(P)$$

☞ M est donc cyclique si et seulement si il est de torsion et engendré par un unique élément.

Remarques :

1. Si $P \in \mathbb{K}[X]$ est de degré $n \neq -\infty$, alors, si on note x la classe de X modulo P, $\mathbb{K}[X]/(P)$ admet $(1, x, \ldots, x^{n-1})$ comme $\mathbb{K}$-base. En particulier $\dim_{\mathbb{K}} (\mathbb{K}[X]/(P)) = n$.
2. On peut toujours prendre P unitaire. Il est alors totalement déterminé par le $\mathbb{K}[X]$–module $\mathbb{K}[X]/(P)$.

Lemme 2.6.1
Soient V un $\mathbb{K}$–e.v.
Soit $u \in \mathrm{End}_{\mathbb{K}}(V)$.
On a alors équivalence entre les propriétés suivantes :

(i) V_u est un $\mathbb{K}[X]$–module cyclique ;
(ii) il existe $v \in V$ et $n \in \mathbb{N}$ tels que $(v, u(v), \ldots, u^{n-1}(v))$ soit une $\mathbb{K}$–base de V ;
(iii) il existe $v \in V$ et $n \in \mathbb{N}$ tels que $(v, u(v), \ldots, u^{n-1}(v))$ engendre V (comme $\mathbb{K}$–e.v).

Lemme 2.6.2
Soient V un $\mathbb{K}$–e.v.
Soit $u \in \mathrm{End}_{\mathbb{K}}(V)$.
On a alors équivalence entre les propriétés suivantes :

(i) V est de dimension finie ;
(ii) V_u est un $\mathbb{K}[X]$–module de type fini et de torsion.

Définition 2.6.2 (Matrice compagnon)
Soit $P = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ un polynôme unitaire de $\mathbb{K}[X]$.
Alors on appelle matrice compagnon de P la matrice :

$$C_p := \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Proposition 2.6.1
Soit P un polynôme unitaire de $\mathbb{K}[X]$.
Alors :

(i) P est le polynôme minimal de C_p ;

(ii) $(-1)^n P$ est le polynôme caractéristique de C_p.

Proposition 2.6.2
Soit V un $\mathbb{K}$−e.v de dimension finie.
Soit $u \in \mathrm{End}_{\mathbb{K}}(V)$.
Alors il existe une unique suite finie $(P_1, \ldots, P_r)$ de polynômes unitaires non constants dans $\mathbb{K}[X]$ telle que :

(i) $\forall 1 \leq i \leq r-1,\ P_i | P_{i+1}$ dans $\mathbb{K}[X]$;

(ii) dans une base convenable de V la matrice de u est diagonale par blocs de la forme :

$$\mathrm{diag}(C_1, \ldots, C_r) := \begin{pmatrix} C_{P_1} & (0) & \ldots & (0) \\ (0) & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & (0) \\ (0) & \ldots & (0) & C_{P_r} \end{pmatrix}$$

Remarques :

1. $P_1, \ldots, P_r$ sont appelés facteurs invariants de u. On définit les facteurs invariants d'une matrice comme étant ceux de son endomorphisme canoniquement associé.
2. Le polynôme minimal de u est P_r.
3. Le polynôme caractéristique de u est $\pm \prod_{i=1}^{r} P_i$.
4. Les matrices C_{P_i} ne sont presque jamais diagonales : si u est diagonalisable, le théorème ne donne pas la "bonne" réduction.

Corollaire 2.6.2.1
Soient $U, U' \in \mathcal{M}_n(\mathbb{K})$.
Alors :

$$U \text{ et } U' \text{ sont semblables} \Leftrightarrow U \text{ et } U' \text{ ont les mêmes facteurs invariants.}$$

DÉMONSTRATION : D'après le théorème précédent, $(\mathbb{K}^n)_u$ et $(\mathbb{K}^n)_{u'}$ sont isomorphes si et seulement si U et U' ont les mêmes facteurs invariants (où u et u' sont les endomorphismes canoniquement associés à U et U'. Or la première condition est équivalente à la similitude U et U'.

Corollaire 2.6.2.2
Soit $k \subset \mathbb{K}$ un corps.
Soit $A \in \mathcal{M}_n(k)$ de facteurs invariants $P_1, \ldots, P_r$.
Alors $P_1, \ldots, P_r$ sont les facteurs invariants de A dans $\mathcal{M}_n(\mathbb{K})$.

Corollaire 2.6.2.3
Soit $k \subset \mathbb{K}$ un corps.
Soit $A \in \mathcal{M}_n(\mathbb{K})$.
Alors A est semblable à une matrice à coefficients dans k si et seulement si ses facteurs invariants sont des éléments de $k[X]$.

Exemple : Le $\mathbb{K}[X]$–module associé à $M := \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ (les $\lambda_i \in \mathbb{K}$ deux à deux distincts) est :

$$\bigoplus_{i=1}^{n} P_{\lambda_i} = \mathbb{K}[X] / \left(\prod_{i=1}^{n} (X - \lambda_i) \right)$$

En effet, les $X - \lambda_i$ sont premiers entre eux donc M a pour unique facteur invariant $\prod_{i=1}^{n}(X - \lambda_i)$.

Dans le cas $n = 2$, le théorème précédent donne la matrice :

$$\begin{pmatrix} 0 & -\lambda_1\lambda_2 \\ 1 & \lambda_1 + \lambda_2 \end{pmatrix}$$

Pour $n \geq 1$ et $\lambda \in \mathbb{K}$, on pose :

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \ldots & \ldots & 0 & \lambda \end{pmatrix}$$

$J_n(\lambda)$ est appelé *bloc de Jordan* de taille n et de valeur propre λ. On remarque de plus que :

$$J_n(\lambda) = \lambda I_n + J_n(0)$$

$J_n(0)$ correspond à l'endomorphisme de $\mathbb{K}^n$ défini comme suit (si $(e_i)_{1 \leq i \leq n}$ est la base canonique de $\mathbb{K}^n$) :

$$e_n \mapsto e_{n-1} \mapsto \ldots \mapsto e_1 \mapsto 0$$

En particulier, $J_n(0)^n = 0$ et $J_n(0)^{n-1} \neq 0$, d'où :

$$\mathbb{K}[X]/(X - \lambda) \cong (\mathbb{K}^n)_{J_n(\lambda)}$$

Remarquez que l'on a ici (honteusement) identifié matrice et endomorphisme canoniquement associé.

Proposition 2.6.3 (Décomposition de Jordan)
Soit $\mathbb{K}$ un corps algébriquement clos.
Soit V un $\mathbb{K}$-e.v de dimension finie.
Soit $u \in \mathrm{End}_{\mathbb{K}}(V)$.
Alors :

(i) il existe une base $\mathcal{B}$ de V dans laquelle la matrice de u est de la forme $J = \mathrm{diag}(B_1, \ldots, B_r)$, où chaque B_i est un bloc de Jordan $J_{n_i}(\lambda_i)$;

(ii) J ne dépend pas (à permutation des blocs près) de la base $\mathcal{B}$.

Corollaire 2.6.3.1
Soit $\mathbb{K}$ un corps algébriquement clos.
Soit V un $\mathbb{K}$-e.v de dimension finie.
Soient $u, v \in \mathrm{End}_{\mathbb{K}}(V)$.
Alors u est semblable à v si et seulement si u et v ont les mêmes blocs de Jordan (à permutation près).

Chapitre 3

Extensions de corps

3.1 Algèbres

Dans tout ce paragraphe, $\mathbb{A}$ désigne un anneau commutatif.

Définition 3.1.1 (Algèbre)
Une $\mathbb{A}$–algèbre est un couple $(\mathcal{A}, j)$ où :

(i) $\mathcal{A}$ est un anneau ;

(ii) $j : \mathbb{A} \to \mathcal{A}$ est un morphisme d'anneaux (appelé morphisme structurel) central, i.e tel que :

$$\forall \lambda \in \mathbb{A},\ \forall x \in \mathcal{A},\ j(\lambda)x = xj(\lambda)$$

✘ On rencontre parfois, au détour d'une ruelle sombre, des "algèbres non–associatives", telles les algèbres de Lie [1]. Elles ne rentrent pas dans le cadre de ce cours.

Exemples :

1. Tout anneau est doté (de façon unique) d'une structure de $\mathbb{Z}$–algèbre via le (ii) de la proposition 1.3.1.
2. $(\mathbb{A}, \mathrm{id}_{\mathbb{A}})$ est une $\mathbb{A}$–algèbre.
3. $\{0\}$ est muni (via le (i) de la proposition 1.3.1) d'une unique structure de $\mathbb{A}$–algèbre, appelée algèbre triviale.
4. La seule $\{0\}$–algèbre est l'algèbre triviale.
5. $\mathbb{A}[X]$ est muni d'une structure de $\mathbb{A}$–algèbre via :

$$\begin{aligned} j : \mathbb{A} &\to \mathbb{A}[X] \\ \lambda &\mapsto \lambda.1_{\mathbb{A}[X]} \end{aligned}$$

6. *Exemple non commutatif.* Soit E un $\mathbb{A}$–module et soit $\mathcal{A} := \mathrm{End}_{\mathbb{A}}(E)$. Alors on peut munir $\mathcal{A}$ d'une structure de $\mathbb{A}$–algèbre via :

$$\begin{aligned} j : \mathbb{A} &\to \mathcal{A} \\ \lambda &\mapsto ((x \in E) \mapsto (\lambda x \in E)) \end{aligned}$$

Définition 3.1.2 (Morphisme d'algèbres)
Soient $(\mathcal{A}, j)$ et $(\mathcal{A}', j')$ deux $\mathbb{A}$–algèbres.
On appelle morphisme d'algèbres tout morphisme d'anneaux $\varphi : \mathcal{A} \to \mathcal{A}'$ tel que :

$$\varphi \circ j = j'$$

✌ N'est-ce pas magnifique ? Je dis que cela se fête. Avec un diagramme commutatif par exemple :

1. Ces algèbres ne sont même pas unitaires, pensez donc !

$$\begin{tikzcd}
\mathbb{A} \arrow[r, "j'"] \arrow[d, "j"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathcal{A}' \\
\mathcal{A} \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

Proposition 3.1.1
Tout anneau quotient d'une $\mathbb{A}$–algèbre est une $\mathbb{A}$–algèbre.

Proposition 3.1.2
Tout produit (même infini) de $\mathbb{A}$–algèbres est une $\mathbb{A}$–algèbre.

Définition 3.1.3 (Sous–algèbre)
Soit $(\mathcal{A}, j)$ une $\mathbb{A}$–algèbre.
Soit $\mathcal{B} \subset \mathcal{A}$.
Alors on dit que $(\mathcal{B}, j_{|\mathcal{B}})$ est une sous–algèbre de $\mathcal{A}$ si :

(i) $\mathcal{B}$ est un sous–anneau de $\mathcal{A}$;

(ii) $j(\mathbb{A}) \subset \mathcal{B}$.

Proposition 3.1.3 (Sous–algèbre engendrée par une partie)
Toute intersection de sous–algèbre d'une de $\mathbb{A}$–algèbre donnée $\mathcal{A}$ est une sous–algèbre de $\mathcal{A}$. Par conséquent, on peut définir la sous–algèbre engendrée par une partie $S \subset \mathcal{A}$ comme étant l'intersection de toutes les sous–algèbres de $\mathcal{A}$ contenant S. C'est alors la plus petite sous–algèbre vérifiant cette propriété, et on la note $\mathbb{K}[S]$.

✍ On peut montrer que la sous–algèbre engendrée par S est le sous–anneau de $\mathcal{A}$ engendré par $j(\mathbb{A}) \cup S$.

Proposition 3.1.4 (Correspondance algèbre–module)

(i) Soit $(\mathcal{A}, j)$ une $\mathbb{A}$–algèbre. Alors $\mathcal{A}$ est munie d'une structure de $\mathbb{A}$–module via la multiplication externe définie par :

$$\forall (\lambda, y) \in \mathbb{A} \times \mathcal{A},\ \lambda . y := j(\lambda) \times y$$

La condition de centralité sur j entraîne que la multiplication interne *de $\mathcal{A}$ est bilinéaire.*

(ii) Inversement, si $\mathcal{A}$ est un $\mathbb{A}$–module muni d'une structure d'anneau avec la "même" addition[2] *que $\mathbb{A}$ et une multiplication bilinéaire, alors il est muni d'une structure de $\mathbb{A}$–algèbre via :*

$$\begin{aligned} j : \mathbb{A} &\to \mathcal{A} \\ \lambda &\mapsto \lambda . 1_{\mathbb{A}} \end{aligned}$$

De plus, ces deux constructions sont réciproques l'une de l'autre, ce qui induit une bijection entre l'ensemble des $\mathbb{A}$–algèbres et celui des $\mathbb{A}$–modules dotés d'une addition qui se respecte et d'une multiplication bilinéaire.

✍ De fait, dans les cas où nous estimerons que nulle confusion n'est possible, nous ne denoterons une $\mathbb{A}$–algèbre $(\mathcal{A}, j)$ que par la donnée de $\mathcal{A}$ et écrirons "λ" à la place de $j(\lambda)$. Notez qu'il serais assez inconscient, voire préoccupant sur le plan clinique, d'envisager d'utiliser cette dernière notation en cas de non–injectivité de j. On identifie ainsi $\mathbb{A}$ et $\mathrm{Im}(j) \subset \mathcal{A}$. Notons que dans le cas particulier où l'on s'intéresse à une algèbre $(\mathcal{A}, j)$ sur un corps $\mathbb{K}$, l'application j est automatiquement injective (car $\mathrm{Ker}(j)$ est un idéal de $\mathbb{K}$) et que l'on peut donc toujours voir $\mathbb{K}$ comme un sous–corps de $\mathcal{A}$.

2. I.e dont l'addition n'est pas définie de façon abjecte mais directement à l'aide de celle de $\mathbb{A}$ "coordonnée par coordonnée".

3.2 Algèbres de polynômes

Dans tout ce paragraphe, $\mathbb{A}$ désigne un anneau commutatif.
On part d'un ensemble I indexant une famille "d'indéterminées" X_i.

