

Notes du cours “Algèbre 1”

Master 1

Paul-Emile PARADAN*

2024

Table des matières

1	Rappels sur les anneaux	3
1.1	Anneaux, sous-anneaux, morphismes	3
1.2	Idéaux	4
1.3	Anneaux quotients	5
1.4	Localisation	8
1.5	Idéaux premiers, idéaux maximaux	9
1.6	Divisibilité dans un anneau intègre	10
1.7	Anneaux principaux	11
1.8	Anneaux factoriels	13
2	Modules sur un anneau	16
2.1	Premières définitions	16
2.1.1	Modules et sous-modules	16
2.1.2	Morphismes entre modules	18
2.1.3	Factorisation	19
2.1.4	Opérations sur les modules et sous-modules	20
2.2	Modules de type fini, modules libres	20
2.3	Modules de type fini sur un anneau principal	22
2.3.1	Sous-modules d’un module libre de rang fini	22
2.3.2	Modules de type fini : théorème de structure	25
2.3.3	Unicité	26
2.4	Quelques applications	28
2.4.1	Groupes abéliens de type fini	28
2.4.2	Réduction des matrices de $M_{p,q}(\mathbb{Z})$	28
2.4.3	Réduction des endomorphismes d’un \mathbb{K} -espace vectoriel de dimension finie	31

*Institut Montpellierain Alexander Grothendieck, CNRS, Université de Montpellier, paul-emile.paradan@umontpellier.fr

3	Produit tensoriel	34
3.1	Applications bilinéaires	34
3.2	Définition du produit tensoriel	35
3.3	Quelques propriétés du produit tensoriel	36
3.4	Algèbre extérieure et produit symétrique d'un espace vectoriel	38
4	Représentations de groupes finis	38
4.1	Premières notions	38
4.1.1	Sous-représentations et quotients	39
4.1.2	Morphismes entre deux représentations	40
4.1.3	Somme et produit tensoriel	41
4.1.4	Représentations irréductibles	41
4.1.5	Lemme de Schur	42
4.2	Le cas des groupes finis	43
4.2.1	L'algèbre $\mathbb{C}[G]$	43
4.2.2	Projection sur les invariants	45
4.2.3	Décomposition en facteurs irréductibles	46
4.2.4	Caractère d'une représentation	47
4.2.5	Premier pas vers la classification des représentations irréductibles	49

1 Rappels sur les anneaux

1.1 Anneaux, sous-anneaux, morphismes

Un anneau A est un ensemble muni de deux lois internes "+" et "." vérifiant

1. $(A, +)$ est un groupe abélien : son élément neutre est noté 0.
2. La loi "." est associative, avec un élément neutre noté 1.
3. La loi "." est distributive par rapport à "+" : $\forall x, y, z \in A, x \cdot (y+z) = x \cdot y + x \cdot z$.

L'anneau est dit commutatif si la loi "." est commutative. **Dans ces notes, nous ne considérons que des anneaux commutatifs, sauf indication contraire.** Dans la suite, le produit $x \cdot y$ est noté xy .

Rappelons quelques notions associées à un anneau commutatif A :

1. $x \in A$ est *invertible* si $\exists y \in A$ tel que $xy = 1$: l'élément $y \in A$ est unique, et il est appelé l'inverse de x .
2. $x \in A$ est un *diviseur de zéro* si $x \neq 0$ et si $\exists y \neq 0$ tel que $xy = 0$.
3. $x \in A$ est *nilpotent* si $\exists n \geq 1$ tel que $x^n = 0$.
4. A est dit *intègre* si $\forall x, y \in A, xy = 0 \implies x = 0$ ou $y = 0$.
5. A est un *corps* si tout élément non nul de A est invertible.

Définition 1.1 Notons A^\times l'ensemble des éléments invertibles de A . On remarque que (A^\times, \cdot) est un groupe abélien.

Exercice 1.2 Montrer les faits suivants dans un anneau commutatif A :

- Si $x, y \in A$ sont nilpotents, alors $x + y$ est nilpotent.
- Si $x \in A^\times$ et y est nilpotent, alors $x + y \in A^\times$.
- Si A a un nombre fini d'éléments, alors A intègre $\iff A$ est un corps.

Voici quelques exemples d'anneaux commutatifs :

- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
- $\mathbb{Z}/N\mathbb{Z}$ pour tout $N \geq 2$.
- Anneaux de polynômes $A[X], A[X, Y], A[X_1, \dots, X_n]$.
- Anneaux de séries formelles $A[[X]]$.
- Anneau produit $A := A_1 \times \dots \times A_p$.

Exercice 1.3 — Montrer que $(A[X])^\times = A^\times$ lorsque A est intègre.

- Montrer que $(\mathbb{Z}/4\mathbb{Z}[X])^\times$ possède une infinité d'éléments.
- Montrer que $P = \sum_{k \in \mathbb{N}} a_k X^k \in A[[X]]$ est invertible ssi $a_0 \in A^\times$.

Définition 1.4 Un sous-ensemble $B \subset A$ est un sous-anneau de A si

- $(B, +)$ est un sous-groupe de $(A, +)$.
- $\forall x, y \in B, xy \in B$.
- $1 \in B$.

Voici des exemples élémentaires de sous-anneaux :

- \mathbb{Z} est un sous-anneau de \mathbb{Q} .
- $\mathbb{Z}[X] \subset \mathbb{Q}[X] \subset \mathbb{R}[X]$ sont des sous-anneaux de $\mathbb{C}[X]$.

Soient A_1 et A_2 deux anneaux commutatifs. Une application $\varphi : A_1 \rightarrow A_2$ est un *morphisme d'anneaux* si

- $\forall a, b \in A_1, \varphi(a + b) = \varphi(a) + \varphi(b)$.
- $\forall a, b \in A_1, \varphi(ab) = \varphi(a)\varphi(b)$.
- $\varphi(1) = 1$.

On note que l'image de φ , notée $\varphi(A_1)$, est un sous-anneau de A_2 .

Voici quelques exemples de morphismes.

Exemple 1.5 Soit $\varphi : A \rightarrow B$ un morphisme d'anneaux. Alors l'application $\tilde{\varphi} : A[X] \rightarrow B[X]$ définie par $\tilde{\varphi}(\sum_{k=0}^n a_k X^k) = \sum_{k=0}^n \varphi(a_k) X^k$ est un morphisme d'anneaux.

Exemple 1.6 Soit A un sous-anneau de B . Pour tout $\beta \in B$, l'application le morphisme d'anneaux $\phi_\beta : A[X] \rightarrow B$ définie par $\phi_\beta(\sum_{k=0}^n a_k X^k) = \sum_{k=0}^n a_k \beta^k$ est un morphisme d'anneaux.

L'image de ϕ_β est notée $A[\beta]$: c'est le plus petit sous-anneau de B contenant A et β .

Ainsi pour tout $z \in \mathbb{C}$, on définit les sous-anneaux $\mathbb{Z}[z] \subset \mathbb{Q}[z]$ de \mathbb{C} .

1.2 Idéaux

Soit A un anneau commutatif.

Définition 1.7 $I \subset A$ est un idéal de A si

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

Définition 1.8 Un idéal $I \subset A$ est dit principal s'il existe $a \in A$ tel que $I = \{xa, x \in A\}$. Cet idéal, noté (a) ou bien aA , est le plus petit idéal de A contenant a .

Nous avons des opérations élémentaires sur les idéaux. Soient I, J deux idéaux de A . On définit alors les idéaux suivants :

- $I \cap J$,
- $I + J := \{a + b; (a, b) \in I \times J\}$,
- $IJ = \{\sum_{k=1}^n a_k b_k; (a_k, b_k) \in I \times J, \forall k\}$.

De manière générale, si $I_k, k \in \mathcal{X}$ est une famille d'idéaux de A , l'intersection

$$\bigcap_{k \in \mathcal{X}} I_k$$

est un idéal de A .

A toute partie $T \subset A$, on associe

$$(T) := \bigcap_{I \text{ idéal}, T \subset I} I,$$

qui est le plus petit idéal contenant T .

Voici quelques propriétés faciles à démontrer.

Proposition 1.9 — Soit $I \subset A$ un idéal. Alors $I = A \iff 1 \in I$.

- Si A est intègre, $(x) = (y) \iff \exists u \in A^\times, x = uy$.
- Si $\varphi : A \rightarrow B$ est un morphisme d'anneaux, alors

$$\ker(\varphi) := \{x \in A, \varphi(x) = 0\}$$

est un idéal de A .

- Si $T = \{x_1, \dots, x_p\}$ alors, $(T) = (x_1) + \dots + (x_p)$.
- $I + J = (I \cup J)$.
- $IJ \subset I \cap J$.
- $IJ = I \cap J$ si $I + J = A$.

Le radical d'un idéal $I \subset A$ est l'idéal suivant :

$$\sqrt{I} := \{x \in A, \exists n \geq 1, x^n \in I\}.$$

Petit exercice d'entraînement : vérifier que \sqrt{I} est bien un idéal de A .

Le radical de $I = \{0\}$ est appelé le *nilradical* de A :

$$\text{Nil}(A) := \{x \in A, x \text{ nilpotent}\}.$$

Exercice 1.10 — Dans \mathbb{Z} , expliciter l'idéal $\sqrt{(300)}$.

- Expliciter le nilradical de l'anneau $\mathbb{Z}/36\mathbb{Z}$.

1.3 Anneaux quotients

Soit I un idéal d'un anneau commutatif A . Considérons la relation d'équivalence \sim_I sur A définie par : $\forall x, y \in A$,

$$x \sim_I y \iff x - y \in I.$$

La classe d'équivalence de $x \in A$ est le sous-ensemble $\bar{x} := x + I \subset A$.

Définition 1.11 1. On note $A/I \subset \mathcal{P}(A)$ l'ensemble des classes d'équivalences de \sim_I .

2. On note $\pi_I : A \rightarrow A/I$ la surjection définie par $\pi(x) = \bar{x}$.

Proposition 1.12 A/I possède une structure d'anneau pour laquelle l'application $\pi_I : A \rightarrow A/I$ est un morphisme d'anneau.

La loi "+" sur A/I est définie par les relations

$$\bar{x} + \bar{y} = \overline{x + y}, \quad \forall x, y \in A.$$

L'égalité précédente est bien définie car si $\bar{x} = \bar{a}$ et $\bar{y} = \bar{b}$, alors $\overline{x + y} = \overline{a + b}$. L'élément neutre pour $(A/I, +)$ est $\bar{0}$.

La loi "." sur A/I est définie par les relations

$$\bar{x} \cdot \bar{y} = \overline{xy}, \quad \forall x, y \in A.$$

L'égalité précédente est bien définie car si $\bar{x} = \bar{a}$ et $\bar{y} = \bar{b}$, alors $\overline{xy} = \overline{ab}$. L'élément neutre pour $(A/I, \cdot)$ est $\bar{1}$.

Voici un exemple fondamental.

Exemple 1.13 Considérons l'anneau quotient $M := \mathbb{R}[X]/I$ où I est l'idéal principal $(X^2 + 1)$.

1. Vérifier que pour tout $m \in M$, il existe un unique couple $(a, b) \in \mathbb{R}^2$ tel que $m = \bar{a} + b\bar{X}$.
2. Vérifier que l'application $\varphi : M \rightarrow \mathbb{C}$, définie par $\varphi(\bar{a} + b\bar{X}) := a + ib$, est un isomorphisme d'anneaux.

Soit $\varphi : A \rightarrow B$ un morphisme d'anneau. Notons $\pi_\varphi : A \rightarrow A/\ker(\varphi)$ le morphisme canonique.

Proposition 1.14 L'application $\bar{\varphi} : A/\ker(\varphi) \rightarrow B$ définie par la relation $\bar{\varphi}(\bar{x}) = \varphi(x), \forall x \in A$, est un morphisme d'anneau injectif. De plus, on a la relation $\varphi = \bar{\varphi} \circ \pi_\varphi$.

Considérons l'application $\varphi^{-1} : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$ définie par la relation $\varphi^{-1}(\mathcal{Y}) = \{x \in A, \varphi(x) \in \mathcal{Y}\}$ pour tout $\mathcal{Y} \subset B$.

Proposition 1.15 1. Si J est un idéal de B , alors $\varphi^{-1}(J)$ est un idéal de A contenant $\ker(\varphi)$.

2. Supposons φ surjectif. Dans ce cas :

- φ^{-1} détermine une bijection entre les idéaux de B et les idéaux de A qui contiennent $\ker(\varphi)$.
- Pour tout idéal J de B , le morphisme φ induit un isomorphisme $A/\varphi^{-1}(J) \xrightarrow{\sim} B/J$.

Considérons un premier exemple d'application de la proposition 1.14. Soit $\alpha \in A$, et $\pi_\alpha : A \rightarrow A/\alpha A$ le morphisme quotient (ici αA désigne l'idéal engendré par α). On a vu dans l'exemple 1.5 que π_α permet de définir un morphisme d'anneaux

$$\tilde{\pi}_\alpha : A[X] \rightarrow A/\alpha A[X].$$

On voit alors que $\ker(\tilde{\pi}_\alpha)$ est égal à l'idéal $\alpha A[X]$. Grâce à la proposition 1.14 on sait que le morphisme $\tilde{\pi}_\alpha$ induit un isomorphisme d'anneaux

$$A[X]/\alpha A[X] \xrightarrow{\sim} A/\alpha A[X]. \quad (1)$$

Considérons un autre exemple de passage au quotient. Soient $I \subset J$ deux idéaux de A . On considère le morphisme

$$\pi_I : A \rightarrow A/I.$$

L'image $\pi_I(J)$ est un idéal de A/I que l'on note J/I . On considère alors le quotient de l'anneau A/I par rapport à l'idéal J/I . C'est un anneau noté $(A/I)/(J/I)$. Considérons le morphisme quotient $\pi_{J/I} : A/I \rightarrow (A/I)/(J/I)$, et le morphisme d'anneaux

$$\varphi = \pi_{J/I} \circ \pi_I : A \rightarrow (A/I)/(J/I).$$

Proposition 1.16 1. φ est surjectif.