Définition 3.2.1 (Monôme en les X_i)
Formellement, on appelle monôme en les X_i une expression de la forme :

$$\underline{X}^{\underline{n}} := \prod_{i\in I} X_i^{n_i}$$

Où $\underline{n} = (n_i)_{i\in I} \in \mathbb{N}^{(I)}$.

On peut alors munir d'une multiplication évidente l'ensemble $\mathcal{M}_I$ des monômes en les X_i, ce qui nous livre un monoïde commutatif :

$$(\mathcal{M}_I, \times) \cong (\mathbb{N}^{(I)}, +) \text{ via } \prod_{i\in I} X_i^{n_i} \mapsto (n_i)_i$$

Définition 3.2.2 (Polynôme à I indéterminées)
On appelle polynôme à I indéterminées à coefficients dans $\mathbb{A}$ toute combinaison linéaire finie à coefficients dans $\mathbb{A}$ de monômes en les X_i.

L'ensemble des polynômes à I indéterminées à coefficients dans $\mathbb{A}$ est noté $\mathbb{A}[(X_i)_{i\in I}]$ ou $\mathbb{A}[I]$. Remarquons qu'il s'agit par construction du $\mathbb{A}$–module libre standard de base $\mathcal{M}_I$ (ou $\mathbb{N}^{(I)}$) $\mathbb{A}^{(\mathcal{M}_I)}$. Cet ensemble admet une multiplication $\mathbb{A}$–bilinéaire obtenue en prolongeant le produit défini précédemment sur les monômes. On peut donc munir $\mathbb{A}[I]$ d'une structure de $\mathbb{A}$–algèbre.

✘ Un polynôme donné ne fait intervenir qu'un nombre *fini* d'indéterminées. Autrement dit :

$$\mathbb{A}[I] = \bigcup_{J\subset I,\, \mathrm{card}(J)<\infty} \mathbb{A}[J]$$

Exemple : Plaçons nous dans le cas $I = \mathbb{N}$. Alors :

$$\mathbb{A}[(X_n)_{n\in\mathbb{N}}] = \bigcup_{n\in\mathbb{N}} \mathbb{A}[X_0, \dots, X_n]$$

Avec $\mathbb{A}[X_0] \subset \mathbb{A}[X_0, X_1] \subset \dots$ Ainsi $\mathbb{A}[(X_n)_{n\in\mathbb{N}}]$ contient les polynômes $X_0, X_0X_1, \dots, X_0X_1X_2\dots X_n, \dots$ mais les expressions suivantes n'y ont *aucun sens* :

$$\prod_{n=0}^{\infty} X_n \text{ et } \sum_{n=0}^{\infty} X_n$$

Soient à présent $\underline{\alpha} = (\alpha_i)_i \in \mathbb{A}^I$ et $P \in \mathbb{A}[I]$. On peut alors définir *l'évaluation de P en $\underline{\alpha}$*, notée $P(\underline{\alpha}) \in \mathbb{A}$ de la façon suivante :

$$\text{si } P = \sum_{\underline{n}\in\mathbb{N}^{(I)}} \lambda_{\underline{n}} \underline{X}^{\underline{n}}, \text{ on pose } P(\underline{\alpha}) := \sum_{\underline{n}\in\mathbb{N}^{(I)}} \lambda_{\underline{n}} \underline{\alpha}^{\underline{n}}$$

Où les $\lambda_{\underline{n}}$ sont (par définition) presque tous nul et où :

$$\underline{\alpha}^{\underline{n}} = \prod_{i\in I} \alpha_i^{n_i}$$

Plus généralement, si $\mathcal{A}$ est une $\mathbb{A}$–algèbre et $\underline{\alpha} \in \mathcal{A}^I$, on peut définir une évaluation $P(\underline{\alpha}) \in \mathcal{A}$ par la même formule ***si*** les α_i commutent.

Proposition 3.2.1 (Propriété universelle des algèbres de polynômes)
Soit $\mathcal{A}$ une $\mathbb{A}$–algèbre.
Soit $\underline{\alpha} \in \mathcal{A}^I$ tel que les α_i commutent.
Alors l'application suivante est un morphisme de $\mathbb{A}$–algèbres, appelé morphisme d'évaluation :

$$\begin{aligned} ev_{\underline{\alpha}} : \mathbb{A}[I] &\to \mathcal{A} \\ P &\mapsto P(\underline{\alpha}) \end{aligned}$$

Il s'agit en outre du seul morphisme entre ces deux algèbres qui envoie X_i sur α_i pour tout $i \in I$.

☞ Ainsi, l'ensemble des morphismes d'algèbres de $\mathbb{A}[I]$ dans $\mathcal{A}$, noté $\mathrm{Hom}_{\mathbb{A}\text{-alg}}(\mathbb{A}[I],\mathcal{A})$, est isomorphe à l'ensemble des $\underline{\alpha} \in \mathcal{A}^I$ tels que les α_i commutent via $\varphi \mapsto (\varphi(X_i))_{i\in I}$ et $\underline{\alpha} \mapsto ev_{\underline{\alpha}}$.

Remarques :

1. Dans les cas suivants la condition de commutation sur les α_i est automatiquement vérifiée.
   (a) Si $\mathrm{card}(I) = 1$. Dans ce cas :
   $$\mathrm{Hom}_{\mathbb{A}\text{-alg}}(\mathbb{A}[X],\mathcal{A}) \cong \mathcal{A}$$
   (b) Si $\mathcal{A}$ est commutative. Dans ce cas :
   $$\mathrm{Hom}_{\mathbb{A}\text{-alg}}(\mathbb{A}[I],\mathcal{A}) \cong \mathcal{A}^I$$
2. L'image de $ev_{\underline{\alpha}}$ est la sous–$\mathbb{A}$–algèbre de $\mathcal{A}$ engendrée par $\underline{\alpha}$.
3. Un polynôme $P \in \mathbb{A}[I]$ fixé détermine, si $\mathcal{A}$ est commutative, une application :
   $$\begin{aligned}\widehat{P} : \mathcal{A}^I &\to \mathcal{A}\\ \underline{\alpha} &\mapsto P(\underline{\alpha})\end{aligned}$$
   $\widehat{P}$ est appelée *fonction polynôme* définie par P. En particulier, si $\mathcal{A} = \mathbb{A}$ on obtient un morphisme d'algèbres :
   $$\begin{aligned}\mathbb{A}[I] &\to \mathbb{A}^{\mathbb{A}^I}\\ P &\mapsto \widehat{P}\end{aligned}$$
   ✗ Ce morphisme n'est en général ni injectif, ni surjectif.

3.3 Algèbres commutatives sur un corps, éléments algébriques

Dans tout ce paragraphe, $\mathbb{K}$ désigne un corps et $\mathcal{A}$ une $\mathbb{K}$–algèbre ***commutative***.

Soit $\underline{\alpha} = (\alpha_1,\ldots,\alpha_n) \in \mathcal{A}^n$. On note $\mathbb{K}[\alpha_1,\ldots,\alpha_n]$ (ou $\mathbb{K}[\underline{\alpha}]$) la sous–algèbre engendrée par les α_i, i.e l'image de l'application :

$$\begin{aligned}ev_{\underline{\alpha}} : \mathbb{K}[X_1,\ldots,X_n] &\to \mathcal{A}\\ P &\mapsto P(\underline{\alpha})\end{aligned}$$

Ainsi, l'ensemble $\mathbb{K}[\alpha_1,\ldots,\alpha_n]$ s'identifie à un quotient de $\mathbb{K}[X_1,\ldots,X_n]$.

✗ Il est important de ne pas confondre $\mathbb{K}[\underline{\alpha}]$ avec le s-ev $\langle\underline{\alpha}\rangle_{\mathbb{K}} \subset \mathcal{A}$. En effet :

$$\langle\underline{\alpha}\rangle_{\mathbb{K}} = \left\{ \sum_{i=1}^n \lambda_i\alpha_i \;\middle|\; (\lambda_i)_i \in \mathbb{K}^n \right\} \subset \mathbb{K}[\underline{\alpha}] = \{P(\underline{\alpha}) \,|\, P \in \mathbb{K}[X_1,\ldots,X_n]\}$$

Mais il n'y a en général pas égalité.

Définition 3.3.1 ($\mathbb{K}$–algèbre commutative de type fini)
On dit que $\mathcal{A}$ est de type fini si elle vérifie l'une des conditions équivalentes suivantes :
(i) il existe une partie finie *$S \subset \mathcal{A}$ qui engendre $\mathcal{A}$ comme $\mathbb{K}$–algèbre ;*
(ii) il existe un entier $n \in \mathbb{N}$ et un morphisme surjectif de $\mathbb{K}$–algèbre $\varphi : \mathbb{K}[X_1,\ldots,X_n] \to \mathcal{A}$.

Remarque :

1. Un $\mathbb{K}$–e.v de dimension finie est une $\mathbb{K}$–algèbre de type fini.
2. $\mathbb{K}[X]$ est une $\mathbb{K}$–algèbre de type fini, engendrée par $\{X\}$ mais est de dimension infinie comme $\mathbb{K}$–e.v.

Algèbres monogènes :
On se place dans le cas où $\mathcal{A} = \mathbb{K}[\alpha]$, avec $\alpha \in \mathcal{A}$. On a alors un morphisme surjectif :

$$\begin{aligned} ev_\alpha : \mathbb{K}[X] &\to \mathcal{A} \\ P &\mapsto P(\alpha) \end{aligned}$$

$\mathrm{Ker}(ev_\alpha)$ est alors engendré par un polynôme $P_0 \in \mathbb{K}[X]$ car $\mathbb{K}[X]$ est principal (car $\mathbb{K}$ est un corps). On distingue alors deux cas.

1. *Si* $P_0 = 0$. Alors ev_α est un isomorphisme donc $\dim_{\mathbb{K}} \mathbb{K}[\alpha] = \infty$.
2. *Si* $P_0 \neq 0$. On peut alors supposer que P_0 est unitaire. Alors :

$$\mathbb{K}[X]/(P_0) \cong \mathbb{K}[\alpha]$$

En particulier, si $d := \deg(P_0)$ la famille $(1, \overline{X}, \ldots, \overline{X}^{d-1})$ est une $\mathbb{K}$–base de $\mathbb{K}[X]/(P_0)$, ce qui entraîne que $(1, \alpha, \ldots, \alpha^{d-1})$ est une $\mathbb{K}$–base de $\mathbb{K}[\alpha]$. Ainsi $\dim_{\mathbb{K}} \mathbb{K}[\alpha] = \deg(P_0) < \infty$. P_0 est alors appelé *polynôme minimal* (unitaire) de α sur $\mathbb{K}$ et $\deg(P_0)$ se voit affubler du sobriquet fort surprenant de *degré* de α sur $\mathbb{K}$, noté $\deg_{\mathbb{K}}(\alpha)$.

Proposition 3.3.1 (Critère d'Eisenstein)
Soit $P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$.
Supposons qu'il existe un nombre premier p *tel que :*

(i) $\forall 0 \leq i \leq n-1,\ p | a_i$;
(ii) $p \nmid a_n$;
(iii) $p^2 \nmid a_0$.

Alors P *est irréductible dans* $\mathbb{Q}[X]$.

Définition 3.3.2 (Éléments algébriques, transcendants)
Soit $\alpha \in \mathcal{A}$.
Alors on dit que α *est . . .*

(i) . . . algébrique si ev_α *n'est pas injective, i.e si* $\exists P \in \mathbb{K}[X] \setminus \{0\}$ *tel que* $P(\alpha) = 0$ *;*
(ii) . . . transcendant dans le cas contraire.

Exemple : Si $\mathbb{K} = \mathbb{Q}$ et $\mathcal{A} = \mathbb{C}$, les éléments algébriques (resp. transcendants) sont appelés [3] *nombres algébriques* (resp. *nombres transcendants*).

1. i est algébrique de polynôme minimal $X^2 + 1$ donc de degré 2.
2. Si p est un nombre premier et $n \geq 1$, $\sqrt[n]{p}$ est algébrique de polynôme minimal $X^n - P$. En effet , ce polynôme est irréductible (par critère d'Eisenstein), unitaire et s'annule en p donc est son polynôme minimal.
3. Il existe des nombres transcendants. Les premiers exemples explicites en sont dus à Liouville ($\sum_{n\geq 0} \frac{1}{2^{n!}}$), Hermite ($e$, 1873) et Lindemann ($\pi$, 1882). De nombreux problèmes restent toutefois ouverts : on ne sait par exemple toujours pas à l'heure actuelle si $e + \pi$ est transcendant !

Proposition 3.3.2
Soient $\alpha_1, \ldots, \alpha_n \in \mathcal{A}$ *des éléments algébriques sur* $\mathbb{K}$.
Alors :

(i)
$$\dim_{\mathbb{K}} \mathbb{K}[\alpha_1, \ldots, \alpha_n] \leq \prod_{i=1}^{n} \deg_{\mathbb{K}}(\alpha_i)$$

(ii) tout élément de $\mathbb{K}[\alpha_1, \ldots, \alpha_n]$ *est algébrique sur* $\mathbb{K}$.

DÉMONSTRATION :

– Remarquons tout d'abord que (i) implique (ii). En effet, si on suppose (i) et que l'on se donne $a \in \mathbb{K}[\alpha_1, \ldots, \alpha_n]$, $\mathbb{K}[a]$ est une sous–algèbre de $\mathbb{K}[\alpha_1, \ldots, \alpha_n]$ donc est de dimension finie. Qui plus est, a est annulé par un polynôme de degré inférieur à $\prod_{i=1}^{n} \deg_{\mathbb{K}}(\alpha_i)$.

3. Surprise . . .

– Démontrons à présent le point (i). L'algèbre $\mathbb{K}[\alpha_1, \ldots, \alpha_n]$ est engendré *comme* $\mathbb{K}$*–e.v* par les monômes en les α_i. Si on pose, pour tout $1 \leq i \leq n$ $d_i := \deg_{\mathbb{K}}(\alpha_i)$, alors :

$$\mathbb{K}[\alpha_i] = \langle 1, \alpha_i, \ldots, \alpha_i^{d_i - 1} \rangle_{\mathbb{K}}$$

Ainsi, pour tout $m \in \mathbb{N}$, α_i^m est combinaison linéaire de la famille $(\langle 1, \alpha_i, \ldots, \alpha_i^{d_i-1})$. De facto, pour tout $\underline{m} = (m_1, \ldots, m_n) \in \mathbb{N}^n$, $\underline{\alpha}^{\underline{m}} := \prod_i \alpha_i^{m_i}$ est combinaison linéaire des $\prod_i \alpha_i^{e_i}$, avec les $e_i < d_i$, qui sont en nombre fini. D'où le résultat.

✍ Désormais, on dira qu'une $\mathbb{K}$–algèbre est de dimension finie si elle est de dimension finie *en tant que* $\mathbb{K}$*–e.v.*

Corollaire 3.3.2.1
L'ensemble $\mathcal{A}_0$ des éléments de $\mathcal{A}$ algébriques sur $\mathbb{K}$ est une sous algèbre de $\mathcal{A}$ qui est réunion de sous–algèbres de dimension finie de $\mathcal{A}$.

☞ En particulier, le produit et la somme de deux éléments algébriques est algébrique.
✗ $\mathcal{A}_0$ n'est pas nécessairement de dimension finie.
Démonstration : Soit $j : \mathbb{K} \to \mathcal{A}$ le morphisme structural. Alors, comme pour tout $\lambda \in \mathbb{K}$ $j(\lambda)$ est annulé par $X - \lambda$, $j(\mathbb{K}) \subset \mathcal{A}_0$. Il ne nous reste donc plus qu'à montrer que si $a, b \in \mathcal{A}_0$, $\mathbb{K}[a, b] \subset \mathcal{A}_0$. Or la proposition précédente, $\mathbb{K}[a, b]$ est un sous–espace de dimension finie de $\mathcal{A}_0$. $\mathcal{A}_0$ est donc bien une $\mathbb{K}$–algèbre, qui vérifie en outre que :

$$\mathcal{A}_0 = \bigcup_{\alpha \in \mathcal{A}_0} \mathbb{K}[\alpha]$$

Avec les $\mathbb{K}[\alpha]$ de dimension finie sur $\mathbb{K}$.

Proposition 3.3.3
Soit $\mathcal{B}$ une $\mathbb{K}$–algèbre (non nécessairement commutative) de dimension finie.
Alors tout élément régulier à gauche (par exemple) de $\mathcal{B}$ est inversible à droite et à gauche.
Par conséquent :

$$\begin{gathered} \mathcal{B} \textit{ est un anneau intègre} \\ \Leftrightarrow \\ \mathcal{B} \textit{ est un corps} \end{gathered}$$

Démonstration : Si $a \in \mathcal{B}$ est régulier à gauche, $x \mapsto ax \in \mathrm{End}_{\mathbb{K}}(\mathcal{B})$ et est injectif, donc bijectif car $\dim_{\mathbb{K}}(\mathcal{B}) < \infty$. D'où le résultat.

Remarque : Autrement dit, tout élément algébrique α non diviseur de zéro est inversible. Mieux[4] : on peut en expliciter l'inverse. En effet, si il existe $\lambda_0, \ldots \lambda_{d-1}$ tels que $\alpha^d + \lambda_{d-1}\alpha^{d-1} + \ldots + \lambda_0 = 0$, alors si $\lambda_0 = 0$, on peut factoriser par α puis simplifier, obtenant ainsi une relation de degré strictement inférieur à d : on peut donc supposer $\lambda_0 \in \mathbb{K}^* = \mathbb{K}^\times$. Ainsi :

$$\alpha^{-1} = -(\lambda_{d-1} + \lambda_{d-1}\alpha^{d-2} + \ldots + \lambda_1)\lambda_0^{-1}$$

Corollaire 3.3.3.1 (Fermetures algébriques d'un corps)
Si $\mathcal{A}$ est intègre, alors $\mathcal{A}_0$ est un corps, appelé fermeture algébrique de $\mathbb{K}$ dans $\mathcal{A}$.

Exemple : On se place dans le cas $\mathbb{K} = \mathbb{Q}$, $\mathcal{A} = \mathbb{R}$. $\mathcal{A}_0$ est alors l'ensemble des nombres algébriques réels et est donc un sur–corps de $\mathbb{Q}$. Cependant, $\dim_{\mathbb{K}}(\mathcal{A}_0) = \infty$ car pour tout $n \in \mathbb{N}^*$, $\mathcal{A}_0$ contient $\mathbb{Q}[\sqrt[n]{2}]$, qui est de dimension n car le polynôme minimal sur $\mathbb{Q}$ de $\sqrt[n]{2}$ est $X^n - 2$.

3.4 Généralités sur les extensions de corps

Définition 3.4.1 (Extension de corps)
Soit k un corps.
On appelle alors extension de k toute k–algèbre qui est un corps.

4. Enfin, cela dépend du point de vue ...

Remarques :

1. Si $\mathbb{K}$ est une extension d'un corps k, on a un morphisme structural $j : k \to \mathbb{K}$ qui est injectif car k est un corps et $\mathbb{K} \neq \{0\}$. De fait, $k \hookrightarrow \mathbb{K}$ et donc on identifiera en général k au sous–corps $j(k)$ de $\mathbb{K}$.
2. Si S est une partie d'une extension $\mathbb{K}$ d'un corps k, il existe une plus petite extension de k contenant S. On l'appelle (à la surprise générale) *extension engendrée par* S et on la note $k(S)$. Il s'agit de l'intersection de tous les sous–corps de $\mathbb{K}$ contenant $j(k)$ et S. De plus, $k(S)$ est l'ensemble de quotients de $k[S]$, i.e :
$$k(S) = \left\{ \frac{P(s_1, \ldots, s_n)}{Q(s_1, \ldots, s_n)} \;\middle|\; n \in \mathbb{N}^*,\, s_1, \ldots s_n \in S,\, P, Q \in k[X_1, \ldots, X_n],\, Q(s_1, \ldots, s_n) \neq 0 \right\}$$
De facto, $k(S)$ est également isomorphe au corps des fractions de $k[S]$.
3. Si S est une partie d'une extension $\mathbb{K}$ d'un corps k, l'extension $\mathbb{K}$ contient donc :
   (a) l'ensemble $\langle S \rangle_k$ des combinaison k–linéaires d'éléments de S ;
   (b) l'ensemble $k[S]$ des polynômes en les éléments de S ;
   (c) l'ensemble $k(S)$ des fractions rationnelles en les éléments de S.

   On a bien évidemment les inclusions suivantes :
$$\langle S \rangle_k \subset k[S] \subset k(S)$$
4. Si S est une partie d'une extension $\mathbb{K}$ d'un corps k telle que tous les éléments de S soient algébriques sur k, alors $k[S]$ est un corps et donc $k(S) = k[S]$.
5. $k(X)$ est bien l'extension de corps engendrée par $\{X\} \subset k[X]$. On a alors $k[X] \subsetneq k(X)$.

✍ Désormais, on notera (si nulle ambiguité n'est à craindre) $\mathbb{K}/k$ une extension $\mathbb{K}$ d'un corps k.

Définition 3.4.2 (Extensions algébrique, transcendante, finie, de type fini)
Soit $\mathbb{K}/k$ une extension de corps.
Alors $\mathbb{K}$ est dite :

(i) algébrique si ses éléments sont algébriques sur k ;

(ii) transcendante sinon ;

(iii) finie si $\dim_k \mathbb{K} < \infty$. On appelle alors degré de $\mathbb{K}$ sur k la quantité suivante :
$$[\mathbb{K} : k] := \dim_k \mathbb{K}$$

(iv) de type fini si elle est engendrée par une partie finie.

✗ Évitons de trop quotienter !
Nous avons vu que si $\mathbb{A}$ est un anneau commutatif, alors :

1. Un $\mathbb{A}$–module de type fini est isomorphe à un quotient d'un des $\mathbb{A}$–modules $\mathbb{A}^n$, $n \geq 1$;
2. Une $\mathbb{A}$–algèbre de type fini est isomorphe à un quotient d'une des $\mathbb{A}$–algèbres $\mathbb{A}[X_1, \ldots, X_n]$, $n \geq 1$.

Qu'on se le dise : IL N'EXISTE PAS D'ANALOGUE À CETTE PROPRIÉTÉ POUR LES EXTENSIONS DE TYPE FINI. En effet, le seuls anneaux quotients d'un corps sont $\{0\}$ et lui–même et ne présentent de fait qu'assez peu d'intérêt.

Proposition 3.4.1
Soit $\mathbb{K}/k$ une extension de corps.
Alors :

(i) $\mathbb{K}/k$ est finie $\Leftrightarrow$ $\mathbb{K}/k$ est algébrique et de type fini ;

(ii) $\mathbb{K}/k$ est algébrique $\Leftrightarrow$ $\mathbb{K}/k$ est réunion d'extensions finies de k.

DÉMONSTRATION :

(i) ($\Rightarrow$) Trivial.

($\Leftarrow$) $\mathbb{K}$ est de type fini, donc $\mathbb{K} = k(S)$, avec S finie. De plus, cette extension est algébrique donc tous les éléments de S le sont. Donc $k[S]$ est une algèbre de dimension finie, qui est de plus intègre en tant que sous–anneau d'un corps. Donc $k(S) = k[S]$ est de dimension finie. D'où le résultat.

(i) ($\Rightarrow$) Il suffit de remarquer que :

$$\mathbb{K} = \bigcup_{\alpha \in \mathbb{K}} k(\alpha)$$

Comme les $k(\alpha)$ sont algébriques et de type fini, on déduit le résultat du point (i).

($\Leftarrow$) Trivial.

Exemples :

1. L'extension $k(X_1, \ldots, X_n)/k$ est transcendante et de type fini.
2. $\mathbb{R}/\mathbb{Q}$ est quant à elle transcendante mais pas de type fini.
3. $\mathbb{C}/\mathbb{R}$ est finie et $[\mathbb{C} : \mathbb{R}] = 2$.
4. $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$ est finie et $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = 2$.
5. L'ensemble des nombres algébriques réels est une extension algébrique infinie (i.e non finie) de $\mathbb{Q}$, donc n'est pas de type fini.

Définition 3.4.3 (Plongement)
Soient $\mathbb{K}/k$ et $\mathbb{L}/k$ deux extensions de corps.
Un morphisme d'extensions $\varphi : \mathbb{K} \to \mathbb{L}$ (i.e un morphisme d'algèbres entre deux extensions d'un même corps) est appelé k–plongement.

☞ Remarquons qu'un plongement est *toujours* injectif.
✗ Il arrivera que nous ayons à considérer des plongements différents d'une extension dans une autre. Il conviendra alors de ne pas identifier l'extension de départ à son image par l'un ou l'autre des dits plongements [5]

Exemple : L'inclusion et la conjugaison complexe sont deux $\mathbb{Q}$–plongements de $\mathbb{Q}(i)$ dans $\mathbb{C}$.

Remarque : Si $\sigma : \mathbb{K} \to \mathbb{L}$ est un k–plongement et que $P \in \mathbb{K}[X]$, on notera P^σ l'image de P par le morphisme $\widehat{\sigma} : \mathbb{K}[X] \to \mathbb{L}[X]$ induit par σ (i.e obtenu en appliquant σ aux coefficients des polynômes de $\mathbb{K}[X]$). Dans le cas où nulle ambiguité ne sera à craindre, on notera P^σ simplement "P".

Extensions monogènes :
Soit $\mathbb{K}/k$ une extension de corps et soit $\alpha \in \mathbb{K}$. Interessons nous à l'extension $k(\alpha)/k$.

1. *Si α est transcendant sur k.* Alors le morphisme d'évaluation $ev_\alpha : k[X] \to \mathbb{K}$ est injectif donc induit un isomorphisme :
$$k[X] \cong k[\alpha]$$
On peut de plus prolonger cet isomorphisme aux corps des fractions, via $\underbrace{\frac{P}{Q}}_{\neq 0} \mapsto \underbrace{\frac{P(\alpha)}{Q(\alpha)}}_{\neq 0 \text{ car } \alpha \text{ est transcendant}}$,
ce qui nous donne :0
$$k(X) \cong k(\alpha)$$

2. *Si α est algébrique sur k.* Soit $P_0 \in k[X]$ le polynôme minimal de α sur k. Alors le morphisme d'évaluation $ev_\alpha : k[X] \to \mathbb{K}$ induit un isomorphisme :
$$k[X]/(P_0) \cong k[\alpha] = k(\alpha)$$
On a donc que $(1, \alpha, \ldots, \alpha^{\deg(P_0)-1})$ forme une k–base de $k(\alpha)$ et que :
$$[k(\alpha) : k] = \deg(P_0)$$

5. À moins de souhaiter absolument écrire des choses catastrophiquement obscures.

☞ *En résumé* :

(i) un extension transcendante monogène d'un corps k est isomorphe à $k(X)$;

(ii) un extension algébrique monogène d'un corps k est isomorphe à un quotient $k[X]$ par un polynôme irréductible unitaire.

Lemme 3.4.1 (Bases télescopiques)
Soit $\mathbb{A}$ un anneau commutatif.
Soit $\mathcal{A}$ une $\mathbb{A}$–algèbre commutative et soit $(\alpha_i)_i \in \mathcal{A}^I$.
Soit E un $\mathcal{A}$–module et soit $(e_\ell)_\ell \in E^L$.
Alors :

(i) si $(\alpha_i)_i$ est $\mathbb{A}$–libre dans le $\mathbb{A}$–module $\mathcal{A}$ et si $(e_\ell)_\ell$ est $\mathcal{A}$–libre dans le $\mathcal{A}$–module E, alors $(\alpha_i e_\ell)_{i,\ell}$ est $\mathbb{A}$–libre dans E.

(ii) si $(\alpha_i)_i$ est une famille $\mathbb{A}$–génératrice du $\mathbb{A}$–module $\mathcal{A}$ et si $(e_\ell)_\ell$ est une famille $\mathcal{A}$–génératrice du $\mathcal{A}$–module E, alors $(\alpha_i e_\ell)_{i,\ell}$ est une famille $\mathbb{A}$–génératrice de E.