2. Le noyau de φ est égal à J .

3. Le morphisme $\bar{\varphi} : A/J \rightarrow (A/I)/(J/I)$ est bijectif.

Nous allons regarder un exemple qui permettra de comprendre l'utilité de l'isomorphisme $A/J \simeq (A/I)/(J/I)$.

On considère l'anneau quotient $\mathbb{K} = \mathbb{Z}[X]/(3, 1 + X^2)$. Ici $J = (3, 1 + X^2) = (3) + (1 + X^2)$ est un idéal de $A = \mathbb{Z}[X]$ contenant $I = (3)$. En utilisant (1), on voit que l'anneau quotient A/I est isomorphe à $\mathbb{Z}/3\mathbb{Z}[X]$ et que l'idéal J/I est égal à $(X^2 + 1) \subset \mathbb{Z}/3\mathbb{Z}[X]$. Ainsi l'anneau $(A/I)/(J/I)$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}[X]/(X^2 + 1)$. D'après la proposition précédente, on peut conclure que

$$\mathbb{K} \simeq \mathbb{Z}/3\mathbb{Z}[X]/(X^2 + 1).$$

On verra à la section 1.7 que $\mathbb{Z}/3\mathbb{Z}[X]/(X^2 + 1)$ est un corps de cardinal 9.

On termine cette section avec le lemme chinois.

Soient I, J deux idéaux de A tels que $I + J = A$. On considère le morphisme d'anneau $\varphi : A \rightarrow A/I \times A/J$ défini par $\varphi(x) = (\pi_I(x), \pi_J(x))$. C'est immédiat de voir que $\ker(\varphi) = I \cap J$: de plus la relation $I + J = A$ implique que $I \cap J = IJ$. Vérifions maintenant que φ est surjective.

Comme $I + J = A$, il existe $a \in I$ et $b \in J$ tel que $a + b = 1$. Considérons $(\pi_I(x), \pi_J(y)) \in A/I \times A/J$ et posons $z = ay + bx$. Les relations $ax + bx = x$ et $ay + by = y$ permettent de voir que $\pi_I(z) = \pi_I(x)$, et $\pi_J(z) = \pi_J(y)$. Ainsi $\varphi(z) = (\pi_I(x), \pi_J(y))$.

Théorème 1.17 (Lemme chinois) *Soient I, J deux idéaux de A tels que $I + J = A$. Alors l'application $\bar{\varphi} : A/IJ \rightarrow A/I \times A/J$ est un isomorphisme d'anneaux.*

1.4 Localisation

Définition 1.18 *Une partie $S \subset A$ est dite multiplicative si*

1. $1 \in S$,
2. $a, b \in S \implies ab \in S$.

Nous allons construire un anneau $S^{-1}A$ et un morphisme $j : A \rightarrow S^{-1}A$ tel que $j(S) \subset (S^{-1}A)^\times$.

Pour cela, on considère l'ensemble $A \times S$ que l'on muni de la relation d'équivalence \mathcal{R} définie de la manière suivante : $(a, s)\mathcal{R}(b, t) \iff \exists u \in S$ tel que $u(at - bs) = 0$. On note $S^{-1}A$ l'ensemble quotient $A \times S/\mathcal{R}$.

La classe de (a, s) dans $S^{-1}A$ est noté a/s , et on note $j : A \rightarrow S^{-1}A$ l'application $j(a) = a/1$.

Proposition 1.19 1. $S^{-1}A$ admet une structure d'anneau pour laquelle $j : A \rightarrow S^{-1}A$ est un morphisme d'anneaux.

2. La loi "+" sur $S^{-1}A$ est définie par les relations $a/s + b/t = (at + bs)/st$.
3. La loi "." sur $S^{-1}A$ est définie par les relations $a/s \cdot b/t = ab/st$.

On remarque que $1/s$ est l'inverse de $j(s)$ pour tout $s \in S$.

Remarque 1.20 1. Si $0 \in S$, alors l'anneau $S^{-1}A$ est réduit à $\{0\}$.

2. Si $S \subset A^\times$, alors $j : A \rightarrow S^{-1}A$ est un isomorphisme.

Un exemple important est celui d'un anneau A intègre. On peut alors considérer la partie multiplicative $S := A - \{0\}$. Dans ce cas, l'anneau $S^{-1}A$ est un corps, appelé le corps de fraction de A . Par exemple, cette construction permet de construire \mathbb{Q} à partir de \mathbb{Z} : \mathbb{Q} est le corps de fraction de \mathbb{Z} .

Voici un autre exemple : considérons la partie multiplicative $S = \{10^k, k \in \mathbb{N}\}$ de l'anneau \mathbb{Z} . Dans ce cas, $S^{-1}\mathbb{Z}$ est le sous-anneau de \mathbb{Q} formé des nombres décimaux :

$$S^{-1}\mathbb{Z} \simeq \left\{ \frac{x}{10^k}, x \in \mathbb{Z}, k \in \mathbb{N} \right\}.$$

Exercice 1.21 Notons A_s l'anneau $S^{-1}A$, lorsque $S = \{s^k, k \in \mathbb{N}\}$. Considérons le morphisme d'anneau $\varphi : A[X] \rightarrow A_s$ qui envoie un polynôme $P(X)$ sur $P(1/s)$.

1. Vérifier que φ est surjectif.
2. Montrer que $\ker(\varphi)$ est égal à l'idéal $(1 - sX)$.
3. En déduire que $A[X]/(1 - sX) \simeq A_s$.

1.5 Idéaux premiers, idéaux maximaux

On veut comprendre sous quelles conditions l'anneau quotient A/I est intègre, ou est un corps.

Définition 1.22 1. Un idéal $I \subset A$ est dit maximal si $I \neq A$, et si pour tout idéal J contenant I , on a $J = I$ ou bien $J = A$.

2. Un idéal $I \subset A$ est dit premier si $\forall x, y \in A, xy \in I \implies x \in I$ ou $y \in I$.

On peut caractériser le fait que $I \subset A$ est maximal de la manière suivante : $I \neq A$ et pour tout $a \notin I$ on a $I + (a) = A$.

Proposition 1.23 1. A/I est intègre ssi l'idéal I est premier.

2. A/I est un corps ssi l'idéal I est maximal.

Exemple 1.24 Dans l'anneau $\mathbb{R}[X, Y]$:

1. L'idéal (X) est premier, mais pas maximal.
2. L'idéal $(X) + (Y)$ est maximal.

Théorème 1.25 (Krull) Soit A un anneau (non-nul) et I un idéal de A distinct de A . Il existe un idéal maximal $M \subset A$ contenant I .

La preuve de ce théorème utilise le lemme de Zorn :

Lemme 1.26 (Zorn) Soit \mathcal{E} un ensemble munie d'une relation d'ordre¹ \leq . On suppose que toute partie $\mathcal{F} \subset \mathcal{E}$ totalement ordonnée² possède un majorant³.

Alors \mathcal{E} possède un élément maximal⁴

-
1. Attention, l'ensemble (E, \leq) n'est à priori pas totalement ordonné.
 2. Pour tout $x, y \in \mathcal{F}$, $x \leq y$ ou $y \leq x$.
 3. $m \in \mathcal{E}$ est un majorant de \mathcal{F} si $\forall x \in \mathcal{F}, x \leq m$
 4. $M \in \mathcal{E}$ est maximal si $\forall x \in \mathcal{E}, M \leq x \implies M = x$.

La preuve du Théorème de Krull s'obtient en considérant l'ensemble \mathcal{E} des idéaux J de A tels que $I \subset J \neq A$: \mathcal{E} est non-vide et il est ordonné au moyen de la relation d'inclusion \subset . On voit alors que pour partie $\mathcal{F} \subset \mathcal{E}$ totalement ordonnée, l'élément

$$J_{\mathcal{F}} = \bigcup_{J \in \mathcal{F}} J$$

est un idéal de \mathcal{E} qui majore tous les éléments de \mathcal{F} . D'après le lemme de Zorn, l'ensemble (\mathcal{E}, \subset) admet donc un élément maximal J_o . Par définition, J_o est un idéal maximal de A contenant I . \square

1.6 Divisibilité dans un anneau intègre

Dans cette section, A est un anneau intègre.

Définition 1.27 Soient $a, b \in A - \{0\}$. On dit que a divise b (notation $a \setminus b$) s'il existe $q \in A$ tel que $b = aq$. Cette dernière condition est équivalent à demander que $(b) \subset (a)$.

Définition 1.28 On dit que $a, a' \in A - \{0\}$ sont associés s'il existe un élément inversible $u \in A^\times$ tel que $a' = ua$.

Lemme 1.29 Soient $a, b \in A - \{0\}$. Les conditions suivantes sont équivalentes :

- $a \setminus b$ et $b \setminus a$,
- $(a) = (b)$,
- a et b sont associés.

Définition 1.30 Soient $a, b \in A - \{0\}$. On dit que a et b sont premiers entre eux ou sans facteur commun, si tout diviseur commun à a et b est inversible. Ceci équivaut à dire que : A est le seul idéal principal contenant a et b .

Définition 1.31 Soit A un anneau intègre.

1. $a \in A - \{0\}$ est dit irréductible si $a \notin A^\times$ et si $\forall x, y \in A$ on a :

$$a = xy \implies x \in A^\times \text{ ou } y \in A^\times.$$

2. $a \in A - \{0\}$ est dit premier si $a \notin A^\times$ et si $\forall x, y \in A$, on a :

$$a \setminus xy \implies a \setminus x \text{ ou } a \setminus y.$$

3. On remarque que "a premier" \implies "a irréductible".

Voici deux faits généraux, valables dans un anneau intègre : pour tout $a \notin A^\times \cup \{0\}$,

- a est premier si et seulement si l'idéal (a) est premier.
- a est irréductible si l'idéal (a) est maximal.

1.7 Anneaux principaux

Définition 1.32 Un anneau commutatif A est dit principal si

1. A est intègre.
2. Tout idéal de A est principal.

Définition 1.33 Un anneau commutatif A est dit euclidien si

1. A est intègre,
2. Il existe $\phi : A - \{0\} \rightarrow \mathbb{N}$ satisfaisant la condition suivante : pour tout $(a, b) \in A \times A - \{0\}$ il existe $q, r \in A$ vérifiant
 - $a = bq + r$
 - $r = 0$ ou bien $\phi(r) < \phi(b)$.

- Exemple 1.34**
1. L'anneau \mathbb{Z} est euclidien. Ici on prend $\phi(n) = |n|$.
 2. Si \mathbb{K} est un corps, l'anneau $\mathbb{K}[X]$ est euclidien. Ici $\phi : \mathbb{K}[X] - \{0\} \rightarrow \mathbb{N}$ est l'application "degré".
 3. L'anneau $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$ est euclidien. Ici $\phi(a + ib) = a^2 + b^2$.

Considérons l'anneau quotient $\mathbb{K}[X]/(P)$ où P est un polynôme non nul. L'utilisation de la division euclidienne dans $\mathbb{K}[X]$ donne une preuve directe du fait suivant.

Exercice 1.35 $\mathbb{K}[X]/(P)$ est un \mathbb{K} -espace vectoriel de dimension finie. Si $d^\circ P = n \geq 1$, alors $\{\bar{1}, \dots, \bar{X}^{n-1}\}$ est une base de $\mathbb{K}[X]/(P)$.

La prochaine proposition est fondamentale.

Proposition 1.36 Tout anneau euclidien est principal.

La preuve de ce fait est élémentaire. Si I est un idéal non nul d'un anneau euclidien, on considère $b \in I - \{0\}$ tel que $\phi(b) = \min \phi(I - \{0\})$. On montre alors, au moyen de la division euclidienne, que $I = (b)$.

Terminons cette section en abordant les questions de divisibilité dans un anneau principal.

Proposition 1.37 Dans un anneau principal A , on a l'équivalence des assertions suivantes pour $a \in A - \{0\}$:

1. L'anneau quotient $A/(a)$ est intègre.
2. a est premier.
3. a est irréductible.
4. L'idéal (a) est maximal.
5. L'anneau quotient $A/(a)$ est un corps.

On remarque que les implications suivantes

$$1. \Leftrightarrow 2. \Rightarrow 3. \Leftarrow 4. \Leftrightarrow 5.$$

sont valables dans n'importe quel anneau intègre.

L'implication $3. \Rightarrow 2.$ est appelée le **Lemme d'Euclide** : dans un anneau principal, si a divise bc et a est irréductible, alors a divise b ou c .

La proposition 1.37, appliquée aux anneaux principaux \mathbb{Z} et $\mathbb{K}[X]$, donne le résultat suivant.