(iii) si $(\alpha_i)_i$ est une $\mathbb{A}$–base du $\mathbb{A}$–module $\mathcal{A}$ et si $(e_\ell)_\ell$ est une $\mathcal{A}$–base du $\mathcal{A}$–module E, alors $(\alpha_i e_\ell)_{i,\ell}$ est une $\mathbb{A}$–base de E.

Démonstration : Contentons nous de démontrer le (i). Supposons qu'il existe une famille $(\xi_{i,\ell})_{i,\ell}$ d'éléments de $\mathbb{A}$ telle que :

$$\sum_{\ell\in L}\sum_{i\in I}\xi_{i,\ell}\alpha_i e_\ell = 0$$

Alors, par $\mathcal{A}$–liberté de $(e_\ell)_\ell$, on a :

$$\forall \ell \in L,\ \sum_{i\in I}\xi_{i,\ell}\alpha_i e_\ell = 0$$

Et donc, comme (α_i) est $\mathbb{A}$–libre :

$$\forall \ell \in L, \forall i \in I, \xi_{i,\ell} = 0$$

D'où le résultat.

Exemple : Soit $E = \langle e_1, \ldots, e_n\rangle_{\mathbb{C}}$ un $\mathbb{C}$–e.v. Alors la famille $(e_1, ie_1, \ldots, e_n, ie_n)$ forme une $\mathbb{R}$–base de E est donc $\dim_{\mathbb{R}} E = 2\dim_{\mathbb{C}} E$.

Proposition 3.4.2
Soit $\mathbb{K}/k$ une extension de corps.
Soit E un $\mathbb{K}$–e.v.
Alors :

$$\dim_k E = [\mathbb{K} : k]\dim_{\mathbb{K}} E$$

Corollaire 3.4.2.1
Soient $\mathbb{K}/k$ et $\mathbb{L}/\mathbb{K}$ deux extensions de corps.
Alors $\mathbb{L}$ est une extension de k et :

$$[\mathbb{L} : k] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : k]$$

Exemple : Démontrons que $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$. À cet effet, remarquons que :
- $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$;
- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Ainsi, si $\sqrt{2}$ appartenait à $\mathbb{Q}(\sqrt[3]{2})$, alors 2 diviserait 3, ce qui constitue un fait relativement inhabituel. On démontre de la même façon que les seuls sous–corps de $\mathbb{Q}(\sqrt[3]{2})$ dont $\mathbb{Q}$ et $\mathbb{Q}(\sqrt[3]{2})$.

Corollaire 3.4.2.2
Soient $\mathbb{K}/k$ et $\mathbb{L}/\mathbb{K}$ deux extensions algébriques.
Alors $\mathbb{L}/k$ est une extension algébrique.

Démonstration : Soit $\alpha \in \mathbb{L}$. Comme $\mathbb{L}/\mathbb{K}$ est algébrique, il existe un polynôme non nul $P = \sum_{i=0}^{d} a_i X_i \in \mathbb{K}[X]$ admettant α comme racine. De fait, $k(a_1, \ldots, a_d)/k$ est une extension algébrique de type fini (car $k(a_1, \ldots, a_d) \subset \mathbb{K}$) donc est finie. De plus, $P \in k(a_1, \ldots, a_d)[X]$ donc α est algébrique sur $k(a_1, \ldots, a_d)$. Ainsi, $[k(a_1, \ldots, a_d)(\alpha) : k(a_1, \ldots, a_d)]$ et $[k(a_1, \ldots, a_d) : k]$ sont finis, ce qui implique que $k(a_1, \ldots, a_d)(\alpha) : k]$ est fini, donc α est algébrique sur k.

Corollaire 3.4.2.3
Soit $\mathbb{K}/k$ une extension finie de degré premier.
Alors $\mathbb{K}$ et k sont les seuls sous–corps de $\mathbb{K}$ contenant k.

☞ En particulier, $\mathbb{K}/k$ est un extension monogène, engendrée par n'importe quel élément de $\mathbb{K} \setminus k$.

3.5 Extensions quadratiques

Définition 3.5.1 (Extension quadratique)
On appelle extension quadratique toute extension de corps finie de degré 2.

Considérons un polynôme $P := X^2 + pX + q \in k[X]$.

✍ On rappelle qu'étant donné un polynôme $Q \in k[X]$, on a :

$$(Q \text{ est irréductible sur } k) \Rightarrow (Q \text{ n'admet aucune racine sur } k) \text{ dés que } \deg(Q) > 1$$

En revanche :

$$(Q \text{ est irréductible sur } k) \Leftarrow (Q \text{ n'admet aucune racine sur } k) \text{ si et seulement si } \deg(Q) \in \{1, 2, 3\}$$

- *Cas 1 : k n'est pas de caractéristique* 2. On a alors :

$$P = \left(X + \frac{p}{2}\right)^2 - \frac{p^2 - 4q}{4} = \frac{1}{4}\left((2X + p)^2 - \Delta\right)$$

  Où $\Delta := p^2 - 4q$ est le discriminant de P.
  Ainsi :

$$\begin{gathered} \alpha \text{ est racine de } P \text{ dans une extension de } k \\ \Leftrightarrow \\ \beta := 2\alpha + p \text{ vérifie } \beta^2 = \Delta \end{gathered}$$

  De facto :

$$\begin{gathered} P \text{ est irréductible sur } k \\ \Leftrightarrow \\ \Delta \text{ n'est pas un carré dans } k. \end{gathered}$$

  Dans ce cas, on a, via l'isomorphisme $Y \bmod Y^2 - \Delta \mapsto 2X + p \bmod P$:

$$k[Y]/(Y^2 - \Delta) \cong k[X]/(P)$$

  Le quotient $k[Y]/(Y^2 - \Delta)$ est souvent noté $k(\sqrt{\Delta})$ car $\overline{Y}^2 = \Delta$. Cela ne veut *absolument pas* dire qu'on dispose sur cet ensemble d'une quelconque fonction "$\sqrt{\ }$".
  De plus, P admet deux racines dans l'extension $k(\sqrt{\Delta})/k$, égales à $\dfrac{-p \pm \delta}{2}$, où $\delta = \overline{Y}$. On vérifie de plus que :

$$\begin{gathered} k(\sqrt{\Delta_1}) \cong k(\sqrt{\Delta_2}) \\ \Leftrightarrow \\ \frac{\Delta_2}{\Delta_1} \text{ est un carré} \end{gathered}$$

- *Cas 2 : k est de caractéristique* 2.
  - Si $p = 0$, alors :
    - si q est un carré ($q = \alpha^2$), $P = (X + \alpha)^2$ donc admet α comme racine double ;
    - si q n'est pas un carré, P est irréductible et donc $k[X]/(X^2 + q)$ est une extension quadratique de k , notée $k(\sqrt{q})$ (car $q = -q$), dans laquelle P admet une racine double.

– Si $p \neq 0$, alors :

$$P = p^2\left(\left(\frac{X}{p}\right)^2 + \frac{X}{p} + \frac{q}{p^2}\right)$$

De fait :

$$\alpha \text{ est racine de } P \text{ dans une extension de } k$$
$$\Leftrightarrow$$
$$\beta := \frac{\alpha}{p} \text{ est racine de } Q = Y^2 + Y + \frac{q}{p^2}$$

Dans ce cas, comme $Q(Y) = Q(Y+1)$, l'autre racine de Q est $\beta + 1$.

Conclusion : Donnons nous à présent une extension quadratique $\mathbb{K}$ sur un corps k. Alors, d'après le corollaire 3.4.2.3, cette extension est monogène donc isomorphe au quotient $k[X]/(P)$, où P est un polynôme irréductible de degré 2. Ainsi, d'après ce qui précède :

– si k n'est pas de caractéristique 2, alors :

$$\mathbb{K} \cong k[X]/(X^2 - \Delta), \text{ avec } \Delta \in k^* \text{ non carré} ;$$

– si k est de caractéristique 2, alors :

$$\mathbb{K} \cong k[X]/(X^2 + q), \text{ avec } q \in k^* \text{ non carré}$$

ou bien :

$$\mathbb{K} \cong k[X]/(X^2 + X + c), \text{ avec } c \in k \text{ n'étant pas de la forme } c = u^2 + u,\ u \in k$$

Remarque : En caractéristique 2, $x \mapsto x^2$ est un endomorphisme injectif de k et $x \mapsto x^2 + x$ est un endomorphisme de k de noyau $\mathbb{F}_2 := \{0, 1\}$.

Chapitre 4

Racines

Dans tout ce chapitre et sauf mention du contraire, les anneaux seront supposés ***commutatifs***.

4.1 Algèbre des restes, corps de rupture

Donnons nous un anneau $\mathbb{A}$ et un polynôme non nul $P \in \mathbb{A}[X]$. On pose $\mathcal{A} = \mathbb{A}[X]/(P)$ et on munit ce quotient de sa structure naturelle d'algèbre sur $\mathbb{A}$. Enfin, on pose $\omega = X \bmod P \in \mathcal{A}$ et on remarque que $P(\omega) = 0$ dans $\mathcal{A}$. On a alors la propriété universelle suivante :

Proposition 4.1.1
Soit $\mathcal{R}$ une $\mathbb{A}$–algèbre.
Alors :

$$\mathrm{Hom}_{\mathbb{A}-\mathrm{alg}}(\mathcal{A}, \mathcal{R}) \cong \{\alpha \in \mathcal{R} \mid P(\alpha) = 0\}$$

via l'isomorphisme $\varphi \mapsto \varphi(\omega)$, de réciproque $\alpha \mapsto (ev_\alpha : \mathcal{A} \to \mathcal{R})$.

Soit $P = \sum_{i=0}^{d} a_i X^i \in \mathbb{A}[X]$, avec $a_d \in \mathbb{A}^\times$. On peut alors effectuer une division euclidienne par P dans $\mathbb{A}[X]$, même si $\mathbb{A}$ n'est pas un corps. Ainsi, $\mathbb{A}_{d-1}[X]$ est le supplémentaire de (P) dans $\mathbb{A}[X]$, i.e :

$$\mathbb{A}[X] \cong \mathbb{A}_{d-1}[X] \oplus (P)$$

On obtient de fait un isomorphisme de $\mathbb{A}$–modules :

$$\mathbb{A}_{d-1}[X] \cong \mathbb{A}[X]/(P)$$

Et donc l'algèbre $\mathcal{A}$ est libre (en tant que $\mathbb{A}$–module) de base $(1, \omega, \ldots, \omega^{d-1})$.

On se donne dans la suite de ce paragraphe un corps k.

Définition 4.1.1 (Algèbre des restes)
Soit $P \in k[X] \setminus \{0\}$.
On appelle (k–)algèbre des restes de P le quotient $k[X]/(P)$.

Exemples :

1. $\mathbb{C}$ est la $\mathbb{R}$–algèbre des restes de $X^2 + 1$.
2. La k–algèbre des restes de X^2 est appelée *k–algèbre des nombres duaux*. On la note $k[\varepsilon]$. Les éléments de cette algèbre sont de la forme $x + y\varepsilon$, avec $x, y \in k$ et $\varepsilon := \overline{X}$ (donc vérifiant $\varepsilon^2 = 0$). On a de fait la relation :

$$\forall x, x', y, y' \in k,\ (x + y\varepsilon)(x' + y'\varepsilon) = xx' + (xy' + x'y)\varepsilon$$

Proposition 4.1.2 (Cas irréductible)
Soit $P \in k[X]$ un polynôme non nul.
Soit $\mathcal{A}$ l'algèbre des restes de P.
Alors :

(i) P est irréductible $\Leftrightarrow$ $\mathcal{A}$ est un corps ;

(ii) *si P est irréductible, alors $\mathcal{A}$ forme une extension de k dans laquelle P admet une racine ω et vérifiant :*

$$[\mathcal{A} : k] = \deg(P)$$

De plus, P est alors le polynôme minimal de ω sur k

Remarque : Si P est irréductible et que $\mathbb{L}/k$ est une extension de corps, on a une bijection entre l'ensemble des racines de P dans $\mathbb{L}$ et l'ensemble $\hom_{k-\mathrm{alg}}(\mathcal{A}, \mathbb{L})$ des k–plongements de $\mathcal{A}$ dans $\mathbb{L}$. Ainsi, il y a au plus $\deg(P)$ tels k–plongements.

De plus, si σ est un k–plongement de $\mathcal{A}$ dans $\mathbb{L}$ correspondant à une racine $\alpha \in \mathbb{L}$ de P, on a :

$$\sigma(\mathcal{A}) = k(\alpha) \subset \mathbb{L}$$

Ce qui induit un isomorphisme d'extensions de corps :

$$\mathcal{A} \cong k(\alpha) \subset \mathbb{L}$$

Définition 4.1.2 (Corps de rupture)
Soit $P \in k[X]$ un polynôme irréductible.
On appelle corps de rupture de P (sur k) tout couple $(\mathbb{K}, \alpha)$, où

(i) *$\mathbb{K}/k$ est une extension de corps ;*
(ii) *$\alpha \in \mathbb{K}$ est une racine de P ;*
(iii) *$\mathbb{K} = k(\alpha)$.*

Proposition 4.1.3
Tout polynôme irréductible $P \in \mathbb{K}[X]$ un corps de rupture défini par :

$$(\mathcal{A}, \omega) := (k[X]/\left(P\right), X \bmod P)$$

De plus, si $(\mathbb{K}, \alpha)$ est un corps de rupture de P, il existe un unique k–isomorphisme de $\mathcal{A}$ sur $\mathbb{K}$ envoyant ω sur α.

Corollaire 4.1.3.1 (Unicité du corps de rupture)
Soit $P \in k[X]$ un polynôme irréductible.
Alors le corps de rupture de P est unique à isomorphisme unique près, i.e si $(\mathbb{K}, \alpha)$ et $(\mathbb{L}, \beta)$ sont deux corps de rupture de P, il existe un unique k–isomorphisme de $\mathbb{K}$ dans $\mathbb{L}$ envoyant α sur β.