Proposition 1.38 1. *Considérons l'idéal $(n) \subset \mathbb{Z}$ associé à $n \geq 2$. Alors (n) maximal $\Leftrightarrow (n)$ premier $\Leftrightarrow n$ est un nombre premier.*
 2. *Considérons l'idéal $(P) \subset \mathbb{K}[X]$ associé à un polynôme non constant P . Alors (P) maximal $\Leftrightarrow (P)$ premier $\Leftrightarrow P$ est un polynôme irréductible.*

Exemple 1.39 À la section 1.3, on a considéré l'anneau quotient $\mathbb{K} := \mathbb{Z}/3\mathbb{Z}[X]/(X^2 + 1)$. Le polynôme $X^2 + 1$ est irréductible dans $\mathbb{Z}/3\mathbb{Z}[X]$ car il ne possède pas de racine dans $\mathbb{Z}/3\mathbb{Z}$. Comme l'anneau $\mathbb{Z}/3\mathbb{Z}[X]$ est principal, on peut conclure que \mathbb{K} est un corps.

Dans un anneau principal, on peut définir la définition de "pgcd" et "ppcm" comme suit.

Définition 1.40 Soient A un anneau principal et $a, b \in A - \{0\}$.

1. $\text{pgcd}(a, b)$ est défini (modulo A^\times) par la relation $(a) + (b) = (\text{pgcd}(a, b))$.
2. $\text{ppcm}(a, b)$ est défini (modulo A^\times) par la relation $(a) \cap (b) = (\text{ppcm}(a, b))$.

Dans un anneau principal, les assertions suivantes sont équivalentes :

- a et b sont sans facteur commun,
- $(a) + (b) = A$,
- $\exists x, y \in A, ax + by = 1$.

C'est le **théorème de Bezout**. Ce résultat permet d'obtenir une généralisation du lemme d'Euclide qui est le **lemme de Gauss** : soient $a, b, c \in A$ non-nuls tel que a divise bc . Si a et b sont sans facteur commun alors a divise c .

On considère maintenant une partie $\text{Irr}(A) \subset A$ formée d'éléments irréductibles et satisfaisant la condition suivante : pour tout irréductible $p' \in A$, il existe un unique $(u, p) \in A^\times \times \text{Irr}(A)$ tel que $p' = up$.

À tout $p \in \text{Irr}(A)$, on associe la fonction valuation $v_p : A - \{0\} \rightarrow \mathbb{N}$ grâce à la relation

$$v_p(x) = \sup\{k \in \mathbb{N}, p^k \mid x\}.$$

Le fait que $v_p(x)$ soit finie est assurée au moyen du résultat suivant.

Lemme 1.41 Soit A anneau principal.

1. Toute suite croissante d'idéaux de A est stationnaire.
2. Considérons une suite (x_k) d'éléments non-nuls de A tel que $\forall k \in \mathbb{N}$, $x_{k+1} \mid x_k$. Alors, $\exists N \in \mathbb{N}$, tel que $\forall k, \ell \geq N$, x_k et x_ℓ sont associés.

On voit sans trop de difficultés que les énoncés 1. et 2. sont équivalents. Pour vérifier le point 1., on procède ainsi. Si $I_k \subset I_{k+1}, k \in \mathbb{N}$ est une suite croissante d'idéaux, on vérifie que $J = \bigcup_{k \in \mathbb{N}} I_k$ est un idéal. Comme A est principal, il existe $a \in \bigcup_{k \in \mathbb{N}} I_k$ tel que $J = (a)$. Soit $N \in \mathbb{N}$ tel que $a \in I_N$: comme $(a) \subset I_N \subset J = (a)$, on obtient $I_N = J$. Cela implique que $\forall k \geq N, I_k = I_{k+1}$. \square

On peut maintenant énoncer le théorème de décomposition.

Théorème 1.42 Soit A un anneau principal. Pour tout $x \in A - \{0\}$ il existe un unique $u \in A^\times$ tel que

$$x = u \prod_{p \in \text{Irr}(A)_x} p^{v_p(x)}$$

où $\text{Irr}(A)_x = \{p \in \text{Irr}(A), v_p(x) \neq 0\}$ est fini.

Corollaire 1.43 Pour tout $x, y \in A - \{0\}$, on a

$$\text{pgcd}(x, y) = \prod_{p \in \text{Irr}(A)} p^{\min(v_p(x), v_p(y))} \quad \text{et} \quad \text{ppcm}(x, y) = \prod_{p \in \text{Irr}(A)} p^{\max(v_p(x), v_p(y))}$$

Dans cette notation, on utilise la convention $p^0 = 1$ pour tout $p \in \text{Irr}(A)$.

On remarque en particulier que pour $a, b \in A - \{0\}$, a divise b si et seulement si $v_p(a) \leq v_p(b)$, pour tout $p \in \text{Irr}(A)$.

1.8 Anneaux factoriels

Partant d'un anneau A principal, l'anneau de polynômes $A[X]$ n'est pas nécessairement principal. Par exemple, dans $\mathbb{Z}[X]$, l'idéal $(2) + (X)$ n'est pas principal. Le but de cette section est d'introduire une notion plus faible qui sera "stable" pour l'opération $A \rightsquigarrow A[X]$.

Définition 1.44 A est un anneau factoriel si

- A est intègre.
- $\forall a \in A - \{0\}$, $\exists p_1, \dots, p_N$ irréductibles tels que

$$a = p_1 \cdots p_n.$$

— Cette décomposition est unique au sens suivant. Si

$$a = p_1 \cdots p_n = p'_1 \cdots p'_m$$

alors $m = n$ et il existe une permutation $\tau \in \mathcal{S}_n$ telle que $\forall k, (p_k) = (p'_{\sigma(k)})$.

Grâce au théorème 1.42 nous avons le résultat suivant.

Théorème 1.45 *Tout anneau principal est factoriel.*

Ainsi, nous savons que l'anneau $\mathbb{Z}[i]$ est factoriel, car il est principal. Par contre, on peut facilement montrer que l'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel : il suffit d'examiner la relation $4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ dans $\mathbb{Z}[i\sqrt{3}]$. Comme les trois éléments $2, 1 + i\sqrt{3}, 1 - i\sqrt{3}$ sont irréductibles dans $\mathbb{Z}[i\sqrt{3}]$ (*pourquoi ?*), on a deux décompositions distinctes de 4 comme produit d'irréductibles : cela contredit la condition d'unicité d'une décomposition en produit d'irréductibles pour les anneaux factoriels.

Remarque 1.46 *Dans un anneau factoriel, on peut encore définir les "pgcd" et les "ppcm" au moyen des formules du lemme 1.43.*

Le résultat principal de la section est le suivant.

Théorème 1.47 *Si A est factoriel, alors l'anneau de polynômes $A[X]$ est factoriel.*

Voici les grandes étapes de la preuve.

Pour tout polynôme non-nul $P = \sum_{k=1}^n a_k X^k \in A[X]$, on définit son contenu

$$c(P) = \text{pgcd}(a_0, \dots, a_n).$$

On dira que $P \in A[X]$ est primitif, si $c(P) = 1$.

Lemme 1.48 *À tout $p \in A$ irréductible, on associe le morphisme canonique $\varphi_p : A[X] \rightarrow A/(p)[X]$. Alors $P \in A[X]$ est primitif si $\varphi_p(P) \neq 0$ pour tout p irréductible.*

Le lemme précédent permet de montrer facilement le résultat suivant.

Lemme 1.49 $\forall P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.

On considère maintenant le corps de fraction \mathbb{K} de A .

Proposition 1.50 *Les polynômes irréductibles de $A[X]$ sont*

— *Les éléments irréductibles de A (i.e. les polynômes de degré 0).*

— Les polynômes primitifs et de degré ≥ 1 dans $A[X]$ qui sont irréductibles dans $\mathbb{K}[X]$.

On termine la preuve du théorème 1.47 de la manière suivante.

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

1. On considère la décomposition $P = c(P)\tilde{P}$ avec $\tilde{P} \in A[X]$ primitif.
2. Dans l'anneau principal $\mathbb{K}[X]$, on a la décomposition en irréductibles

$$\tilde{P} = \alpha \pi_1 \cdots \pi_n$$

où $\alpha \in \mathbb{K} - \{0\}$ et chaque π_k est un polynôme primitif de $A[X]$ qui est irréductible dans $\mathbb{K}[X]$.

3. En utilisant le lemme 1.49, on montre que $\alpha \in A^\times$.
4. En décomposant $c(P) = u p_1 \cdots p_m$ dans l'anneau factoriel A , on obtient dans $A[X]$ la décomposition de P en irréductibles

$$P = u \alpha p_1 \cdots p_m \pi_1 \cdots \pi_n.$$

On vérifie facilement que cette décomposition est unique. \square

Le théorème 1.47 nous permet de produire beaucoup d'exemples d'anneaux factoriel qui ne sont pas principaux :

- $\mathbb{Z}[X]$,
- $\mathbb{Z}[X_1, \dots, X_n]$,
- $\mathbb{K}[X_1, \dots, X_n]$, si $n \geq 2$ et \mathbb{K} un corps.

Certaines propriétés des anneaux principaux sont encore valables dans les anneaux factoriels.

Proposition 1.51 *Supposons A factoriel et soient $a, b, c \in A - \{0\}$.*

(Lemme d'Euclide) *a est irréductible et $a \setminus bc \implies a \setminus b$ ou $a \setminus c$.*

(Lemme de Gauss) *Si $a \setminus bc$ et a, b sont sans facteur commun, alors $a \setminus c$.*

On remarque que le Lemme de Gauss est équivalent à l'énoncé suivant : si a, b sont sans facteur commun et divisent c , alors $ab \setminus c$.

Terminons cette section avec des considérations élémentaires sur les polynômes irréductibles de $A[X]$ de petit degré (voir Proposition 1.50). Dans ce qui suit, a, b, c, \dots désignent des éléments d'un anneau **factoriel** A .

Exercice 1.52 — *a est irréductible dans $A[X]$ si et seulement si a est irréductible dans A .*

— *$a + bX$ est irréductible dans $A[X]$ si et seulement si a et b sont sans facteurs communs.*

- $P(X) = a + bX + cX^2$ est irréductible dans $A[X]$ si et seulement si a , b et c sont sans facteurs communs et si, de plus, $P(X)$ n'admet pas de racines dans la corps de fractions de A .
- $P(X) = a + bX + cX^2 + dX^3$ est irréductible dans $A[X]$ si et seulement si a , b , c et d sont sans facteurs communs et si, de plus, $P(X)$ n'admet pas de racines dans la corps de fractions de A .

Notons que tout se complique pour les polynômes de degré supérieur à 4. Par exemple, $P(X) = (X^2 - 2)(X^2 + 1) = X^4 - X^2 - 2$ n'est pas irréductible dans $\mathbb{Z}[X]$ alors qu'il n'admet aucune racine rationnelle.

2 Modules sur un anneau

La notion de module est la généralisation naturelle de celle d'espace vectoriel.

2.1 Premières définitions

Dans toute la suite, A désigne un anneau commutatif.

2.1.1 Modules et sous-modules

Définition 2.1 *Un A -module M est un groupe abélien munie d'une multiplication externe $A \times M \rightarrow M$, $(a, m) \mapsto a \cdot m$ vérifiant : $\forall a, b \in A$, $\forall m, n \in M$*

$$a) \ a \cdot (m + n) = a \cdot m + a \cdot n,$$

$$b) \ (a + b) \cdot m = a \cdot m + b \cdot m,$$

$$c) \ a \cdot (b \cdot m) = ab \cdot m,$$

$$d) \ 1 \cdot m = m.$$

On remarque que $\forall m \in M$, on a $0 \cdot m = 0$ et $(-1) \cdot m = -m$.

À un groupe abélien $(M, +)$, on associe l'anneau (à priori, non-commutatif)

$$\text{End}(M) := \{f : M \rightarrow M \text{ morphisme de groupe}\}.$$

Une structure de A -module sur M correspond à la donnée d'un morphisme d'anneaux $\rho : A \rightarrow \text{End}(M)$: on aura $\rho(a)(m) = a \cdot m$.

Exemple 2.2 • Si $A = \mathbb{K}$ est un corps, la structure de \mathbb{K} -module correspond à celle de \mathbb{K} -espace vectoriel.

- Si $A = \mathbb{Z}$, la structure de \mathbb{Z} -module correspond à celle de groupe abélien.

Exemple 2.3 *Voici quelques exemples de A -modules :*

- A ,

- A^n ,
- un idéal $I \subset A$.

On peut aussi associer à un ensemble \mathcal{X} (non-vidé), les A -modules suivants :

- $A^{\mathcal{X}} = \{\lambda : \mathcal{X} \rightarrow A\}$,
- $A^{(\mathcal{X})} = \{\lambda : \mathcal{X} \rightarrow A, \text{ tel que } \{x, \lambda(x) \neq 0\} \text{ est fini}\}$

Exemple 2.4 Soit $\varphi : A \rightarrow B$ un morphisme d'anneau. La multiplication externe $a \cdot b := \varphi(a)b$ munit B d'une structure de A -module.

Par exemple, si I est un idéal de A , le morphisme canonique $A \rightarrow A/I$ permet de voir A/I comme un A -module.

Soit E un \mathbb{K} -espace vectoriel. Tout endomorphisme $u \in \text{End}_{\mathbb{K}}(E)$ munit E d'une structure de $\mathbb{K}[X]$ -module, le produit externe étant défini par la relation

$$P(X) \cdot x = P(u)x, \quad \forall P(X) \in \mathbb{K}[X], \forall x \in E. \quad (2)$$

Respectivement, si E est un $\mathbb{K}[X]$ -module, alors :

- E est un \mathbb{K} -espace vectoriel,
- $\exists u \in \text{End}_{\mathbb{K}}(E)$, tel que le produit externe est défini par la relation (2).

Définition 2.5 Si E est un \mathbb{K} -espace vectoriel, on note E_u le $\mathbb{K}[X]$ -module associé à $u \in \text{End}_{\mathbb{K}}(E)$.