Exemples :

1. Trois corps de ruptures de X^2+1 sur $\mathbb{R}$ sont $(\mathbb{R}[X]/(X^2+1), \overline{X})$, $(\mathbb{C}, i)$ et $(\mathbb{C}, -i)$. On a alors les isomorphismes suivants :

$$\begin{tikzcd}
 & Q \arrow[r, mapsto] & Q(i) & (\mathbb{C}, i) \arrow[dd] & z \arrow[dd, mapsto] \\
(\mathbb{R}[X]/(X^2+1), \overline{X}) \arrow[urrr] \arrow[drrr] & & & & \\
 & Q \arrow[r, mapsto] & Q(-i) & (\mathbb{C}, -i) & \overline{z}
\end{tikzcd}$$

2. Quatre corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$ sont, si on pose $j = e^{2i\frac{\pi}{3}}$:

(a) $(\mathcal{A}, \omega) := (\mathbb{Q}[X]/(X^3-2), \overline{X})$;

(b) $(\mathbb{K}_1, \alpha_1) := (\mathbb{Q}(\sqrt[3]{2}), \sqrt[3]{2})$;

(c) $(\mathbb{K}_2, \alpha_2) := (\mathbb{Q}(j\sqrt[3]{2}), j\sqrt[3]{2})$;

(d) $(\mathbb{K}_3, \alpha_3) := (\mathbb{Q}(j^2\sqrt[3]{2}), j^2\sqrt[3]{2})$.

Les corps $\mathbb{K}_1$, $\mathbb{K}_2$ et $\mathbb{K}_3$ sont isomorphes mais deux à deux distincts. En effet, $\mathbb{K}_1 \neq \mathbb{K}_2$ car $\mathbb{K}_2 \subsetneq \mathbb{R}$. En fait, α_1 est la seule racine réelle de X^3-2 car $\alpha_2, \alpha_3 \notin \mathbb{R}$: P a une unique racine dans $\mathbb{K}_1$ donc il en est de même dans $\mathbb{K}_2$ et $\mathbb{K}_3$ par isomorphisme. Par conséquent :

$$\mathbb{K}_1 \neq \mathbb{K}_2 \neq \mathbb{K}_3 \neq \mathbb{K}_1$$

4.2 Corps de décomposition

Définition 4.2.1 (Corps de décomposition)
Soit $\mathbb{K}$ un corps.
Soit $P \in \mathbb{K}[X] \setminus \{0\}$.
On appelle corps de décomposition de P sur $\mathbb{K}$ une extension de corps $E/\mathbb{K}$ vérifiant que :

(i) P est scindé sur E, i.e $\exists \lambda, \alpha_1, \ldots, \alpha_d \in E$ tels que :

$$P = \lambda \prod_{i=1}^{d} (X - \alpha_i)$$

(ii) $E = \mathbb{K}(\alpha_1, \ldots, \alpha_d)$.

☞ Au sens de l'inclusion, E est donc la plus petite extension de $\mathbb{K}$ où "P a toutes ses racines".
✍ Remarquons que l'on n'a pas supposé ici que P était irréductible sur $\mathbb{K}$. De plus, on a nécessairement $\lambda \in \mathbb{K}$ (λ est le coefficient dominant de P).

Proposition 4.2.1
Soit $\mathbb{K}$ un corps.
Soit $P \in \mathbb{K}[X] \setminus \{0\}$.
Alors, si E est un corps de décomposition de P, l'extension $E/\mathbb{K}$ est finie (i.e $[E : \mathbb{K}] < \infty$).

Démonstration : Trivial.

Proposition 4.2.2
Soit $\mathbb{K}$ un corps.
Soit $P \in \mathbb{K}[X] \setminus \{0\}$.
Soit $\mathbb{L}$ une extension de $\mathbb{K}$ sur laquelle P est scindé.
Alors $\mathbb{L}$ contient un unique *corps de décomposition de P sur $\mathbb{K}$. Il s'agit de facto de l'extension de $\mathbb{K}$ engendrée par les racines de P sur $\mathbb{L}$.*

Proposition 4.2.3
Soit $\mathbb{K}$ un corps.
Soit $P \in \mathbb{K}[X] \setminus \{0\}$.
Alors :

(i) P admet un corps de décomposition E sur $\mathbb{K}$ tel que :

$$[E : \mathbb{K}] \leq (\deg(P))!$$

(ii) Si E et F sont deux corps de décomposition de P sur $\mathbb{K}$ alors :

$$E \cong F$$

Démonstration :

(i) On procède par récurrence sur $\deg(P)$ (adjonction itérée de racines).

(ii) Admis.

✌ À ce stade, il peut être intéressant[1] de dresser un petit tableau récapitulatif :

	Corps de rupture	**Corps de décomposition**
Hypothèse sur P	P est irréductible	$P \neq 0$
Nature	Extension de corps contenant une racine de P	Extension de corps contenant les racines de P
Existence, unicité	Existence et unicité à ismorphisme unique près	Existence et unicité à ismorphisme près
Dans une extension donnée $\mathbb{L}/\mathbb{K}$ **...**	Il peut y avoir plusieurs corps de rupture de P	On a au plus un corps de décomposition de P, qui peut avoir des automorphismes non triviaux

Exemples :

1. On se place dans le cas $\mathbb{K} := \mathbb{Q}$, $P := X^3 - 2$. On note $\alpha_1 := \sqrt[3]{2}$, $\alpha_2 := j\sqrt[3]{2}$ et $\alpha_3 := j^2\sqrt[3]{2}$ les racines complexes de P. Alors $E := \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ est le seul corps de décomposition de P inclus dans $\mathbb{C}$. Démontrons que $[E : \mathbb{Q}] = 6$.
   - *Méthode 1.* On a vu que $\alpha_2 \notin \mathbb{Q}(\alpha_1)$, donc :
   $$\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subsetneq \mathbb{Q}(\alpha_1, \alpha_2) \subset E$$
   Or $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 3$ donc $3 < [E : \mathbb{Q}]$ et $3 | [E : \mathbb{Q}]$. De facto, par la proposion 4.2.3, $[E : \mathbb{Q}] \leq 6$. In fine, on a bien $[E : \mathbb{Q}] = 6$
   - *Méthode 2.* P a deux racines dans $\mathbb{Q}(\alpha_1, \alpha_2)$. Or, $\alpha_1 + \alpha_2 + \alpha_3 = 0$ donc $\alpha_3 = -(\alpha_1 + \alpha_2) \in \mathbb{Q}(\alpha_1, \alpha_2)$. De fait, $E = \mathbb{Q}(\alpha_1, \alpha_2)$.
   Calculons à présent $\deg_{\mathbb{Q}(\alpha_1)}(\alpha_2)$. On sait que dans $\mathbb{Q}(\alpha_1)[X]$, il existe un polynôme Q de degré 2 n'admettant pas α_1 comme racine tel que :
   $$X^3 - 2 = (X - \alpha_1)Q \text{ et } Q(\alpha_2) = 0$$
   De fait, $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] \leq 2$. D'autre part, $\alpha_2 \notin \mathbb{Q}(\alpha_1)$ donc $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] = 2$:
   $$[E : \mathbb{Q}] = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)][\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 2 \times 3 = 6$$
2. On se place dans le cas $\mathbb{K} := \mathbb{Q}$, $P := X^2 - 2$. Alors $\mathbb{Q}[X]/(P)$ et $\mathbb{Q}(-\sqrt{2}, \sqrt{2})$ sont deux corps de décompositions distincts (mais isomorphes) de P qui y admet pour racines respectivement $-\overline{X}, \overline{X}$ et $-\sqrt{2}, \sqrt{2}$.
3. On se place dans le cas $\mathbb{K} := \mathbb{Q}(j)$, $P := X^3 - 2$. Le polynôme minimal de j sur $\mathbb{Q}$ est $1 + X + X^2$ donc $[\mathbb{K} : \mathbb{Q}] = 2$. De plus, P est irréductible sur $\mathbb{K}$ car dans le cas contraire, comme il est de degré 3, il admettrait une racine sur $\mathbb{K}$, ce qui est impossible car P est un polynôme irréductible de degré 3 sur $\mathbb{Q}$ et que $[\mathbb{K} : \mathbb{Q}] = 2$. Or (avec les notations du 1.) $\alpha_2 = j\alpha_1$, $\alpha_3 = j\alpha_2$ et $j = \dfrac{\alpha_2}{\alpha_1}$ donc $\mathbb{K}(\alpha_1) = \mathbb{Q}(j, \alpha_2) = E$. De fait, E est aussi le corps de décomposition dans $\mathbb{C}$ de P sur $\mathbb{K}$ et $[E : \mathbb{K}] = 3$.

4.3 Corps algébriquement clos, clôture algébrique

Définition 4.3.1 (Corps algébriquement clos)
Un corps $\mathbb{K}$ est dit algébriquement clos si il vérifie l'une des conditions équivalentes suivantes :

(i) tout polynôme de $\mathbb{K}[X]$ non constant admet une racine dans $\mathbb{K}$;

(ii) tout polynôme non nul de $\mathbb{K}[X]$ est scindé sur $\mathbb{K}$;

(iii) tout polynôme irréductible de $\mathbb{K}[X]$ est de degré 1 ;

(iv) toute extension algébrique de $\mathbb{K}$ est isomorphe à $\mathbb{K}$;

(v) toute extension finie de $\mathbb{K}$ est isomorphe à $\mathbb{K}$.

1. Et ludique !

Définition 4.3.2 (Clôture algébrique)
Un clôture algébrique d'un corps $\mathbb{K}$ est une extension algébrique *de $\mathbb{K}$ qui est un corps algébriquement clos.*

Lemme 4.3.1
Soit $\Omega/\mathbb{K}$ une extension algébrique telle que tout polynôme non nul de $\mathbb{K}[X]$ soit scindé sour Ω. Alors Ω est un corps algébriquement clos (et donc une clôture algébrique de $\mathbb{K}$).

DÉMONSTRATION : Soit $\mathbb{L}/\Omega$ une extension algébrique. Démontrons que $\mathbb{L} = \Omega$. Si $\alpha \in \mathbb{L}$, alors α est algébrique sur Ω qui est algébrique sur $\mathbb{K}$ donc α est algébrique sur $\mathbb{K}$, i.e $\exists P \in \mathbb{K}[X] \setminus \{0\}$ tel que $P(\alpha) = 0$. Or, par hypothèse, il existe $\lambda \in \mathbb{K}$ et $\beta_1, \ldots, \beta_d \in \Omega$ tel que :

$$P = \lambda \prod_{i=1}^{d} (X - \beta_i)$$

Or α est racine de P donc il existe un indice $1 \leq i \leq d$ tel que $\alpha = \beta_i \in \Omega$. D'où le résultat.

Le théorème qui suit fut énoncé par Jean le Rond D'Alembert et démontré par Johann Carl Friedrich Gauss :

Théorème 4.3.1 (D'Alembert–Gauss)
$\mathbb{C}$ est algébriquement clos.

DÉMONSTRATION : Se référer à un cours d'analyse complexe (par exemple).

Corollaire 4.3.1.1
Le corps $\overline{\mathbb{Q}}$ des nombres complexes algébriques est une clôture algébrique de $\mathbb{Q}$.

DÉMONSTRATION : Soit $P \in \mathbb{Q}[X] \setminus \{0\}$. Par théorème de D'Alembert–Gauss, P est scindé sur $\mathbb{C}$. Or, par définition de $\overline{\mathbb{Q}}$, les racines de P sont dans $\overline{\mathbb{Q}}$. De fait, P est scindé sur $\overline{\mathbb{Q}}$, d'où le résultat par lemme 4.3.1.

Proposition 4.3.2 (Steinitz)
Soit $\mathbb{K}$ un corps.
Alors :

(i) $\mathbb{K}$ admet une clôture algébrique ;
(ii) deux clôtures algébriques de $\mathbb{K}$ sont $\mathbb{K}$–isomorphes.

DÉMONSTRATION : ADMIS (utilise le lemme de Zorn).

4.4 Éléments algébriques séparables

Définition 4.4.1 (Éléments séparables)
Soit k un corps.

(i) Un polynôme $P \in k[X] \setminus \{0\}$ est dit séparable si ses racines (dans un corps de décomposition ou une clôture algébrique de k) sont simples (i.e de multiplicité 1).
(ii) Un élément α algébrique sur k (dans une extension de k) est dit séparable (sur k) si son polynôme minimal sur k l'est.

Proposition 4.4.1
Soit k un corps.
Soient $P, Q \in k[X] \setminus \{0\}$.
Alors :

(i) si Q est séparable et si $P|Q$, P est séparable ;
(ii) si P est séparable, ses facteurs irréductibles dans $k[X]$ sont de multiplicité 1 (on dit que P est sans facteur carré dans $k[X]$).

Proposition 4.4.2
Soient $\mathbb{K}/k$ et $\mathbb{L}/\mathbb{K}$ deux extensions de corps.
Soit $\alpha \in \mathbb{L}$ un élément algébrique séparable sur k.
Alors α est algébrique séparable sur $\mathbb{K}$ et son polynôme minimal sur $\mathbb{K}$ divise son polynôme minimal sur k.

Exemple : Soit k un corps de caractéristique 2. On considère le polynôme $P := X^2 + t$, avec $t \in k$ non carré dans k. Si α est une racine de P dans une extension de k, alors $\alpha^2 = t$ donc (par relation de Frobénius) $P = (X + \alpha)^2$. Ainsi, α est racine double de son polynôme minimal donc est inséparable sur k et P est irréductible dans $k[X]$ mais inséparable.

Définition 4.4.2 (Caractéristique d'un anneau)
Soit $\mathbb{A}$ un anneau (commutatif).
On appelle caractéristique de $\mathbb{A}$ l'unique générateur positif du noyau de l'unique morphisme d'anneau $\varphi : \mathbb{Z} \to \mathbb{A}$. On note cette quantité $\mathrm{car}(\mathbb{A})$.

☞ On a alors :

$$\mathrm{Im}(\varphi) \cong \mathbb{Z}/\mathrm{car}(\mathbb{A})\mathbb{Z}$$

Caractéristique d'un corps :
Soit k un corps de caractéristique p. D'après la remarque ci–dessus, $\mathbb{Z}/n\mathbb{Z}$ est intègre. On doit donc distinguer deux cas.