Définition 2.6 Soit M un A -module. Une partie $N \subset M$ est un sous A -module si

- N est un sous groupe de $(M, +)$,
- $\forall a \in A, aN := \{a \cdot n, n \in N\}$ est contenu dans N .

Dans ce cas, N admet une structure de A -module, induite par celle de M .

Exemple 2.7 • Les sous A -module de A sont les idéaux de A .

- Si $A = \mathbb{Z}$, un sous \mathbb{Z} -module de M est juste un sous groupe de $(M, +)$.
- Soit E_u le $\mathbb{K}[X]$ -module associé à $u \in \text{End}_{\mathbb{K}}(E)$. Alors les sous $\mathbb{K}[X]$ -modules de E_u sont les sous espace vectoriels F de E tels que $u(F) \subset F$.

Considérons un A -module M . A chaque $m \in M$, on associe

$$\text{ann}_A(m) = \{a \in A, a \cdot m = 0\}$$

Lemme 2.8 Pour tout $m \in M$, $\text{ann}_A(m)$ est un idéal de A .

Introduisons maintenant la notion de torsion d'un module.

Définition 2.9 Soit M un A -module. On note M_{tor} , l'ensemble des $m \in M$ tels que $\text{ann}_A(m) \neq \{0\}$. Si l'anneau A est **intègre**, on vérifie facilement que M_{tor} est un sous A -module de M : on l'appelle la torsion de M .

M est dit sans torsion si $M_{\text{tor}} = \{0\}$.

- Exercice 2.10**
1. Soit G un groupe abélien, vu comme un \mathbb{Z} -module.
 - Montrer que si G est fini, alors $G_{\text{tor}} = G$.
 - Donner un exemple où G est sans torsion.
 2. Soit E_u le $\mathbb{K}[X]$ -module associé à $u \in \text{End}_{\mathbb{K}}(E)$. Montrer que si $\dim_{\mathbb{K}} E$ est finie, alors $(E_u)_{\text{tor}} = E_u$.
 3. On considère l'anneau $\mathbb{K}[X]$ comme un $\mathbb{K}[X]$ -module. Dans ce cas, montrer que $\mathbb{K}[X]$ est sans torsion.

Considérons maintenant le cas d'un A -module M et d'un sous A -module $N \subset M$.

Proposition 2.11 *Le groupe quotient M/N admet une structure canonique de A -module. Le produit externe est défini par la relation suivante dans M/N :*

$$a \cdot \bar{m} := \overline{a \cdot m}, \quad \forall a \in A, \forall m \in M.$$

2.1.2 Morphismes entre modules

Soient M et N deux A -modules. Une application $f : M \rightarrow N$ est un **morphisme** de A -modules si

- f est un morphisme de groupe abélien,
- $\forall a \in A, \forall m \in M$, on a $f(a \cdot m) = a \cdot f(m)$.

Définition 2.12 *On note $\text{hom}_A(M, N)$, l'ensemble des morphismes de A -modules $f : M \rightarrow N$. Lorsque $M = N$, on note $\text{End}_A(M) := \text{hom}_A(M, M)$.*

Lorsque $A = \mathbb{Z}$, $\text{hom}_{\mathbb{Z}}(M, N)$ désigne l'ensemble des morphismes de groupes $f : M \rightarrow N$.

Exercice 2.13 *On considère un $\mathbb{K}[X]$ -module E_u . Montrer que $f \in \text{End}_{\mathbb{K}[X]}(E)$ si et seulement si $f \in \text{End}_{\mathbb{K}}(E_u)$ et de plus $f \circ u = u \circ f$.*

- On remarque que pour tout $f \in \text{hom}_A(M, N)$:
- $\ker(f)$ est un sous A -module de M ,
 - $\text{Image}(f)$ est un sous A -module de N .

Exercice 2.14 *Rappelons que l'anneau A est commutatif.*

- Montrer que $\text{hom}_A(M, N)$ admet une structure canonique de A -module.
- Identifiez $\text{End}_A(M)$ à un sous-anneau de $\text{End}(M)$.

Considérons maintenant trois A -modules M , N et P . La composition $(f, g) \mapsto f \circ g$ définit une application

$$\text{hom}_A(M, N) \times \text{hom}_A(P, M) \longrightarrow \text{hom}_A(P, N).$$

Un morphisme $\varphi : M \rightarrow N$ est un **isomorphisme** de A -modules si l'une des deux conditions (équivalentes) suivantes est satisfaite :

- $\exists g \in \text{hom}_A(N, M)$ tel que $\varphi \circ g = Id_N$ et $g \circ \varphi = Id_M$.
- φ est bijective.

Exercice 2.15 Soient $a, b \geq 2$. Montrer que le \mathbb{Z} -module $\text{hom}_{\mathbb{Z}}(\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z})$ est isomorphe à $\mathbb{Z}/c\mathbb{Z}$ où $c = \text{pgcd}(a, b)$.

Exercice 2.16 Montrer que le A -module $\text{hom}_A(A^k, A^\ell)$ est isomorphe au A -module $M_{\ell, k}(A)$ formé des matrices de tailles $\ell \times k$ à coefficients dans A .

Exercice 2.17 Montrer que le A -module $A^{\mathbb{N}}$ est isomorphe à $A[[X]]$, tandis que $A^{(\mathbb{N})}$ est isomorphe à $A[X]$.

Considérons maintenant une matrice $X \in M_n(A)$. Celle-ci définit un morphisme $\tilde{X} : A^n \rightarrow A^n, v \mapsto Xv$. L'application $X \mapsto \tilde{X}$ définit un isomorphisme entre $M_n(A)$ et $\text{End}_A(A^n)$.

Lemme 2.18 $\forall X \in M_n(A)$ les énoncés suivants sont équivalents :

- $\exists Y \in M_n(A)$ tel que $XY = I_n$.
- $\exists Y \in M_n(A)$ tel que $YX = I_n$.
- $\tilde{X} : A^n \rightarrow A^n$ est une application bijective.
- $\det(X) \in A^\times$.

Exercice 2.19 Déterminer $a, b \in \mathbb{Z}$ de telle manière à ce que le morphisme $\varphi : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ définie par $\varphi(x, y) = (50x + ay, 21x + by)$ soit bijectif.

2.1.3 Factorisation

Soit $f : M \rightarrow N$ un morphisme de A -modules. On considère le A -module quotient $M/\ker(f)$. Notons $\pi : M \rightarrow M/\ker(f)$ la projection canonique : c'est un morphisme de A -modules.

Proposition 2.20 L'application $\bar{f} : M/\ker(f) \rightarrow N$, définie par les relations

$$\bar{f}(\bar{m}) = f(m), \quad \forall m \in M$$

est un morphisme injectif de A -modules. On a alors la factorisation

$$f = \bar{f} \circ \pi.$$

Considérons un A -module M et un idéal I de A .

Lemme 2.21 Supposons que $\forall m \in M, I \subset \text{ann}_A(m)$. Dans ce cas, M possède une structure de A/I -module : le produit externe $A/I \times M \rightarrow M$ est défini par la relation

$$\bar{a} \cdot m := a \cdot m, \quad \forall a \in A, \forall m \in M.$$

Considérons l'exemple du groupe abélien $(\mathbb{Z}/2\mathbb{Z})^n$. On voit que $\forall m \in (\mathbb{Z}/2\mathbb{Z})^n, 2\mathbb{Z} \subset \text{ann}_{\mathbb{Z}}(m)$. Ainsi la structure de \mathbb{Z} -module de $(\mathbb{Z}/2\mathbb{Z})^n$ induit une structure de $\mathbb{Z}/2\mathbb{Z}$ -module : cette dernière est en fait la structure de $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel sur $(\mathbb{Z}/2\mathbb{Z})^n$.

2.1.4 Opérations sur les modules et sous-modules

Nous allons définir quelques opérations élémentaires.

• **Intersection** : Si $N_s, s \in S$ est une famille de sous A -modules de M , alors $\bigcap_{s \in S} N_s$ est un sous A -module de M .

• **Réunion croissante** : Si $N_k, k \in \mathbb{N}$ est une famille croissante⁵ de sous A -modules de M , alors $\bigcup_{k \in \mathbb{N}} N_k$ est un sous A -module de M .

• **Sous A -module engendré** : Si $X \subset M$, on note $\langle X \rangle$ le plus petit sous A -module de M contenant X : il est formé de tous les éléments de la forme $\sum_{m \in X} \lambda_m \cdot m$, où les $\lambda_m \in A$ sont tous nuls à part un nombre fini. On appelle $\langle X \rangle$ le sous A -module engendré par X

• **Somme de sous A -modules** : Si $N_s, s \in S$ est une famille de sous A -modules de M , on note $\sum_{s \in S} N_s$, le sous A -module engendré par $\bigcup_{s \in S} N_s$: il est formé de toutes les sommes (finies) $\sum_{s \in S} m_s$ où les $m_s \in N_s$ sont tous nuls à part un nombre fini.

• **Produit cartésien** : Si M_1, \dots, M_p sont des A -modules, le produit cartésien $M_1 \times \dots \times M_p$ admet une structure canonique de A -module. On notera aussi

$$\bigoplus_{k=1}^p M_k$$

ce produit cartésien.

• **Produit par un idéal** : Si M est un A -module et que I est un idéal de A , on note IM le sous A -module de M formé des sommes (finies) $\sum_{\lambda \in I} \lambda m_\lambda$, où les $\lambda \in I$ sont tous nuls à part un nombre fini et $m_\lambda \in M, \forall \lambda \in I$.

Lorsque G est un groupe abélien, on peut considérer l'idéal $(n) \subset \mathbb{Z}$ et le sous-groupe $(n)G$ qui est égal à $nG := \{nx, x \in G\}$.

Exercice 2.22 Montrer que M/IM admet une structure de A/I -module.

Ainsi, lorsque G est un groupe abélien, pour tout nombre premier $p \geq 2$, le quotient G/pG admet une structure de $\mathbb{Z}/p\mathbb{Z}$ -espace vectoriel.

2.2 Modules de type fini, modules libres

Soit M un A -module et $S \subset M$ une partie non vide.

— $S \subset M$ est dite *génératrice* si $\langle S \rangle = M$.

— $S \subset M$ est dite *libre*, si pour toute application $\lambda : S \rightarrow A$ nulle presque partout, $\sum_{s \in S} \lambda(s) \cdot s = 0$ seulement si $\forall s \in S, \lambda(s) = 0$.

— $S \subset M$ est une *base*, si S est libre et génératrice.

5. $\forall k \in \mathbb{N}, N_k \subset N_{k+1}$

On peut reformuler les notions précédentes en considérant le morphisme de A -modules $\varphi_S : A^{(S)} \rightarrow M$ défini par la relation

$$\varphi_S(\lambda) := \sum_{s \in S} \lambda(s) \cdot s.$$

Alors

- S est génératrice $\iff \varphi_S$ est surjective.
- S est libre $\iff \varphi_S$ est injective.
- S est une base $\iff \varphi_S$ est bijective.

Définition 2.23 — *Un A -module est libre s'il admet une base.*

- *Un A -module est de type fini s'il admet une partie génératrice finie.*

Voici le résultat principal de cette section.

Théorème 2.24 *Soit M un A -module non-nul que l'on suppose libre et de type fini. Alors il admet une base finie. De plus toutes les bases de M ont le même cardinal, qu'on appelle le rang de M , et que l'on note $\text{rang}(M) \geq 1$.*

Remarque 2.25 *Si M est le A -module nul, son rang est fixé égal à 0.*

Le théorème 2.24 nous permet de voir qu'un A -module (non-nul) M est libre et de type fini si et seulement si il est isomorphe à un certain A^ℓ avec $\ell = \text{rang}(M)$.

Exemple 2.26 — *Pour tout $\ell \geq 1$, A^ℓ est un A -module libre.*

- *$A[X]$ est un A -module libre mais il n'est pas de type fini.*
- *$\mathbb{Z}/n\mathbb{Z}$, pour $n \geq 2$ est un \mathbb{Z} -module de type fini, mais il n'est pas libre.*

Remarque 2.27 *Si M est un A -module libre et A est intègre, alors $M_{\text{tor}} = \{0\}$.*

Lorsque l'on travaille avec un \mathbb{K} -espace vectoriel E , on a les deux propriétés suivantes :

1. Une base de E est une famille libre maximale.
2. Une base de E est une famille génératrice minimale.

Notons que ces deux énoncés ne sont plus valables lorsque l'on travaille avec des A -modules. Voici deux exemples élémentaires obtenus avec le \mathbb{Z} -module \mathbb{Z} :

1. $\{2\}$ est une famille libre maximale de \mathbb{Z} , mais ce n'est pas une base.
2. $\{3, 5\}$ est une famille génératrice minimale de \mathbb{Z} , mais ce n'est pas une base.

2.3 Modules de type fini sur un anneau principal

Dans tout ce paragraphe, A désigne un anneau **principal**.

Nous commençons par étudier tout d'abord les sous A -modules d'un A -module libre de rang fini.

2.3.1 Sous-modules d'un module libre de rang fini

Nous avons un premier résultat important.

Théorème 2.28 *Soit A un anneau principal. Alors tout sous-module N de A^ℓ est libre et de rang fini $k \leq \ell$.*

La preuve se fait par récurrence sur $\ell \geq 1$.

Traisons le cas $\ell = 1$. Un sous-module N de A est un idéal de A . Comme A est principal, il existe $a \in A$ tel que $N = (a)$. Si $a = 0$, alors $N = 0$ est $\text{rang}(M) = 0$. Si $a \neq 0$, l'application $x \in A \mapsto xa \in N$ est un isomorphisme de A -modules. Cela montre que N est libre de rang 1.