– *Cas 1 : $p = 0$.* Le morphisme $\varphi : \mathbb{Z} \hookrightarrow k$ se prolonge en un unique plongement $j : \mathbb{Q} \hookrightarrow k$ donc k est une extension de $\mathbb{Q}$. Le corps $j(\mathbb{Q})$ est alors le plus petit sous–corps de k, appelé ***sous–corps premier*** de k.
– *Cas 2 : p est un nombre premier positif.* Alors :

$$\varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} \hookrightarrow k$$

$\varphi(\mathbb{Z})$ est alors le plus petit sous–corps de k, appelé ***corps premier*** de k. On peut ainsi voir k comme une extension de $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Dans ce cas, $F : x \mapsto x^p$ est un k–endomorphisme de k, appelé *endomorphisme de Frobénius* (cette dernière propriété est vraie dans tout anneau commutatif de caractéristique p). Comme k est un corps, F est injectif : *tout élément de k admet au plus une racine p–ième.*

Proposition 4.4.3 (Dérivation des polynômes)
Soit $\mathbb{A}$ un anneau (commutatif).
On définit :

$$D : \mathbb{A}[X] \to \mathbb{A}[X]$$
$$P = \sum_{k=0}^{d} a_k X^k \mapsto P' := \sum_{k=1}^{d} k a_k X^{k-1}$$

Alors :

(i) D est $\mathbb{A}$–linéaire et nulle sur $\mathbb{A}$;
(ii) $\forall P, Q \in \mathbb{A}[X]$, $(PQ)' = P'Q + PQ'$;
(iii) $\forall P \in \mathbb{A}[X]$, $\forall n \geq 1$, $(P^n)' = nP^{n-1}P'$;
(iv) si $\mathrm{car}(\mathbb{A}) = 0$, *alors D est surjective* si $\mathbb{A}$ est un corps *et :*

$$\mathrm{Ker}(D) = \mathbb{A}$$

(v) si $\mathrm{car}(\mathbb{A})$ *est un nombre premier positif p, alors $X^{p-1} \notin \mathrm{Im}(D)$ et :*

$$\mathrm{Ker}(D) = \mathbb{A}[X^p]$$

Proposition 4.4.4
Soit $\mathbb{K}/k$ une extension de corps.
Soit $\alpha \in \mathbb{K}$.
Soit $P \in k[X]$.
Alors :

(i) α est racine simple de $P \Leftrightarrow P(\alpha) = 0$ et $P'(\alpha) \neq 0$;
(ii) P est séparable $\Leftrightarrow$ P et P' sont premiers entre eux dans $k[X]$.

DÉMONSTRATION :

(i) Immédiat.

(*ii*) Soit Ω une clôture algébrique de k. Alors :

$$\begin{aligned} P \text{ et } P' \text{ sont premiers entre eux dans } k[X] &\Leftrightarrow P \text{ et } P' \text{ sont premiers entre eux dans } \Omega[X] \\ &\Leftrightarrow P \text{ et } P' \text{ sont sans racine commune dans } \Omega \\ &\Leftrightarrow P \text{ est sans racine multiple dans } \Omega \\ &\Leftrightarrow P \text{ est séparable} \end{aligned}$$

Proposition 4.4.5
Soit k un corps.
Soit $a \in k^*$.
Soit $n \geq 1$.
Alors :

(*i*) *$X^n - a$ est séparable $\Leftrightarrow \operatorname{car}(k) \nmid n \Leftrightarrow n1_k \neq 0$;*

(*ii*) *si $\operatorname{car}(k) = p > 0$,*

(*a*) *si il existe $\alpha \in k$ tel que $a = \alpha^p$, alors (par relation de Frobénius) $X^p - a = (X - \alpha)^p$;*

(*b*) *si a n'est pas une puissance p–ième dans k alors $X^p - a$ est irréductible et non séparable.*

Proposition 4.4.6
Soit k un corps.
Soit $P \in k[X]$ un polynôme irréductible.
Alors :

$$P \text{ est séparable } \Leftrightarrow P' \neq 0$$

Démonstration :

$$\begin{aligned} P \text{ est séparable } &\Leftrightarrow \operatorname{pgcd}(P, P') = 1 \\ &\Leftrightarrow P \nmid P' \end{aligned}$$

La dernière équivalence provient du fait que comme P est irréductible, pour tout polynôme $Q \in k[X]$ ou bien $\operatorname{pgcd}(P, Q) = 1$ ou bien $P|Q$. De fait :

$$\begin{aligned} P \text{ est inséparable } &\Leftrightarrow P' \text{ est un multiple de } P \\ & p' = 0 \end{aligned}$$

Corollaire 4.4.6.1
Soit k un corps.
Soit $P \in k[X]$ un polynôme irréductible.
Alors :

(*i*) *si $\operatorname{car}(k) = 0$, P est séparable ;*

(*ii*) *si $\operatorname{car}(k) = p > 0$, on a :*

$$\begin{aligned} P \text{ est inséparable } &\Leftrightarrow P \in k[X]^p \\ &\Leftrightarrow \text{ il existe une extension } \mathbb{L}/k \text{ telle que } P \text{ soit une puissance } p\text{–ième dans } \mathbb{L}[X] \end{aligned}$$

Démonstration :

(i) Trivial : en caractéristique 0, la nullité de P' est équivalente au fait que P est constant.

(ii) $P' = 0 \Leftrightarrow P \in k[X]^p$, i.e :

$$P = \sum_{i=0}^{n} a_i X^{ip}, \text{ les } a_i \in k$$

Soit $\mathbb{L}/k$ une extension dans laquelle chaque a_i admet une racine p–ième α_i (e.g $\mathbb{L} = k[X]/\prod_i (X^p - a_i)$). Alors, dans $\mathbb{L}[X]$ on a, "par la magie de Frobénius" :

$$P = \sum_{i=0}^{n} (\alpha_i X^i)^p = \left(\sum_{i=0}^{n} \alpha_i X^i \right)^p$$

D'où le résultat.

Définition 4.4.3 (Corps parfait)
Soit k un corps.
On dit que k est un corps parfait s'il vérifie l'une des conditions équivalentes suivantes :

(i) tout polynôme irréductible de $k[X]$ est séparable ;

(ii) tout élément algébrique sur k y est séparable.

Proposition 4.4.7
Soit p un nombre premier positif.

(i) tout corps algébriquement clos est parfait ;

(ii) toute extension algébrique *d'un corps parfait est un corps parfait ;*

(iii) tout corps de caractéristique nulle est parfait ;

(iv) si k est un corps de caractéristique p, alors :

$$\begin{aligned} k \text{ est parfait } &\Leftrightarrow \text{ le morphisme de Frobénius } F : x \mapsto x^p \text{ est surjectif} \\ &\Leftrightarrow F \in \mathrm{Aut}_k(k) \\ &\Leftrightarrow \text{ tout élément de } k \text{ y admet une unique racine } p\text{–ième} \end{aligned}$$

Démonstration :

(i) Trivial (les irréductibles sont de degré 1).

(ii) Soit k un corps parfait et $\mathbb{K}/k$ une extension algébrique. Tout élément de $\mathbb{K}$ est algébrique sur k donc y est séparable car ce dernier est parfait, donc est séparable sur $\mathbb{K}$. Quod erat demonstrandum.

(iii) Immédiat car irréductible implique séparable en caractéristique nulle.

(iv)
- Si il existe $P \in k[X]$ irréductible et inséparable, alors on sait (corollaire 4.4.6.1) que $P \in k[X^p]$. Or, si tous les coefficients de P admettait une racine p–ième dans k, P serait une puissance p–ième et donc non irréductible. De facto, F n'est pas surjectif.
- Si F n'est pas surjectif, il existe $a \in k$ n'admettant pas de racine p–ième dans k. De fait $X^p - a$ est irréductible et inséparable d'après le corollaire 4.4.6.1. Donc k n'est pas parfait.

Corollaire 4.4.7.1
Tout corps fini est parfait.

Démonstration : Par argument de cardinal, le morphisme de Frobénius est bijectif dans tout corps fini car injectif.

Remarque :

1. Si k est un corps de caractéristique $p > 0$, alors $k(T)$ est non parfait car T n'y est pas une puissance p–ième.
2. Étant donné un corps non parfait,on peut l'étendre (resp. le "réduire") en un corps parfait via clôture algébrique (resp. corps premier).

Chapitre 5

Théorie de Galois

5.1 Plongements d'une extension finie dans une clôture algébrique

Définition 5.1.1 (Degré séparable)
Soit $\mathbb{K}$ un corps.
Soit Ω une clôture algébrique de $\mathbb{K}$.
Pour toute extension finie $\mathbb{L}/\mathbb{K}$, on appelle degré séparable de $\mathbb{L}/\mathbb{K}$ la quantité :

$$d\left(\mathbb{L}/\mathbb{K}\right) := \operatorname{card}\left(\operatorname{Hom}_{\mathbb{K}}\left(\mathbb{L}, \Omega\right)\right)$$

✍ $d\left(\mathbb{L}/\mathbb{K}\right)$ est de fait le nombre de $\mathbb{K}$–plongements de $\mathbb{L}$ dans Ω. Comme deux clôtures algébriques de $\mathbb{K}$ sont $\mathbb{K}$–isomorphes, $d(\mathbb{L}/\mathbb{K})$ ne dépend pas de Ω.

Proposition 5.1.1
Soit $\mathbb{L}/\mathbb{K}$ une extension finie.
Alors :

$$d(\mathbb{L}/\mathbb{K}) \geq 1$$

Démonstration : Comme $d(\mathbb{L}/\mathbb{K})$ ne dépend pas de Ω, on peut prendre pour Ω une clôture algébrique de $\mathbb{L}$ (car $\mathbb{L}/\mathbb{K}$ est finie).

Cas monogène :
Supposons que $\mathbb{L} = \mathbb{K}(\alpha) = \mathbb{K}[X]/(P)$, avec P irréductible. Alors, si Ω est une clôture algébrique de $\mathbb{K}$ et si on note $\operatorname{Rac}_{\Omega}(P)$ l'ensemble des racines de P sur Ω, on a :

$$\operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega) \cong \operatorname{Rac}_{\Omega}(P)$$

Et donc :

$$1 \leq d(\mathbb{L}/\mathbb{K}) \leq \deg(P) = [\mathbb{L} : \mathbb{K}]$$

On a de plus égalité à droite si et seulement si P n'a que des racines simples dans Ω, i.e est séparable sur $\mathbb{K}$, ce qui équivaut à dire que α l'est.

Lemme 5.1.1
Soient $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ deux extensions finies.
Alors :

$$d(\mathbb{M}/\mathbb{K}) = d(\mathbb{M}/\mathbb{L})d(\mathbb{L}/\mathbb{K})$$

De plus, tout $\mathbb{K}$–plongement de $\mathbb{L}$ dans une clôture algébrique de $\mathbb{K}$ se prolonge à $\mathbb{M}$.

Démonstration : Soit Ω une clôture algébrique de $\mathbb{K}$. On définit $r : \operatorname{Hom}_{\mathbb{K}}(\mathbb{M}, \Omega) \to \operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$ par $r(f) := f_{|\mathbb{L}}$. Pour tout $j \in \operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$, $r^{-1}(\{j\})$ est le nombre de plongements de $\mathbb{M}$ dans Ω induisant j sur $\mathbb{L}$, i.e le nombre de prolongements $\mathbb{K}$–linéaires de j à $\mathbb{M}$. De fait :

$$r^{-1}(\{j\}) = \operatorname{Hom}_{\mathbb{L}}(\mathbb{M}, (\Omega, j))$$

De plus, (Ω, j), vue comme $\mathbb{L}$–algèbre est une clôture algébrique de $\mathbb{L}$. De fait, co $\mathrm{card}(r^{-1}(\{j\})) = d(\mathbb{M}/\mathbb{L}) \geq 1$ donc r est surjective. In fine :

$$d(\mathbb{M}/\mathbb{K}) = \sum_{j \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)} \underbrace{\mathrm{card}(r^{-1}(\{j\}))}_{=d(\mathbb{M}/\mathbb{L})} = d(\mathbb{M}/\mathbb{L})d(\mathbb{L}/\mathbb{K})$$

D'où le résultat.

Proposition 5.1.2 (Extension (finie) séparable)
Soit $\mathbb{L}/\mathbb{K}$ une extension finie.
Alors :

$$1 \leq d(\mathbb{L}/\mathbb{K}) \leq [\mathbb{L} : \mathbb{K}]$$

On a de plus équivalence entre les propriétés suivantes :

(i) $d(\mathbb{L}/\mathbb{K}) = [\mathbb{L} : \mathbb{K}]$ *;*

(ii) $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$*, avec* $\alpha_1, \ldots, \alpha_n$ *séparables sur* $\mathbb{K}$ *;*

(iii) tout élément de $\mathbb{L}$ *est séparable sur* $\mathbb{K}$.

Un extension vérifiant l'une de (et donc toutes) ces trois propriétés est dite séparable.

Démonstration : On procède par récurrence sur $n = [\mathbb{L} : \mathbb{K}]$ en utilisant le lemme 5.1.1.

Définition 5.1.2 (Extension algébrique séparable)
Une extension algébrique est dite séparable si chacune de ses sous–extensions finies l'est (i.e si chacun de ses éléments l'est sur le corps de base).

Proposition 5.1.3
Soit $\mathbb{K}$ un corps.
Alors :

$$\begin{aligned} \mathbb{K} \textit{ est parfait} &\Leftrightarrow \textit{ toute extension finie de } \mathbb{K} \textit{ est séparable} \\ &\Leftrightarrow \textit{ toute extension algébrique de } \mathbb{K} \textit{ est séparable} \end{aligned}$$

Proposition 5.1.4 (Extension radicielle)
Soit $\mathbb{L}/\mathbb{K}$ une extension finie.
Alors l'ensemble $\mathbb{L}_0$ des éléments de $\mathbb{L}$ séparables sur $\mathbb{K}$ est un sous–corps de $\mathbb{L}$ et :

$$d(\mathbb{L}/\mathbb{K}) = [\mathbb{L}_0 : \mathbb{K}]$$

De fait :

(i) $d(\mathbb{L}/\mathbb{K}) | [\mathbb{L} : \mathbb{K}]$ *;*

(ii) $d(\mathbb{L}/\mathbb{L}_0) = 1$.

Si $\mathbb{L}_0 = \mathbb{K}$ (i.e $d(\mathbb{L}/\mathbb{K}) = 1$), on dit que $\mathbb{L}/\mathbb{K}$ est une extension radicielle[1]*. Dans ce cas, $[\mathbb{L} : \mathbb{K}]$ est une puissance de $p := \mathrm{car}(\mathbb{K})$ et :*

$$\forall \alpha \in \mathbb{L},\ \exists s \geq 0,\ \alpha^{p^s} \in \mathbb{K}$$

Exemple : Soit $\mathbb{K}$ un corps non parfait et soit $a \in \mathbb{K}$ sans racine p–ième dans $\mathbb{K}$. Alors $\mathbb{L} := \mathbb{K}[X]/(X^p - a)$ est une extension radicielle de degré p de $\mathbb{K}$ vérifiant $d(\mathbb{L}/\mathbb{K}) = \mathrm{Rac}_{\Omega}(P) = 1$.

5.2 Automorphismes, extensions galoisiennes

✍ Si $\mathbb{L}/\mathbb{K}$ est une extension de corps, on notera $\mathrm{Aut}(\mathbb{L}/\mathbb{K}) := \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ l'ensemble des $\mathbb{K}$–automorphismes de $\mathbb{L}$, i.e l'ensemble des automorphismes du corps $\mathbb{L}$ induisant l'identité sur $\mathbb{K} \hookrightarrow \mathbb{L}$.

1. On parle aussi outre–Manche de "purement inséparable".

Exemples :

1. $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, z \mapsto \overline{z}\}$.
2. Si $\mathbb{K}$ est un corps , on montre que les $\mathbb{K}$–automorphismes de $\mathbb{K}(T)$ sont de la forme :

$$R(T) \mapsto R\left(\frac{aT+b}{cT+d}\right), \text{ avec } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G\ell_2(\mathbb{K})$$

D'où :

$$PG\ell_2(\mathbb{K}) := G\ell_2(\mathbb{K})/\mathbb{K}^* \cong \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}(T))$$

Proposition 5.2.1
Soit $\mathbb{L}/\mathbb{K}$ *une extension de corps.*
Soit $P \in \mathbb{K}[X] \setminus \{0\}$.
Soit $\sigma \in \mathrm{End}_{\mathbb{K}}(\mathbb{L})$.
Alors :

$$\sigma\left(\mathrm{Rac}_{\mathbb{L}}\left(P\right)\right) = \mathrm{Rac}_{\mathbb{L}}(P)$$

Démonstration : Découle immédiatement du fait que σ est injective et que $\mathrm{Rac}_{\mathbb{L}}(P)$ est un ensemble fini. En effet, comme $P \in \mathbb{K}[X]$, $\forall z \in \mathbb{L}$, $\sigma(P(z)) = P(\sigma(z))$ car $\sigma_{|_{\mathbb{K}}} = \mathrm{id}_{\mathbb{K}}$.

✍ Soit $\mathbb{L}/\mathbb{K}$ une extension de corps et soit $P \in \mathbb{K}[X] \setminus \{0\}$. Si $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{K})$, σ ne fait que permuter les racines de P sur $\mathbb{L}$. De fait, on obtient une action du groupe $\mathrm{Aut}(\mathbb{L}/\mathbb{K})$ sur l'ensemble fini $\mathrm{Rac}_{\mathbb{L}}(P)$.

Corollaire 5.2.1.1
Soit $\mathbb{L}/\mathbb{K}$ *une extension* algébrique.
Alors :

$$\mathrm{End}_{\mathbb{K}}(\mathbb{L}) = \mathrm{Aut}(\mathbb{L}/\mathbb{K})$$

✘ En revanche, dans l'extension transcendante $\mathbb{K}(T)/\mathbb{K}$, l'endomorphisme $R(T) \mapsto R(T^2)$ n'est pas surjectif.

Proposition 5.2.2
Soit $\mathbb{L}/\mathbb{K}$ *une extension* finie.
Alors :

$$\mathrm{card}\left(\mathrm{Aut}\left(\mathbb{L}/\mathbb{K}\right)\right) \leq [\mathbb{L} : \mathbb{K}] < \infty$$

De plus, si on a égalité, l'extension $\mathbb{L}/\mathbb{K}$ *est séparable.*

Démonstration : Soit Ω une clôture algébrique de $\mathbb{L}$. Alors $\mathrm{Aut}(\mathbb{L}/\mathbb{K}) \subset \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$, d'où le résultat par proposition 5.1.2.

Définition 5.2.1 (Extension galoisienne, groupe de Galois)
Soit $\mathbb{L}/\mathbb{K}$ *une extension* finie.
Alors l'extension $\mathbb{L}/\mathbb{K}$ *est dite galoisienne si :*

$$\mathrm{card}\left(\mathrm{Aut}\left(\mathbb{L}/\mathbb{K}\right)\right) = [\mathbb{L} : \mathbb{K}]$$

Dans ce cas, le groupe $\mathrm{Aut}\left(\mathbb{L}/\mathbb{K}\right) = \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ *est appelé groupe de Galois de* $\mathbb{L}$ *sur* $\mathbb{K}$*. On le note alors* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

Proposition 5.2.3
Une extension galoisienne est séparable.

Proposition 5.2.4 (Ordre du groupe de Galois)
Soit $\mathbb{L}/\mathbb{K}$ *une extension finie.*
Alors le groupe de Galois $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ *est fini d'ordre* $[\mathbb{L} : \mathbb{K}]$.

Exemples :

1. L'extension $\mathbb{C}/\mathbb{R}$ est galoisienne.
2. Plus généralement ...
   - En caractéristique différente de 2, toute extension quadratique est galoisienne. En effet, une telle extension est (modulo isomorphisme) de la forme $\mathbb{K}(\sqrt{d})$, avec d non carré dans $\mathbb{K}$ et donc possède uniquement deux automorphismes : l'identité et la "conjugaison" $a+b\sqrt{d} \mapsto a-b\sqrt{d}$.
   - Les contrées lointaines de caractéristique 2 abritent deux types d'extensions quadratiques : celles du types $\mathbb{K}[X]/(X^2-t)$, avec t non carré dans $\mathbb{K}$, qui sont inséparables donc non galoisiennes et celles de la forme $\mathbb{K}[X]/(X^2+X+c)$, avec c n'étant pas de la forme $c=u^2+u$, $u \in \mathbb{K}$. Ces dernières possèdent un automorphisme non trivial envoyant $\overline{X}$ sur $\overline{X}+1$ et sont donc galoisiennes.
3. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas galoisienne. En effet, $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \cong \mathrm{Rac}_{\mathbb{Q}}(X^3-2)$ et donc $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}\}$.

Proposition 5.2.5
Soit $\mathbb{L}/\mathbb{K}$ une extension finie.
Les propriétés suivantes sont alors équivalentes :

(i) $\mathbb{L}/\mathbb{K}$ *est galoisienne ;*
(ii) $\mathbb{L}/\mathbb{K}$ *est séparable et tout* $\mathbb{K}$*–plongement de* $\mathbb{L}$ *dans une clôture algébrique de* $\mathbb{L}$ *a pour image* $\mathbb{L}$ *;*
(iii) $\mathbb{L}/\mathbb{K}$ *est séparable et tout polynôme irréductible* $P \in \mathbb{K}[X]$ *admettant une racine sur* $\mathbb{L}$ *est scindé sur* $\mathbb{L}$ *;*
(iv) $\mathbb{L}$ *est un corps de décomposition d'une polynôme séparable de* $\mathbb{K}[X]$.

Exemples :

1. On considère l'extension $\mathbb{L} := \mathbb{Q}(\sqrt[3]{2})$ du corps $\mathbb{Q}$ et on pose $\alpha_1 := \sqrt[3]{2}$, $\alpha_2 := j\sqrt[3]{2}$ et $\alpha_3 := j^2\sqrt[3]{2}$. Un clôture algébrique de $\mathbb{L}$ est alors le corps $\overline{\mathbb{Q}}$ des nombres algébriques. Alors :
   - $\mathbb{L}/\mathbb{Q}$ ne vérifie pas la condition (i) car $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{L}) \cong \mathrm{Rac}_{\mathbb{L}}(X^3-2) = \{\sqrt[3]{2}\}$;
   - $\mathbb{L}/\mathbb{Q}$ ne vérifie pas la condition (ii) car le plongement (dans $\overline{\mathbb{Q}}$) défini par $\alpha_1 \mapsto \alpha_2$ envoie $\mathbb{L}$ sur $\mathbb{Q}(\alpha_2) \neq \mathbb{L}$;
   - $\mathbb{L}/\mathbb{Q}$ ne vérifie pas la condition (ii) car X^3-2 est irréductible sur $\mathbb{Q}$ et n'admet qu'une seule racine dans $\mathbb{L}$;
   - de fait, (iv) n'est pas non plus vérifiée ...
2. On conserve les notations du 1. et on pose $\mathbb{M} := \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$ (de fait, $\mathbb{M} = \mathbb{Q}(\alpha_1, j)$). Alors $\mathbb{M}$ est le corps de décomposition dans $\overline{\mathbb{Q}}$ du polynôme séparable sur $\mathbb{Q}$ X^3-2, donc l'extension $\mathbb{M}/\mathbb{Q}$ est galoisienne et $[\mathbb{M}:\mathbb{Q}] = 6$. De fait, $G := \mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ est d'ordre 6 et laisse stable l'ensemble $\mathcal{R} := \{\alpha_1,\alpha_2,\alpha_3\} \subset \mathbb{M}$. On obtient donc, par action de G sur $\mathcal{R}$, un morphisme de groupes $\rho : G \to \mathfrak{S}(\mathcal{R}) \cong \mathfrak{S}_3$. Or, ρ est injectif car si $\sigma \in \mathrm{Ker}(\rho)$, σ laisse stable les α_i et donc $\sigma = \mathrm{id}_{\mathbb{M}}$. En conclusion, on a par égalité de cardinaux que :
$$G \cong \mathfrak{S}_3$$
   Par exemple, la restriction τ à $\mathbb{M}$ de la conjugaison complexe a pour image (dans $\mathfrak{S}(\mathcal{R})$) la transposition $\rho(\tau) = (\alpha_2 \quad \alpha_3)$.
3. Une fois n'est pas coutume, conservons les notations des points précédents et posons $E := \mathbb{Q}(j)$. Le groupe G laisse stable l'ensemble $T := \{j, j^2\} = \mathrm{Rac}_{\mathbb{C}}(X^2+X+1)$. On a de facto un morphisme de groupes $\theta : G \to \mathfrak{S}(T) \cong \mathfrak{S}_2$, qui est surjectif car $\theta(\tau) = (j \quad j^2)$. De plus, comme le seul morphisme non trivial de $\mathfrak{S}_3$ dans $\{-1,1\}$ est la signature donc :
$$\begin{aligned}\forall \sigma \in G,\ \sigma(j) = j &\Leftrightarrow \sigma_{|_E} = \mathrm{id}_E \\ &\Leftrightarrow \rho(\sigma) \text{ est paire} \\ &\Leftrightarrow \sigma_{|_{\mathcal{R}}} \text{ est l'identité ou un cycle d'ordre 3}\end{aligned}$$
   De plus :
$$\begin{aligned}\forall \sigma \in G,\ \sigma(j) = j^2 &\Leftrightarrow \sigma_{|_E} \text{ est la restriction à } E \text{ de la conjugaison complexe} \\ &\Leftrightarrow \rho(\sigma) \text{ est impaire} \\ &\Leftrightarrow \sigma_{|_{\mathcal{R}}} \text{ est une transposition}\end{aligned}$$

En conclusion, $\forall\sigma \in G$, $\sigma(E) = E$ et $\sigma(\mathbb{L}) \neq \mathbb{L}$ en général.

Proposition 5.2.6 (Indice d'un sous–groupe)
Soit G un groupe fini.
Soit H un sous groupe de G.
On appelle alors indice de H dans G la quantité $(G : H) := \operatorname{card}(G/H)$. On a de plus :

$$\operatorname{card}(G) = (G : H)\operatorname{card}(H)$$

Lemme 5.2.1 (Artin)
Soit $\mathbb{L}$ un corps.
Soit G un sous groupe fini de $\operatorname{Aut}(\mathbb{L})$.
Soit $\mathbb{K} := \{x \in \mathbb{L} \mid \forall\sigma \in G,\, \sigma(x) = x\}$ (on note souvent[2] cet ensemble $\mathbb{L}^G$).
Alors :

(i) $\mathbb{K}$ *est un sous–corps de* $\mathbb{L}$ *;*
(ii) $[\mathbb{L} : \mathbb{K}] = \operatorname{card}(G)$.

En particulier, $\mathbb{L}/\mathbb{K}$ est une extension galoisienne (donc finie) de groupe de Galois G.

Théorème 5.2.7 (Correspondance de Galois)
Soit $\mathbb{L}/\mathbb{K}$ une extension finie galoisienne.
Soit G le groupe de Galois de $\mathbb{L}/\mathbb{K}$.
Alors :

(i) pour tout sous–groupe H de G, l'ensemble $\mathbb{L}^H := \{x \in \mathbb{L} \mid \forall\sigma \in H,\, \sigma(x) = x\}$ est un sous–corps de $\mathbb{L}$ contenant $\mathbb{K}$ et :

$$[\mathbb{L}^H : \mathbb{K}] = (G : H) \ \textit{i.e}\ [\mathbb{L} : \mathbb{L}^H] = \operatorname{card}(H)$$

(ii) pour tout sous–corps E de $\mathbb{L}$ contenant $\mathbb{K}$, l'extension $\mathbb{L}/E$ est galoisienne et :

$$\operatorname{Gal}(\mathbb{L}/E) = \{\sigma \in G \mid \forall x \in E,\, \sigma(x) = x\}$$

(iii) les applications $H \mapsto \mathbb{L}^H$ et $E \mapsto \operatorname{Gal}(\mathbb{L}/E)$ sont des bijections réciproques, décroissantes pour l'inclusion, entre l'ensemble des sous–groupes de G et celui des sous–corps de $\mathbb{L}$ contenant $\mathbb{K}$.