Supposons le résultat vrai au rang ℓ , et considérons un sous module N de $A^{\ell+1}$. Notons $\pi : A^{\ell+1} \rightarrow A$ la projection sur la dernière coordonnée : $\pi(x_1, \dots, x_{\ell+1}) = x_{\ell+1}$. L'image $\pi(N)$ est un idéal de A et $\ker(\pi)$ s'identifie avec le sous-module $A^\ell \subset A^{\ell+1}$. L'intersection $N_1 = N \cap \ker(\pi)$ est un sous-module de A^n . Nous avons deux cas

- Si $\pi(N) = 0$, alors $N \subset A^n$ et l'hypothèse de récurrence nous permet de conclure que N est libre et de rang fini $k \leq \ell$.
- Si $\pi(N) \neq 0$, il existe $n_o \in M$ non-nul tel que $\pi(M) = (\pi(n_o))$. Alors

$$M = An_o \oplus N_1. \quad (3)$$

L'hypothèse de récurrence, appliquée à $N_1 \subset A^\ell$, nous permet de dire que N_1 est libre de rang inférieur à ℓ . On voit alors, grâce à (3), que N est libre de rang inférieur à $\ell + 1$.

□

Corollaire 2.29 *Soit A un anneau principal et M un A -module libre de rang ℓ . Alors tout sous-module de M est libre et de rang fini $k \leq \ell$.*

Le reste de cette section est consacrée à la preuve du Théorème 2.31. Considérons un A -module M libre de rang $\ell \geq 1$. Fixons une base (e_1, \dots, e_ℓ) de M . Notons $e_k^* \in \text{hom}_A(M, A)$ les morphismes “coordonnées” :

$$m = \sum_{k=1}^{\ell} e_k^*(m) \cdot e_k, \quad \forall m \in M.$$

On vérifie que (e_1^*, \dots, e_ℓ^*) est alors une base du A -module $\text{hom}_A(M, A)$.

Soit N un sous A -module de M . On remarque que pour tout $\varphi \in \text{hom}_A(M, A)$, l'image $\varphi(N)$ est un idéal de A . Considérons l'ensemble

$$\mathcal{E}_N := \{\varphi(N), \varphi \in \text{hom}_A(M, A)\}$$

ordonné au moyen l'inclusion. Le point clé est le résultat suivant.

Proposition 2.30 *Soit $d_1 \in A$ tel que $(d_1) = e_1^*(N) + \dots + e_\ell^*(N)$. Alors (d_1) est le plus grand élément de (\mathcal{E}_N, \subset) . De plus, pour tout $n \in N$, il existe $m \in M$ tel que $n = d_1 m$.*

La preuve nécessite plusieurs étapes.

Étape 1. Supposons qu'un idéal $I \subset A$ soit le plus grand élément de \mathcal{E}_N . Soit $\varphi \in \text{hom}_A(M, A)$ tel que $I = \varphi(N)$. Il existe $a_1, \dots, a_\ell, d \in A$ tels que $I = (d)$ et $\varphi = \sum_{k=1}^{\ell} a_k \cdot e_k^*$. Considérons $n \in N$ tel que

$$d = \varphi(n) = \sum_{k=1}^{\ell} a_k e_k^*(n).$$

Cela montre que $(d_1) \subset e_1^*(N) + \dots + e_\ell^*(N)$. Comme (d) est le plus grand élément de \mathcal{E}_N , on a aussi $e_k^*(N) \subset (d)$, $\forall k$. On obtient finalement que $(d) = e_1^*(N) + \dots + e_\ell^*(N)$. \square

Étape 2. Tout d'abord, comme A anneau principal, on sait que toute suite croissante d'idéaux de A est stationnaire (voir le Lemme 1.41). Cela implique qu'il existe $\varphi_1 \in \text{hom}_A(M, A)$ tel que $\varphi_1(N)$ est un élément maximal de (\mathcal{E}_N, \subset) . Soient $n_1 \in N$ et $d_1 \in A$ tel que $\varphi_1(n_1) = d_1$ et $\varphi_1(N) = (d_1)$. Le reste de la preuve consiste à montrer que (d_1) est le plus grand élément de (\mathcal{E}_N, \subset) . \square

Étape 3. Vérifions que $n_1 \in d_1 M$. Pour cela, il faut montrer que d_1 divise $e_k^*(n_1)$ pour tout $1 \leq k \leq \ell$. Fixons k , et considérons l'idéal

$$(\alpha_k) := (d_1) + (e_k^*(n_1))$$

La relation de Bezout nous assure l'existence de $a, b \in A$ tel que $\alpha_k = a\varphi_1(n_1) + be_k^*(n_1)$. Cela signifie que pour $\varphi = ae_k^* + b\varphi_1$, on a $\alpha_k \in \varphi(N)$ et donc $\varphi_1(N) = (d_1) \subset (\alpha_k) \subset \varphi(N)$. La maximalité de $\varphi_1(N)$ impose que $\varphi_1(N) = \varphi(N)$ et donc $(d_1) = (\alpha_k)$. Ceci signifie que $(e_k^*(n_1)) \subset (d_1)$. \square

Étape 4. A ce stade on sait que $n_1 = d_1 m_1$ avec $m_1 \in M$ vérifiant $\varphi_1(m_1) = 1$. Cela nous donne les sommes directes

$$M = Am_1 \oplus M' \quad \text{et} \quad N = Ad_1 m_1 \oplus N'$$

avec $M' = M \cap \ker(\varphi_1)$ et $N' = N \cap \ker(\varphi_1)$.

À tout $\varphi \in \text{hom}_A(M, A)$, on associe $\tilde{\varphi} \in \text{hom}_A(M, A)$ défini par les relations : $\tilde{\varphi}(m_1) = 1$ et $\tilde{\varphi} = \varphi$ sur M' . On voit alors que

$$\varphi_1(N) = (d_1) \subset (d_1) + \varphi(N') = \tilde{\varphi}(N).$$

Comme $\varphi_1(N)$ est maximal, on a $\varphi_1(N) = \tilde{\varphi}(N)$ et donc $\varphi(N') \subset (d_1)$. Finalement,

$$\varphi(N) = (d_1\varphi(m_1)) + \varphi(N') \subset (d_1) = \varphi_1(N).$$

On a bien démontré que $(d_1) = \varphi_1(N)$ contient tous les éléments de $\mathcal{E}_N := \{\varphi(N), \varphi \in \text{hom}_A(M, A)\}$. \square

Nous pouvons maintenant démontrer le théorème de structure suivant.

Théorème 2.31 (Théorème de la base adaptée) *Soit M un A -module libre de rang $\ell \geq 1$. Soit N un sous A -module de M de rang $1 \leq k \leq \ell$. Il existe une base (m_1, \dots, m_ℓ) de M et des coefficients non-nuls $d_1, \dots, d_k \in A$ tels que*

- $d_1 \setminus \dots \setminus d_k$,
 - $(d_1 m_1, \dots, d_k m_k)$ est une base de N .
- De plus, la suite d'idéaux $(d_1) \supset \dots \supset (d_k)$ est unique.

On reprend la preuve par récurrence du Théorème 2.28.

Revenons à l'étape 4 de la preuve de la proposition 2.30. Il existe $d_1 \in A$, $m_1 \in M$, $\varphi_1 \in \text{hom}_A(M, A)$ tels que

- $\varphi_1(m_1) = 1$,
- $d_1 m_1 \in N$,
- $(d_1) = \varphi_1(N)$ contient tous les éléments de $\mathcal{E}_N := \{\varphi(N), \varphi \in \text{hom}_A(M, A)\}$.

Comme N est non-nul, $d_1 \neq 0$. Nous avons alors des sommes directes

$$M = Am_1 \oplus M' \quad \text{et} \quad N = Ad_1 m_1 \oplus N'$$

où $M' := M \cap \ker(\varphi_1)$ est un module libre de rang $\ell - 1$ et $N' := N \cap \ker(\varphi_1)$ est un sous-module de M' de rang $k - 1$.

Si on applique l'hypothèse de récurrence à $N' \subset M'$, on obtient l'existence d'une base (m_2, \dots, m_ℓ) de M' et des coefficients non-nuls $d_2, \dots, d_k \in A$ tels que

- $d_2 \setminus \dots \setminus d_k$,
- $(d_2 m_2, \dots, d_k m_k)$ est une base de N' .

On remarque maintenant que $\mathcal{E}_{N'} := \{\psi(N'), \psi \in \text{hom}_A(M', A)\}$ est contenu dans $\mathcal{E}_N := \{\varphi(N), \varphi \in \text{hom}_A(M, A)\}$. Comme (d_1) et (d_2) sont respectivement les plus grands éléments de \mathcal{E}_N et de $\mathcal{E}_{N'}$, on obtient $(d_2) \subset (d_1)$, c'est à dire $d_1 \setminus d_2$. De plus, on peut conclure que

- (m_1, m_2, \dots, m_k) est une base de M .
- $(d_1 m_1, d_2 m_2, \dots, d_k m_k)$ est une base de N .

La question de l'unicité est reportée au prochain chapitre. \square

2.3.2 Modules de type fini : théorème de structure

Théorème 2.32 Soit M un A -module de type fini sur un anneau principal A . Alors il existe des éléments non-nuls n_1, \dots, n_q dans M tels que

$$M = \bigoplus_{k=1}^q An_k,$$

et vérifiant $\text{ann}_A(n_1) \supset \text{ann}_A(n_2) \supset \dots \supset \text{ann}_A(n_q)$.

De plus, la suite d'idéaux $\text{ann}_A(n_k)$ est unique.

Posons $q = t + s$ avec $t = \text{cardinal}\{j, \text{ann}_A(n_j) = 0\}$. Alors

$$M_{\text{tor}} = \bigoplus_{k=1}^s An_k \quad \text{et} \quad M/M_{\text{tor}} \simeq A^t.$$

Nous pouvons donner un autre formulation du théorème 2.32.

Théorème 2.33 Soit M un A -module de type fini sur un anneau principal A . Alors il existe d_1, \dots, d_s dans A , non nuls et non inversibles, tels que

$$M \simeq A^t \oplus A/d_1A \oplus \dots \oplus A/d_sA,$$

avec $t \in \mathbb{N}$ et $d_1 \setminus \dots \setminus d_s$.

De plus, l'entier $t \in \mathbb{N}$ et la suite d'idéaux $(d_1) \supset \dots \supset (d_s)$ est unique.

Preuve : Considérons un ensemble $\{m_1, \dots, m_\ell\}$ qui engendre M : le morphisme $f : A^\ell \rightarrow M$, $f(\lambda) = \sum_{i=1}^{\ell} \lambda_i \cdot m_i$ est surjectif. Posons $N := \ker(f)$. Alors f induit un isomorphisme entre A^ℓ/N et $M : \lambda + N \mapsto f(\lambda)$.

Appliquons le Théorème de la base adaptée aux modules $N \subset A^\ell$: il existe une base (v_1, \dots, v_ℓ) de A^ℓ et des coefficients non-nuls $d'_1, \dots, d'_r \in A$, avec $r \leq \ell$, tels que

- $d'_1 \setminus \dots \setminus d'_r$,
- $(d'_1 v_1, \dots, d'_r v_r)$ est une base de N .

Cela entraîne que l'application $\phi : A/d'_1A \times \dots \times A/d'_rA \times A^{\ell-r} \longrightarrow A^\ell/N$ définie par

$$\phi(\bar{x}_1, \dots, \bar{x}_r, x_{r+1}, \dots, x_\ell) = \sum_{i=1}^{\ell} x_i v_i + N$$

est un isomorphisme de A -modules.

Posons $r - s = \text{cardinal}\{i, (d'_i) = A\} \leq r$. Cela signifie que la suite d'idéaux $(d'_1) \supset \dots \supset (d'_r)$ est égale à

$$\underbrace{A \supset \dots \supset A}_{r-s \text{ fois}} \supset (d_1) \supset \dots \supset (d_s),$$

où les d_i sont non-nuls et non-inversibles. On remarque finalement que l'anneau $A/d'_1A \times \cdots \times A/d'_rA \times A^{\ell-r}$ est isomorphe à $A^t \oplus A/d_1A \oplus \cdots \oplus A/d_sA$ avec $t = \ell - r$. \square

L'isomorphisme $M \simeq A^t \oplus A/d_1A \oplus \cdots \oplus A/d_sA$ implique

$$M_{tor} \simeq A/d_1A \oplus \cdots \oplus A/d_sA,$$

et que M/M_{tor} est isomorphe à A^t . On a ainsi montré que le A -module M/M_{tor} est libre : l'entier t correspond à son rang.

Corollaire 2.34 *Soit M un module de type fini sur A principal. Alors M est libre si et seulement s'il est sans torsion.*

2.3.3 Unicité

Pour montrer l'unicité de la suite des idéaux $(d_1) \supset \cdots \supset (d_s)$, on procède de la manière suivante.

À tout élément irréductible $p \in A$, on associe le sous A -module, appelé « la composante p -primaire de M »,

$$M_p = \{m \in M, \exists k \geq 1, p^k \cdot m = 0\},$$

et la suite décroissante de sous-modules

$$M_p \supset p(M_p) \supset p^2(M_p) \supset \cdots \supset p^k(M_p) \supset \cdots$$

Comme M est de rang fini, on vérifie que

1. $M_p \neq 0$ si et seulement si p est associé à une famille finie \mathcal{P} d'éléments irréductibles.
2. $M_{tor} = \bigoplus_{p \in \mathcal{P}} M_p$.
3. $\forall p \in \mathcal{P}, \exists k \geq 1, p^k(M_p) = 0$.
4. $M_p \simeq M_{tor}/p^k(M_{tor})$ pour k assez grand.

Les quotients $p^k(M_p)/p^{k+1}(M_p)$ admettent une structure de A/pA -espace vectoriel⁶. De plus, on remarque que l'application

$$\overline{m} \in p^k(M_p)/p^{k+1}(M_p) \longmapsto \overline{p \cdot m} \in p^{k+1}(M_p)/p^{k+2}(M_p)$$

est une application surjective.

Définition 2.35 *Soit M un module de type fini sur A principal. À tout élément irréductible $p \in A$, on associe la suite décroissante*

$$\lambda_p^\bullet(M) : \lambda_p^0(M) \geq \lambda_p^1(M) \geq \cdots \geq \lambda_p^k(M) \geq \cdots$$

formée par les dimensions des A/pA -espaces vectoriels $p^k(M_p)/p^{k+1}(M_p)$, $k \in \mathbb{N}$.

6. A/pA est un corps.

Remarque 2.36 Comme M est de type fini, la suite $\lambda_p^\bullet(M) = (\lambda_p^k(M))_{k \in \mathbb{N}}$ est nulle à partir d'un certain rang.

Proposition 2.37 Soit $d \in A$ non inversible et $p \in A$ irréductible. Soit $v_p(d) = \max\{k \in \mathbb{N}, p^k \mid d\}$.

- Si p ne divise pas d , i.e. $v_p(d) = 0$, alors $\lambda_p^k(A/dA) = 0, \forall k \in \mathbb{N}$.
- Si p divise d , i.e. $v_p(d) \geq 1$, alors
 - $\lambda_p^k(A/dA) = 1$ si $k \leq v_p(d) - 1$,
 - $\lambda_p^k(A/dA) = 0$ si $k \geq v_p(d)$.

Preuve : Si p ne divise pas d , alors $(A/dA)_p = 0$, et donc la suite $\lambda_p^\bullet(A/dA)$ est nulle.

Supposons que p divise d : alors $p = p^\alpha q$ avec $\alpha = v_p(d)$. Dans ce cas le sous-module $(A/dA)_p$ est égal à $q(A/dA)$, et ce dernier est isomorphe à $A/p^\alpha A$. On vérifie alors que $\lambda_p^k(A/p^\alpha A) = 1$ si $k \leq \alpha - 1$, et que $\lambda_p^k(A/p^\alpha A) = 0$ si $k \geq \alpha$. \square

Considérons un A -module M qui est isomorphe à

$$A^t \oplus A/d_1A \oplus \cdots \oplus A/d_sA, \quad (4)$$

avec $(d_1) \supset \cdots \supset (d_s)$.

Pour tout $p \in A$ irréductible, et tout entier $k \in \mathbb{N}$, on a

$$\lambda_p^k(M) = \sum_{j=1}^s \lambda_p^k(A/d_jA) = \text{Cardinal}\{j, k \leq v_p(d_j) - 1\}.$$

On remarque tout d'abord que la suite $\lambda_p^\bullet(M)$ est nulle si p ne divise pas d_s . Notons $\mathcal{P} = \{p_1, \dots, p_h\}$, l'ensemble⁷ des diviseurs irréductibles de d_s .

Alors pour tout $i = 1, \dots, s$, on a une décomposition en facteurs irréductibles :

$$d_i = u_i \prod_{p \in \mathcal{P}} p^{v_p(d_i)}.$$

Comme $d_1 \supset \cdots \supset d_s$, on a

$$0 \leq v_p(d_1) \leq v_p(d_2) \leq \cdots \leq v_p(d_s), \quad \forall p \in \mathcal{P}. \quad (5)$$

On sait que les idéaux $(d_1) \supset \cdots \supset (d_s)$ sont entièrement déterminés au moyen des suites de nombres entiers (5). Ainsi, pour montrer l'unicité de la suite d'idéaux $(d_1) \supset \cdots \supset (d_s)$ vérifiant (4), il suffit de montrer que les suites de nombres entiers (5) peuvent être exprimées au moyen des suites $\lambda_p^\bullet(M)$, $p \in \mathcal{P}$.

On complète cette preuve d'unicité en remarquant que :

1. $s = \sup\{\lambda_p^0(M), p \in \mathcal{P}\}$.
2. $\lambda_p^{k-1}(M) - \lambda_p^k(M) = \text{Cardinal}\{j, v_p(d_j) = k\}, \forall k \geq 1$.
3. $s - \lambda_p^0(M) = \text{Cardinal}\{j, v_p(d_j) = 0\}$.

7. Si p irréductible divise d_s , alors $\exists! p_i \in \mathcal{P}$ tel que p et p_i sont associés.

2.4 Quelques applications

2.4.1 Groupes abéliens de type fini

Dans le cas $A = \mathbb{Z}$, le théorème de structure 2.32 donne :

Théorème 2.38 *Soit M un groupe abélien de type fini (i.e. engendré par un nombre fini d'éléments). Alors M est isomorphe à*

$$\mathbb{Z}^t \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}$$

où $t \in \mathbb{N}$, et les d_i sont des entiers ≥ 2 vérifiant $d_1 \mid \cdots \mid d_s$.

De plus, $t \in \mathbb{N}$ et les d_i sont entièrement déterminés par M . On appellera facteurs invariants du groupe M la suite $d_1 \mid \cdots \mid d_s$.

Remarque 2.39 *On remarque que si un groupe abélien M est isomorphe à $\mathbb{Z}^t \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}$, alors*

$$M_{tor} \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z} \quad \text{et} \quad M/M_{tor} \simeq \mathbb{Z}^t.$$

En particulier, on a montré qu'un groupe abélien de type fini est libre si et seulement si il est sans torsion.

Voici un petit résultat qui découle immédiatement du théorème.

Exercice 2.40 • *Soit G un groupe abélien fini. Considérons le nombre entier*

$$e(G) = \inf\{k \geq 1; kx = 0, \forall x \in G\}.$$

Montrer qu'il existe un élément de G d'ordre $e(G)$.

• *Soit \mathbb{K} un corps et G un sous-groupe fini du groupe multiplicatif \mathbb{K}^\times . Montrer que G est un groupe cyclique (on utilisera le résultat du premier point).*

Exercice 2.41 *Calculer les facteurs invariants du groupe*

$$G = \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/432\mathbb{Z} \times \mathbb{Z}/1000\mathbb{Z}.$$

2.4.2 Réduction des matrices de $M_{p,q}(\mathbb{Z})$

Rappelons qu'une matrice carrée $M \in M_n(\mathbb{Z})$ admet un inverse dans $M_n(\mathbb{Z})$ si et seulement si $\det(M) = \pm 1$ (cela découle de la formule classique avec la comatrice de X).

On considère alors le groupe

$$GL_n(\mathbb{Z}) = \{M \in M_n(\mathbb{Z}), \det(M) = \pm 1\}.$$

On va considérer le \mathbb{Z} -module des matrices de taille $p \times q$ à coefficients entiers : $M_{p,q}(\mathbb{Z})$.

Définition 2.42 Deux matrices $M, M' \in M_{p,q}(\mathbb{Z})$ sont équivalentes si et seulement si il existe $(P, Q) \in GL_p(\mathbb{Z}) \times GL_q(\mathbb{Z})$ tel que

$$M' = PMQ.$$

Remarque 2.43 Lorsque l'on travaille avec un corps \mathbb{K} , pour toutes matrices $M, M' \in M_{p,q}(\mathbb{K})$, les assertions suivantes sont équivalentes :

- $\exists (P, Q) \in GL_p(\mathbb{K}) \times GL_q(\mathbb{K})$ tel que $M' = PMQ$,
- $\text{rang}(M) = \text{rang}(M')$.

À toute matrice $M \in M_{p,q}(\mathbb{Z})$, on associe les sous-modules

- $\text{Im}(M) = \{Xv, v \in \mathbb{Z}^q\} \subset \mathbb{Z}^p$,
- $\ker(M) \subset \mathbb{Z}^q$.

Le lemme suivant sera très utile par la suite.

Lemme 2.44 Supposons que $\text{rang}(M) = k \neq 0$. Il existe une famille de vecteurs $e_i \in \mathbb{Z}^q, i = 1, \dots, k$, telle que

$$(\clubsuit) \quad \mathbb{Z}^q = \ker(M) \oplus \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_k \quad \text{et} \quad (\spadesuit) \quad \text{Im}(M) = \mathbb{Z}f_1 \oplus \dots \oplus \mathbb{Z}f_k,$$

où $f_i = Me_i \in \mathbb{Z}^p, i = 1, \dots, k$.

Preuve : Comme $\text{Im}(M)$ est un sous \mathbb{Z} -module du module libre \mathbb{Z}^p , il possède une base f_1, \dots, f_k : la relation (\spadesuit) est satisfaite. Pour tout i , choisissons $e_i \in \mathbb{Z}^q$ tel que $f_i = Me_i$. Alors pour tout $v \in \mathbb{Z}^q$, il existe un unique k -uplet $(\lambda_1, \dots, \lambda_k) \in \mathbb{Z}^k$, tel que $Mv = \sum_{i=1}^k \lambda_i f_i = \sum_{i=1}^k \lambda_i Me_i$: cette dernière relation est équivalente à dire que $v - \sum_{i=1}^k \lambda_i e_i \in \ker(M)$. On a bien montré la relation (\clubsuit) . \square

Corollaire 2.45 Pour des matrices $M, M' \in M_{p,q}(\mathbb{Z})$ les relations suivantes sont équivalentes :

1. $\text{Im}(M) = \text{Im}(M')$.
2. Il existe $Q \in GL_q(\mathbb{Z})$ tel que $M = M'Q$.

Preuve : L'implication 2. \implies 1. est immédiate car pour tout $Q \in GL_q(\mathbb{Z})$, $\text{Im}(Q) = \mathbb{Z}^q$ et donc $\text{Im}(M'Q) = M'(\text{Im}(Q)) = \text{Im}(M')$.

Supposons maintenant que $\text{Im}(M) = \text{Im}(M')$ et considérons une base f_1, \dots, f_k de ce sous \mathbb{Z} -module. Soient $e_1, \dots, e_k \in \mathbb{Z}^q$ et $e'_1, \dots, e'_k \in \mathbb{Z}^q$ tels que $f_i = Me_i$ et $f_i = M'e'_i$. On a alors les relations

$$\mathbb{Z}^q = \ker(M) \oplus \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_k = \ker(M) \oplus \mathbb{Z}e'_1 \oplus \dots \oplus \mathbb{Z}e'_k.$$

Choisissons une base e_{k+1}, \dots, e_q de $\ker(M)$ et une base e'_{k+1}, \dots, e'_q de $\ker(M')$. On voit alors que $(e_i)_{1 \leq i \leq q}$ et $(e'_i)_{1 \leq i \leq q}$ sont deux bases de \mathbb{Z}^q . L'élément $Q \in GL_q(\mathbb{Z})$ défini par les relations $Qe_i = e'_i, \forall i$, vérifie $M = M'Q$. \square

Nous avons un autre lemme préparatoire.

Lemme 2.46 Soient E et F deux sous \mathbb{Z} -modules de \mathbb{Z}^p . Les relations suivantes sont équivalentes :

1. Il existe $P \in GL_p(\mathbb{Z})$ tel que $P(E) = F$.
2. les \mathbb{Z} -modules \mathbb{Z}^p/E et \mathbb{Z}^p/F sont isomorphes.

Preuve : Supposons qu'il existe $P \in GL_p(\mathbb{Z})$ tel que $P(E) = F$. Alors l'application $v + E \mapsto P(v) + F$ définit un isomorphisme entre \mathbb{Z}^p/E et \mathbb{Z}^p/F .

Supposons que \mathbb{Z}^p/E et \mathbb{Z}^p/F sont tous deux isomorphes à $\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}$ où les d_i sont des entiers ≥ 2 vérifiant $d_1 \setminus \cdots \setminus d_s$. Cela signifie qu'il existe deux bases $(f_i)_{1 \leq i \leq p}$ et $(f'_i)_{1 \leq i \leq p}$ de \mathbb{Z}^p telles que

$$E = \mathbb{Z}d_1f_1 \oplus \cdots \oplus \mathbb{Z}d_sf_s \quad \text{et} \quad F = \mathbb{Z}d_1f'_1 \oplus \cdots \oplus \mathbb{Z}d_sf'_s.$$

L'élément $P \in GL_p(\mathbb{Z})$ défini par les relations $Qf_i = e'_i, \forall i$, vérifie $P(E) = F$. \square

Notre résultat principal est le suivant.

Théorème 2.47 • Deux matrices $M, M' \in M_{p,q}(\mathbb{Z})$ sont équivalentes si et seulement si

$$\mathbb{Z}^p/\text{Im}(M) \simeq \mathbb{Z}^p/\text{Im}(M').$$

• $\mathbb{Z}^p/\text{Im}(M) \simeq \mathbb{Z}^{p-s} \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}$ si et seulement si $M \in M_{p,q}(\mathbb{Z})$ est équivalente avec la matrice

$$\Delta_d := \begin{pmatrix} \text{Diag}(d_1, \dots, d_s) & 0 \\ 0 & 0 \end{pmatrix} \quad (6)$$

où $\text{Diag}(d_1, \dots, d_s)$ est une matrice diagonale.

• Toute matrice $M \in M_{p,q}(\mathbb{Z})$ est équivalente à une matrice Δ_d où les d_i appartiennent à $\mathbb{N} - \{0\}$ et vérifient $d_1 \setminus \cdots \setminus d_s$. Ici "s" est égal au rang de la matrice X , vue comme élément de $M_{p,q}(\mathbb{Z})$, et les (d_i) sont uniques.