Démonstration :

(i) Découle du lemme 5.2.1.

(ii) Soit E un sous–corps de $\mathbb{L}$ contenant $\mathbb{K}$. Comme $\mathbb{L}/\mathbb{K}$ est galoisienne, $\mathbb{L}$ est corps de décomposition d'un polynôme séparable $P \in \mathbb{K}[X]$, de fait il en est aussi le corps de décomposition sur E et P est séparable sur E. Ainsi, $\mathbb{L}/E$ est galoisienne et :

$$\operatorname{Gal}(\mathbb{L}/E) = \{\sigma \in G \mid \forall x \in E,\, \sigma(x) = x\}$$

(iii) Il est clair que les deux applications considérées sont décroissantes.
- Si E est un sous–corps de $\mathbb{L}$ contenant $\mathbb{K}$ et que l'on pose $E' = \mathbb{L}^{\operatorname{Gal}(\mathbb{L}/E)}$, il est trivial que $E \subset E'$. Inversement, par définition de E', on a que $\operatorname{Aut}(\mathbb{L}/E') = \operatorname{Aut}(\mathbb{L}/E)$. Ainsi, $[\mathbb{L} : E] = [\mathbb{L} : E']$ (les deux extensions sont galoisiennes d'après le (ii)). De facto, on a bien $E = E'$.
- Inversement, si H est un sous–groupe de G, il est clair que $H \subset \operatorname{Gal}(\mathbb{L}/\mathbb{L}^H)$. De plus, on a par le (i) que $[\mathbb{L} : \mathbb{L}^H] = \operatorname{card} H$ donc $H = \operatorname{Gal}(\mathbb{L}/\mathbb{L}^H)$ d'où le résultat.

Proposition 5.2.8 (Propriétés de la correspondance de Galois)
Soit $\mathbb{L}/\mathbb{K}$ une extension (finie) galoisienne de groupe de Galois G.
Soient H et H' deux sous–groupes de G. On note $\langle H, H'\rangle$ le sous–groupe engendré par $H \cup H^prime$.
Alors :

(i) $\mathbb{L}^{\langle H,H'\rangle} = \mathbb{L}^H \cap \mathbb{L}^{H^prime}$ *;*
(ii) $\mathbb{L}^{H\cap H'} = \mathbb{K}(\mathbb{L}^H \cup \mathbb{L}^{H'})$ *;*
(iii) $\forall\sigma \in G$, $\sigma(\mathbb{L}^H) = L^{\sigma H\sigma^{-1}}$ *;*
(iv) $\mathbb{L}^H/\mathbb{K}$ *est galoisienne* $\Leftrightarrow$ $H \lhd G$*. Dans ce cas, on a de plus :*

$$\operatorname{Gal}(\mathbb{L}^H/\mathbb{K}) \cong G/H$$

2. Et en particulier lorsque l'on fait de la théorie des groupes.

5.3 Applications aux extensions finies séparables

Dans ce tout paragraphe, on se donne un corps $\mathbb{K}$ et un clôture algébrique Ω de $\mathbb{K}$. Pour simplifier, toutes les extensions considérées seront considérées incluses dans Ω et contenant $\mathbb{K}$.

Proposition 5.3.1 (Enveloppe galoisienne)
Soit $\mathbb{L}/\mathbb{K}$ une extension finie séparable.
Alors il existe une plus petite extension $\mathbb{M}/\mathbb{L}$ galoisienne sur $\mathbb{K}$, appelée enveloppe galoisienne de $\mathbb{L}$.

Démonstration : On sait que $\mathbb{L} = \mathbb{K}(a_1, \dots, a_n)$, avec les $a_i \in \Omega$ de polynômes minimaux sur $\mathbb{K}$ P_i séparables. Il nous suffit alors de prendre pour $\mathbb{M}$ le corps de décomposition du ppcm des P_i.

Proposition 5.3.2
Soit $\mathbb{L}/\mathbb{K}$ une extension finie séparable.
Alors l'enveloppe galoisienne $\mathbb{M}$ de $\mathbb{L}$ est l'extension engendrée par $\bigcup_{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)} \sigma(\mathbb{L})$, i.e (avec les notations de la démonstration de la proposition 5.3.1) par les $(\sigma(a_i))_{1 \leq i \leq n,\, \sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)}$.

Définition 5.3.1 (Conjugués d'un élément séparable)
Soit $\alpha \in \Omega$ un élément séparable sur $\mathbb{K}$.
Soit P le polynôme minimal (séparable) de α sur $\mathbb{K}$.
Alors les racines de P sont appelés conjugués de α sur $\mathbb{K}$. Il s'agit de fait des images de α par les $\mathbb{K}$–plongements de $\mathbb{K}(\alpha)$ dans Ω.

Proposition 5.3.3
Soit $\mathbb{M}/\mathbb{L}$ une extension galoisienne de groupe de Galois G.
Soit $\alpha \in \mathbb{M} \subset \Omega$ un élément séparable sur $\mathbb{K}$.
Alors les conjugués de α sur $\mathbb{K}$ sont les $g(\alpha)$ pour $g \in G$, i.e les éléments de l'orbite de α sous l'action de G sur $\mathbb{M}$.

Exemples :

1. Les conjugués de i sur $\mathbb{Q}$ sont i et $-i$.
2. Les conjugués de $\sqrt[3]{2}$ sur $\mathbb{Q}$ sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.

Proposition 5.3.4
Soit $\mathbb{L}/\mathbb{K}$ une extension finie séparable.
Alors l'ensemble des corps intermédiaires de $\mathbb{L}/\mathbb{K}$ (i.e des sous–corps de $\mathbb{L}$ contenant $\mathbb{K}$) est fini.

Démonstration : D'après la proposition 5.3.1, on peut supposer que $\mathbb{L}/\mathbb{K}$ est galoisienne. De fait, par correspondance de Galois, l'ensemble des corps intermédiaires de $\mathbb{L}/\mathbb{K}$ est alors équipotent à l'ensemble (fini !) de sous groupes de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

✗ Cette propriété est fausse dans le cas inséparable !
En effet, si l'on se donne un corps k infini de caractéristique $p > 0$ et que l'on pose $\mathbb{M} := k(X, Y)$ et $\mathbb{K} := k(X^p, Y^p)$ ($\mathbb{M}/\mathbb{K}$ est alors de degré p^2), alors les corps (pour $t \in k$) $\mathbb{L}_t := \mathbb{K}(X+tY) = k(X^p, Y^p; X+ty)$ sont des corps intermédiaires deux à deux distincts de $\mathbb{M}/\mathbb{K}$.

Proposition 5.3.5 (Structure du groupe des inversibles d'un corps fini)
Soit $\mathbb{F}$ un corps fini de cardinal q.
Alors le groupe $(\mathbb{F}^\times, \times)$ est cyclique d'ordre $q-1$.

Lemme 5.3.1
Soit $\mathbb{K}$ un corps infini.
Soit V un $\mathbb{K}$–e.v.
Soient $W_1, \dots, W_n \subsetneq V$ des s–e.v strict de V.
Alors :

$$\bigcup_{i=1}^{n} W_i \neq V$$

Démonstration : Récurrence sur n.

Proposition 5.3.6 (Théorème de l'élément primitif)

Soit $\mathbb{L}/\mathbb{K}$ *une extension finie séparable.*
Alors $\mathbb{L}/\mathbb{K}$ *est monogène.*

DÉMONSTRATION :
- Si $\mathbb{K}$ est fini, alors $\mathbb{L}$ aussi et donc, d'après la proposition 5.3.5, le groupe $\mathbb{L}^\times$ est cyclique. De fait, $\mathbb{L}/\mathbb{K}$ est bien monogène.
- Dans le cas contraire, on remarque que :

$$\mathbb{L} = \bigcup_{\alpha \in \mathbb{L}} \mathbb{K}(\alpha)$$

Par proposition 5.3.4, l'ensemble des $\mathbb{K}(\alpha)$ est fini. En contraposant le lemme 5.3.1, on aboutit donc à la conclusion que l'un d'entre eux est égal à $\mathbb{L}$.

Exemple : L'extension $\mathbb{Q}(j, \sqrt[3]{2})$ de $\mathbb{Q}$ est monogène égale à $\mathbb{Q}(j + \sqrt[3]{2})$.

5.4 Corps finis

Définition 5.4.1 (Extension galoisienne cyclique)
Une extension galoisienne est dite cyclique si son groupe de Galois l'est.

Proposition 5.4.1
Soit p *un nombre premier positif.*
Soit Ω *un clôture algébrique du corps* $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
Alors :

(i) *pour tout* $s \in \mathbb{N}^*$, *il existe une unique (dans* Ω*) extension de degré* s *de* $\mathbb{F}^p$, *notée* $\mathbb{F}_{p^s}$ *;*

(ii) *cette extension est galoisienne cyclique et :*

$$\mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p) \cong \mathbb{Z}/s\mathbb{Z}$$

Via $(a \bmod s) \mapsto (\varphi^a : x \mapsto x^{p^s})$.

DÉMONSTRATION :
- Donnons nous un corps fini $\mathbb{F}$ de caractéristique p. Un tel corps est nécessairement une extension finie de $\mathbb{F}_p$, et si on pose $s := [\mathbb{F} : \mathbb{F}_p]$ on a (au sens des espaces vectoriels) :

$$\mathbb{F} \cong \mathbb{F}_p^s$$

Ainsi, $q := \mathrm{card}(\mathbb{F}) = p^s$.
Fixons nous à présent une clôture algébrique Ω de $\mathbb{F}$. D'après la proposition 5.3.5, le groupe $\mathbb{F}^\times$ est cyclique d'ordre $q-1$. De fait :

$$\forall x \in \mathbb{F}^\times,\ x^{q-1} = 1 \text{ i.e } \forall x \in \mathbb{F},\ x^q = x$$

Ce qui revient à dire que les $q-1$ (resp. q) éléments de $\mathbb{F}^\times$ (resp. $\mathbb{F}$) sont racines de $X^{q-1} - 1$ (resp. $X^q - X$). On a donc, du fait de leur degré, déterminé toutes les racines —qui sont de plus simples— de ces deux polynômes sur $\mathbb{F}$. On en déduit les identités :

$$X^{q-1} - 1 = \prod_{a \in \mathbb{F}^\times} (X - a) \text{ et } X^q - X = \prod_{a \in \mathbb{F}} (X - a)$$

De facto, $\mathbb{F}$ est le corps de décomposition (dans Ω) de $X^{q-1} - 1$ et $X^q - 1$. Par conséquent :
- $\mathbb{F}/\mathbb{F}_p$ est une extension galoisienne ;
- $\mathbb{F}$ est le seul sous–corps à q éléments de Ω ;
- $\mathbb{F} = \{x \in \Omega \mid x^q = x\}$ donc $\mathbb{F}$ est le corps des invariants du morphisme de Frobénius "itéré" $\varphi^s(x \in \Omega) \mapsto x^{p^s}$;
- si on note $\varphi : \Omega \to \Omega$ le morphisme de Frobénius, alors $\varphi_{|\mathbb{F}} \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$;
- les points fixes de $\varphi_{|\mathbb{F}}$ sont les éléments de $\mathbb{F}_p$

  - le sous–groupe $\langle \varphi_{|\mathbb{F}} \rangle$ engendré par $\varphi_{|\mathbb{F}}$ dans $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ vérifie $\mathbb{F}^{\langle \varphi_{|\mathbb{F}} \rangle} = \mathbb{F}_p$ et donc (par correspondance de Galois) :
$$\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p) = \langle \varphi_{|\mathbb{F}} \rangle$$
  - $\mathbb{F}/\mathbb{F}^p$ est une extension galoisienne cyclique (au sens de la définition 5.4.1), plus précisément $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ est un groupe cyclique d'ordre s engendré par $\varphi_{|\mathbb{F}}$.
- Inversement, si on fixe $s \geq 1$ et $q := p^s$, les invariants de φ^s forment un sous–corps de $\mathbb{F}' \subset \Omega$ qui est (par définition) l'ensemble des racines de $X^q - X$. Or, ce polynôme est séparable (sa dérivée vaut -1) donc possède exactement q racines dans Ω, d'où $\mathrm{card}\,\mathbb{F}' = q = p^s$.

Corollaire 5.4.1.1
Soit p un nombre premier positif.
Soient $s, t \in \mathbb{N}^*$.
Alors :
$$\mathbb{F}_{p^s} \subset \mathbb{F}_{p^t} \Leftrightarrow s|t$$
Et dans ce cas $\mathrm{Gal}(\mathbb{F}_{p^t}/\mathbb{F}_{p^s})$ est un groupe cyclique d'ordre $\dfrac{t}{s}$.

Proposition 5.4.2
Soit p un nombre premier positif impair.
On a alors équivalence entre les propositions suivantes :
(i) -1 *est un carré modulo* p *;*
(ii) $p \equiv 1[4]$.

DÉMONSTRATION : On sait qu'il existe une racine x de $X^2 + 1$ dans une extension finie de $\mathbb{F}_p$. De fait :
$$x \in \mathbb{F}_p \Leftrightarrow x^p = x$$
De plus, $x^2 = -1 \neq 1$ car $p \neq 2$ et $x^4 = 1$ donc x est d'ordre 4. Or, si $a, b \in \mathbb{Z}$ on a :
$$x^a = x^b \Leftrightarrow x^{b-a} = 1 \Leftrightarrow b - a \equiv 0[4] \text{ car } x \text{ est d'ordre } 4$$
D'où le résultat.

Exemple : -1 est un carré modulo 13, de racines 5 et -5. Ainsi :
$$X^2 + 1 = (X - 5)(X + 5) \text{ dans } \mathbb{F}_13$$