Preuve : Grace au Lemme 2.46, on sait $\mathbb{Z}^p/\text{Im}(M) \simeq \mathbb{Z}^p/\text{Im}(M')$ si et seulement si il existe $P \in GL_p(\mathbb{Z})$ tel que $\text{Im}(PM) = P(\text{Im}(M)) = \text{Im}(M')$. Le corollaire 2.45 permet de voir que $\text{Im}(PM) = \text{Im}(M')$ si et seulement si il existe $Q \in GL_q(\mathbb{Z})$ tel que $PMQ = M'$. Le premier point est démontré.

On voit immédiatement que l'image de la matrice Δ_d est $\mathbb{Z}d_1e_1 \oplus \cdots \oplus \mathbb{Z}d_se_s$ où (e_i) est la base canonique de \mathbb{Z}^p . Ainsi le quotient $\mathbb{Z}^p/\text{Im}(\Delta_d)$ est isomorphe à $\mathbb{Z}^{p-s} \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}$. Le premier point nous permet de voir que les assertions suivantes sont équivalentes :

- M est équivalente à une matrice Δ_d ,
- $\mathbb{Z}^p/\text{Im}(X) \simeq \mathbb{Z}^p/\text{Im}(X_d) \simeq \mathbb{Z}^{p-s} \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z}$.

Le dernier point est une conséquence de second point et du théorème 2.38. \square

Définition 2.48 Soit $M \in M_{p,q}(\mathbb{Z})$. À chaque $1 \leq k \leq \inf\{p, q\}$, on associe $m_M^k \in \mathbb{N}$, qui est le pgcd de tous les mineurs de taille k de la matrice M .

Exercice 2.49 Soit $M \in M_{p,q}(\mathbb{Z})$.

1. Montrer que $m_M^k = m_{PM}^k$ pour tout $P \in GL_p(\mathbb{Z})$.
2. Montrer que $m_M^k = m_{MQ}^k$ pour tout $Q \in GL_q(\mathbb{Z})$.
3. Si M est équivalente à une matrice Δ_d (voir (6)) avec $d_i \in \mathbb{N} - \{0\}$ et $d_1 \setminus \dots \setminus d_s$, alors
 - $m_M^k = d_1 \cdots d_k$ pour tout $k \leq s$,
 - $m_M^k = 0$ si $k > s$.

Tous les résultats de cette section sont encore valables si on travaille avec des matrices de $M_{p,q}(A)$ où A est anneau principal.

2.4.3 Réduction des endomorphismes d'un \mathbb{K} -espace vectoriel de dimension finie

Soit E un \mathbb{K} espace vectoriel de dimension finie : on notera $n \geq 1$ sa dimension. On note $GL_{\mathbb{K}}(E)$ le groupe des isomorphismes de E .

Définition 2.50 Deux endomorphismes $f, h \in \text{End}_{\mathbb{K}}(E)$ sont semblables si et seulement si il existe $g \in GL_{\mathbb{K}}(E)$ tel que

$$h = gfg^{-1}.$$

Les classes d'équivalences $\{gfg^{-1}, g \in GL_{\mathbb{K}}(E)\}$ sont appelées classes de similitudes.

On remarque que f, h sont semblables si et seulement si il existe des bases $\mathcal{B}_1, \mathcal{B}_2$ de E telles que les matrices $\text{Mat}(f, \mathcal{B}_1)$ et $\text{Mat}(h, \mathcal{B}_2)$ sont égales.

Le but de cette section est de caractériser les classes de similitude. Pour cela on va considérer les $\mathbb{K}[X]$ -modules E_f attachés à chaque endomorphisme $f \in \text{End}_{\mathbb{K}}(E)$ (voir la définition 2.5). On commence avec le résultat élémentaire suivant.

Lemme 2.51 Deux endomorphismes $f, h \in \text{End}_{\mathbb{K}}(E)$ sont semblables si et seulement les $\mathbb{K}[X]$ -modules E_f et E_h sont isomorphes.

Définition 2.52 Un endomorphisme $f \in \text{End}_{\mathbb{K}}(E)$ est dit cyclique s'il existe un vecteur $v \in E$, tel que la famille $\{f^k(v), k \in \mathbb{N}\}$ engendre E .

Notons que tout morphisme de $\mathbb{K}[X]$ -modules $\phi : \mathbb{K}[X] \rightarrow E_f$ est défini par la relation $\phi(P) = P(f)(v)$ où $v = \phi(1)$: dans ce cas, l'image de ϕ est égale au sous $\mathbb{K}[X]$ -module $\mathbb{K}[X]v$ et le noyau $\ker(\phi)$ est égal à $\text{ann}_{\mathbb{K}[X]}(v)$.

On voit donc qu'un endomorphisme $f \in \text{End}_{\mathbb{K}}(E)$ est cyclique si et seulement si il existe un morphisme de $\mathbb{K}[X]$ -modules surjectif

$$\phi_f : \mathbb{K}[X] \longrightarrow E_f.$$

Si $P_f = X^n - \sum_{k=0}^{n-1} a_k X^k$ est le polynôme unitaire qui engendre $\ker(\phi_f)$, le morphisme ϕ_f induit un isomorphisme $\mathbb{K}[X]/(P_f) \simeq E_f$ de $\mathbb{K}[X]$ -modules.

De plus, si \mathcal{B} est la base de E formée par la famille $\{v, f(v), \dots, f^{n-1}(v)\}$, on remarque que

$$\text{Mat}(f, \mathcal{B}) = \begin{pmatrix} 0 & \dots & \dots & \dots & a_0 \\ 1 & 0 & \dots & \dots & a_1 \\ 0 & 1 & 0 & \dots & a_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & 1 & a_n \end{pmatrix}.$$

Cette dernière matrice, notée $C(P_f)$, est la *matrice compagnon* associée à P_f . Remarquons que lorsque $n = 1$, la matrice $C(P_f)$ est égale à (a_0) .

Exercice 2.53 — Montrer que le polynôme caractéristique de la matrice $C(P_f)$ est égal à P_f .

— Montrer qu'un endomorphisme $f \in \text{End}_{\mathbb{K}}(E)$ est cyclique si et seulement si son polynôme caractéristique est égal à son polynôme minimal.

On peut maintenant énoncer le résultat principal de cette section.

Théorème 2.54 Pour tout endomorphisme $f \in \text{End}_{\mathbb{K}}(E)$, il existe une base de E dans laquelle la matrice de f est de la forme

$$\begin{pmatrix} C(P_1) & & & \\ & C(P_2) & & \\ & & \ddots & \\ & & & C(P_s) \end{pmatrix}.$$

où les (P_k) sont des polynômes unitaires de $\mathbb{K}[X]$ de degré au moins 1, vérifiant : $P_1 \setminus P_2 \setminus \dots \setminus P_s$.

Les polynômes (P_k) , qui sont entièrement déterminés par l'endomorphisme f , sont appelés les *invariants de similitude* de f .

Deux endomorphismes sont semblables si et seulement si ils ont les mêmes invariants de similitude.

Remarque 2.55 On remarque que le polynôme caractéristique de $f \in \text{End}_{\mathbb{K}}(E)$ est égal au produit $P_1 \cdots P_s$ tandis que son polynôme minimal est égal à P_s .

Preuve : Fixons $f \in \text{End}_{\mathbb{K}}(E)$ et appliquons le théorème 2.32 au $\mathbb{K}[X]$ -module E_f . Il existe des vecteurs non-nuls v_1, \dots, v_q tels que

$$E_f = \bigoplus_{k=1}^s \mathbb{K}[X] v_k,$$

et vérifiant $\text{ann}_{\mathbb{K}[X]}(v_1) \supset \dots \supset \text{ann}_{\mathbb{K}[X]}(v_s) \neq 0$. Désignons par P_k le polynôme unitaire qui engendre l'idéal $\text{ann}_{\mathbb{K}[X]}(v_k)$: on a bien $P_1 \setminus P_2 \setminus \dots \setminus P_s$.

On remarque alors que $\mathcal{B}_k := \{v_k, f(v_k), \dots, f^{d^{\circ} P_k - 1}(v_k)\}$ est une base du sous espace $E_k := \mathbb{K}[X] v_k$ tel que la matrice de l'endomorphisme $f|_{E_k}$ dans la base \mathcal{B}_k est égale à $C(P_k)$. La preuve du théorème est complète. \square

Le reste de cette section est consacrée à la détermination des invariants de similitude d'un endomorphisme $f \in \text{End}_{\mathbb{K}}(E)$. Soit $M = (a_{ij}) \in M_n(\mathbb{K})$ la matrice de f dans une base e_1, \dots, e_n .

On considère le morphisme de $\mathbb{K}[X]$ -modules $\phi : \mathbb{K}[X]^n \rightarrow E_f$ défini par la relation

$$\phi(P_1, \dots, P_n) = \sum_{k=1}^n P_k(f)(e_k).$$

Notons $\epsilon_i = (0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{K}[X]^n$ le vecteur tel que $\phi(\epsilon_j) = e_j$.

Posons $h_j = X\epsilon_j - \sum_{i=1}^n a_{ij}\epsilon_i$. On remarque que $\forall j, \phi(h_j) = 0$, ainsi $\sum_{j=1}^n \mathbb{K}[X]h_j \subset \ker(\phi)$.

Lemme 2.56 *On a les deux relations :*

1. $\mathbb{K}[X]^n = \sum_{j=1}^n \mathbb{K}[X]h_j + \sum_{j=1}^n \mathbb{K}\epsilon_j$.
2. $\ker(\phi) = \sum_{j=1}^n \mathbb{K}[X]h_j$.

La matrice $XI_n - M \in M_n(\mathbb{K}[X])$ détermine le morphisme de $\mathbb{K}[X]$ -modules $\psi : \mathbb{K}[X]^n \rightarrow \mathbb{K}[X]^n, V \mapsto (XI_n - M)V$. Le lemme précédent montre que

$$\ker(\phi) = \text{Image}(\psi),$$

et donc E_f est isomorphe au $\mathbb{K}[X]$ -module $\mathbb{K}[X]^n / \text{Image}(\psi)$.

Si on utilise les résultats de la section 2.4.2, on sait que la matrice

$$XI_n - M \in M_n(\mathbb{K}[X])$$

est équivalente à une matrice diagonale $\text{Diag}(Q_1(X), \dots, Q_n(X))$ où les polynômes $Q_i(X) \in \mathbb{K}[X]$, qui peuvent être choisis unitaires, sont non-nuls et vérifient $Q_1(X) \setminus \dots \setminus Q_n(X)$.

Alors le $\mathbb{K}[X]$ -module $\mathbb{K}[X]^n / \text{Image}(\psi)$ sera isomorphe à

$$\bigoplus_{k=1}^n \mathbb{K}[X] / (Q_k).$$

On voit donc que les invariants de similitudes de l'endomorphisme f sont les polynômes $\{Q_k, d^{\circ}(Q_k) \geq 1\}$.

Définition 2.57 Soit $M \in M_n(\mathbb{K})$. À chaque $1 \leq k \leq n$, on associe le polynôme unitaire $R_M^k \in \mathbb{K}[X]$, qui est le pgcd de tous les mineurs de taille k de la matrice $XI_n - M$.

On termine cette section en établissant le lien entre les invariants de similitudes $P_1 \setminus \cdots \setminus P_s$ d'un endomorphisme $f \in \text{End}_{\mathbb{K}}(E)$ et les polynômes unitaires $R_M^k \in \mathbb{K}[X]$ associés à la matrice $M = \text{Mat}(f, \mathcal{B})$. Sachant que la matrice $XI_n - M \in M_n(\mathbb{K}[X])$ est équivalente à la matrice diagonale $\text{Diag}(1, \dots, 1, P_1, \dots, P_s)$, on obtient les relations suivantes :

1. $s = n - \text{cardinal}\{k, R_M^k = 1\}$,
2. $R_M^{n-s+1} = P_1$,
3. Pour tout $1 \leq i \leq s$, on a $P_1 \cdots P_i = R_M^{n-s+i}$.

3 Produit tensoriel

Dans cette section A désigne un anneau commutatif. Soient M, N deux A -modules. On va montrer l'existence d'un A -module $M \otimes_A N$ et d'une application A -bilinéaire $\otimes : M \times N \rightarrow M \otimes_A N, (m, n) \mapsto m \otimes n$, telle que $M \otimes_A N$ est engendré par tous les éléments $m \otimes n$.

Rappelons que si \mathcal{X} est un ensemble et si P est un A -module, l'ensemble $\mathcal{F}(\mathcal{X}, P)$ formé de toutes les applications $f : \mathcal{X} \rightarrow P$, admet une structure naturelle de A -module.

3.1 Applications bilinéaires

Soient M, N, P trois A -modules.

Définition 3.1 Une application $\phi : M \times N \rightarrow P$ est dite A -bilinéaire si elle est A -linéaire en chacune des variables : $\forall m, m' \in M, \forall n, n' \in N, \forall a \in A$, nous avons

$$\begin{aligned}\phi(m + a \cdot m', n) &= \phi(m, n) + a \cdot \phi(m', n), \\ \phi(m, n + a \cdot n') &= \phi(m, n) + a \cdot \phi(m, n').\end{aligned}$$

On note $\text{bil}_A(M \times N, P)$ l'ensemble de ces applications.

On remarque que $\text{bil}_A(M \times N, P)$ est un sous A -module de $\mathcal{F}(M \times N, P)$.

À tout $\phi \in \text{bil}_A(M \times N, P)$, et tout $(m, n) \in M \times N$, on associe les morphismes de A -modules

$$\phi(m, -) : N \rightarrow P, \quad \text{et} \quad \phi(-, n) : M \rightarrow P$$

définis respectivement par les relations $y \in N \mapsto \phi(m, y)$ et $x \in M \mapsto \phi(x, n)$.

On vérifie aisément que les applications $m \in M \mapsto \phi(m, -) \in \text{hom}_A(N, P)$ et $n \in N \mapsto \phi(-, n) \in \text{hom}_A(M, P)$ sont des morphismes de A -modules. On a ainsi deux morphismes

$$\begin{aligned}\alpha : \text{bil}_A(M \times N, P) &\longrightarrow \text{hom}_A(M, \text{hom}_A(N, P)), \\ \beta : \text{bil}_A(M \times N, P) &\longrightarrow \text{hom}_A(N, \text{hom}_A(M, P)),\end{aligned}$$

définis par $\alpha(\phi) : m \mapsto \phi(m, -)$ et $\beta(\phi) : n \mapsto \phi(-, n)$.

Proposition 3.2 α et β définissent deux isomorphismes de A -modules.

3.2 Définition du produit tensoriel

Notons $\mathcal{F}_0(M \times N)$ le sous-module de $\mathcal{F}(M \times N, A)$ formé de toutes les applications $f : M \times N \rightarrow A$ de support fini, i.e. telle que $\{(m, n) \in M \times N, f(m, n) \neq 0\}$ est fini.

Notons $\delta_{(m,n)} \in \mathcal{F}_0(M \times N)$ la fonction nulle partout sauf en (m, n) , où elle est égale à $1 \in A$. La famille $\{\delta_{(m,n)}, (m, n) \in M \times N\}$ est une base du A -module $\mathcal{F}_0(M \times N)$:

$$f = \sum_{(m,n) \in M \times N} f(m, n) \delta_{(m,n)}, \quad \forall f \in \mathcal{F}_0(M \times N).$$

Soit K le sous A -module de $\mathcal{F}_0(M \times N)$ engendré par les éléments suivants :

$$\begin{aligned}\delta_{(a \cdot m + m', n)} - a \cdot \delta_{(m, n)} - \delta_{(m', n)}, \\ \delta_{(m, a \cdot n + n')} - a \cdot \delta_{(m, n)} - \delta_{(m, n')},\end{aligned}$$

où $m, m' \in M$, $n, n' \in N$ et $a \in A$.

Définition 3.3 On note $M \otimes_A N$, le A -module quotient $\mathcal{F}_0(M \times N)/K$. La classe de $\delta_{(m,n)}$ est notée $m \otimes n \in M \otimes_A N$.

Voici les premières propriétés issues de la définition :

1. $\forall m, m' \in M, \forall n, n' \in N$ et $\forall a \in A$ on a les relations

$$\begin{aligned}(m + m') \otimes n &= m \otimes n + m' \otimes n, \\ m \otimes (n + n') &= m \otimes n + m \otimes n', \\ a \cdot (m \otimes n) &= (a \cdot m) \otimes n = m \otimes (a \cdot n).\end{aligned}$$

2. La famille $\{m \otimes n, (m, n) \in M \times N\}$ est génératrice dans $M \otimes_A N$.

Exemple 3.4 Dans certains cas, le produit tensoriel ne donne que le module trivial réduit au vecteur nul : vérifier que pour tout $n \geq 2$, on a

$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = \{0\}$$

On a vu que l'application canonique $\otimes : M \times N \rightarrow M \otimes_A N$ est A -bilinéaire. Ainsi, la composition $\phi \mapsto \phi \circ \otimes$ définit un morphisme

$$\text{hom}_A(M \otimes_A N, P) \longrightarrow \text{bil}_A(M \times N, P). \quad (7)$$

Réciproquement, si $f : M \times N \rightarrow P$ est une application A -bilinéaire, on définit le morphisme $\tilde{f} : \mathcal{F}_0(M \times N) \rightarrow P$ en posant $\tilde{f}(\delta_{(m,n)}) = f(m, n)$, $\forall (m, n) \in M \times N$. Comme f est A -bilinéaire, le noyau de \tilde{f} contient le module K et donc on peut définir le morphisme

$$\bar{f} : M \otimes_A N \longrightarrow P$$

en posant $\bar{f}(m \otimes n) = f(m, n)$, $\forall (m, n) \in M \times N$.

On montre facilement que l'application $f \in \text{bil}_A(M \times N, P) \mapsto \bar{f} \in \text{hom}_A(M \otimes_A N, P)$ est l'application réciproque du morphisme (7).

Proposition 3.5 *Pour tous A -modules M, N, P , on a des isomorphismes de A -modules canoniques*

$$\text{hom}_A(M \otimes_A N, P) \simeq \text{bil}_A(M \times N, P) \simeq \text{hom}_A(M, \text{hom}_A(N, P)).$$

3.3 Quelques propriétés du produit tensoriel

On commence avec le résultat suivant

Lemme 3.6 1. *Pour tout A -module M , on a un isomorphisme canonique $A \otimes_A M \simeq M$.*

2. *On a un isomorphisme canonique $M \otimes_A N \simeq N \otimes_A M$ qui envoie $m \otimes n$ sur $n \otimes m$.*

3. *On a un isomorphisme canonique $(M \otimes_A N) \otimes P \simeq N \otimes_A (M \otimes P)$ qui envoie $(m \otimes n) \otimes p$ sur $n \otimes (m \otimes p)$.*

Considérons maintenant deux morphismes de A -modules

$$f : M \rightarrow M' \quad \text{et} \quad g : N \rightarrow N'.$$

Lemme 3.7 *Il existe une unique morphisme $f \otimes g : M \otimes_A N \rightarrow M' \otimes_A N'$ qui satisfait les relations*

$$f \otimes g(m \otimes n) = f(m) \otimes g(n).$$

Le résultat précédent se montre en considérant l'application $F : M \times N \rightarrow M' \otimes_A N'$ défini par les relations

$$F(m, n) = f(m) \otimes g(n).$$

On remarque que F est A -bilinéaire, ainsi il se factorise en un morphisme $f \otimes g := \bar{F} : M \otimes_A N \longrightarrow M' \otimes_A N'$ (voir la section précédente).

Remarque 3.8 1. Si $f : M \rightarrow M'$ et $g : N \rightarrow N'$ sont surjectifs, alors $f \otimes g : M \otimes_A N \rightarrow M' \otimes_A N'$ est un morphisme surjectif.

2. Par contre, il existe des cas où $f : M \rightarrow M'$ et $g : N \rightarrow N'$ sont des morphismes injectifs sans que $f \otimes g : M \otimes_A N \rightarrow M' \otimes_A N'$ le soit. Par exemple, si $g : \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ est l'application identité et $f : \mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto 2x$, alors $f \otimes g : \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ est l'application nulle.

On montre maintenant que le produit tensoriel se comporte de manière optimale par rapport aux sommes directes.

Proposition 3.9 Soient N et $M_i, i \in I$, des A -modules. On a un isomorphisme de A -modules

$$\left(\bigoplus_{i \in I} M_i \right) \otimes_A N \simeq \bigoplus_{i \in I} M_i \otimes_A N.$$

Corollaire 3.10 Si $(e_i)_{i \in I}$ est une base du module M et $(f_j)_{j \in J}$ est une base du module N , alors $(e_i \otimes f_j)_{(i,j) \in I \times J}$ est une base du module $M \otimes_A N$.

On va maintenant aborder la question d'extension des coefficients. Soient $\varphi : A \rightarrow B$ un morphisme d'anneaux commutatifs et M un A -module. Rappelons que B possède une structure de A -module en posant $a \cdot b := \varphi(a)b$. Le produit tensoriel $B \otimes_A M$ est par définition un A -module.

Lemme 3.11 $B \otimes_A M$ admet une structure de B -module qui satisfait la relation

$$b \cdot (b' \otimes m) := bb' \otimes m, \quad \forall b, b' \in B, \forall m \in M.$$

Preuve : pour tout $b \in B$, on considère l'application $T_b : B \times M \rightarrow B \otimes_A M$ telle que $T_b(b', m) := bb' \otimes m$. On vérifie que T_b est A -bilinéaire, ainsi elle se factorise en un morphisme A -linéaire $\overline{T}_b : B \otimes_A M \rightarrow B \otimes_A M$. Alors le produit extérieur $B \times B \otimes_A M \rightarrow B \otimes_A M$ est déterminé par la relation : $b \cdot v := \overline{T}_b(v)$. On vérifie facilement que cela définit une structure de B -module sur $B \otimes_A M$. \square

Exercice 3.12 Soient I un idéal de A et M un A -module. Le A/I -module $A/I \otimes_A M$ est canoniquement isomorphe à M/IM .

3.4 Algèbre extérieure et produit symétrique d'un espace vectoriel

4 Représentations de groupes finis

4.1 Premières notions

Une action d'un groupe G sur un ensemble \mathcal{X} est la donnée d'une application

$$\begin{aligned} G \times \mathcal{X} &\longrightarrow \mathcal{X} \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

satisfaisant $h \cdot (g \cdot x) = hg \cdot x$ et $1 \cdot x = x$, $\forall g, h \in G$, $\forall x \in \mathcal{X}$.

Définition 4.1 Une représentation d'un groupe G est la donnée d'un \mathbb{K} -espace vectoriel V et d'un morphisme de groupes

$$\rho : G \rightarrow GL(V),$$

où $GL(V) = \{f : V \rightarrow V \text{ isomorphisme } \mathbb{K} - \text{linéaire}\}$.

L'action du groupe G sur l'espace vectoriel V est défini par la relation $g \cdot v := \rho(g)(v)$. On voit donc qu'une représentation d'un groupe G n'est autre qu'une action $(g, v) \mapsto g \cdot v$ qui est linéaire par rapport à la variable $v \in V$.

Voici quelques exemples de représentations de groupes :

1. $GL_n(\mathbb{K})$ agissant sur $M_n(\mathbb{K})$:

$$\boxed{g \cdot X = gX}, \quad \boxed{g \cdot X = Xg^{-1}}, \quad \boxed{g \cdot X = gXg^{-1}},$$

$$\boxed{g \cdot X = X {}^t g}, \quad \boxed{g \cdot X = gX {}^t g}.$$

2. Le groupe symétrique \mathfrak{S}_n agissant sur \mathbb{K}^n :

$$\sigma \cdot (x_1, \dots, x_n) = (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)}).$$

3. Le groupe symétrique \mathfrak{S}_n agissant sur $\mathbb{K}[X_1, \dots, X_n]$:

$$(\sigma \cdot P)(X_1, \dots, X_n) = P(X_{\sigma^{-1}(1)}, \dots, X_{\sigma^{-1}(n)}).$$

4. Le groupe linéaire $GL_n(\mathbb{K})$ agissant sur $\mathbb{K}[X_1, \dots, X_n]$:

$$(g \cdot P)(X_1, \dots, X_n) = P(g^{-1}(X_1, \dots, X_n)).$$

5. Le groupe symétrique \mathfrak{S}_n agissant sur \mathbb{K} au moyen de la signature $\epsilon : \mathfrak{S}_n \rightarrow \{\pm 1\}$:

$$\sigma \cdot z = \epsilon(\sigma)z.$$

6. Le groupe $(\mathbb{K}, +)$ agissant sur \mathbb{K}^2 à travers le morphisme

$$\rho(\lambda) := \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}.$$

7. Le groupe $\mathbb{Z}/n\mathbb{Z}$ agissant sur \mathbb{R}^2 à travers le morphisme $\rho_\ell : \mathbb{Z}/n\mathbb{Z} \rightarrow GL_2(\mathbb{R})$:

$$\rho_\ell(\bar{k}) = \begin{pmatrix} \cos\left(\frac{2k\ell\pi}{n}\right) & -\sin\left(\frac{2k\ell\pi}{n}\right) \\ \sin\left(\frac{2k\ell\pi}{n}\right) & \cos\left(\frac{2k\ell\pi}{n}\right) \end{pmatrix}.$$

4.1.1 Sous-représentations et quotients

Définition 4.2 Soit (V, ρ) une représentation du groupe G .

Un sous-espace vectoriel $W \subset V$ est une sous-représentation de V si

$$\rho(g)(W) \subset W, \quad \forall g \in G.$$

Dans ce cas le morphisme $\rho' : G \rightarrow GL(W)$, défini par $\rho'(g) = \rho(g)|_W$ définit une représentation du groupe G .

Voici quelques exemples :

1. Le groupe symétrique \mathfrak{S}_n agissant sur \mathbb{K}^n : les sous-espaces $W_1 = \mathbb{K}(1, \dots, 1)$ et $W_2 = \{x_1 + \dots + x_n = 0\}$ sont des sous-représentations.
2. Le groupe $GL_n(\mathbb{K})$ agissant sur $M_n(\mathbb{K})$ avec $g \cdot X = gX^t g$: les sous-espaces $S_n := \{\text{matrices symétriques}\}$ et $A_n := \{\text{matrices antisymétriques}\}$ sont des sous-représentations.
3. Le groupe $GL_n(\mathbb{K})$ agissant sur $M_n(\mathbb{K})$ par conjugaison : $g \cdot X = gXg^{-1}$. Le sous-espace $W := \{X \in M_n(\mathbb{K}), \text{Tr}(X) = 0\}$ est une sous-représentation.
4. Le groupe $GL_n(\mathbb{K})$ agissant sur l'espace fonctionnel $\mathcal{F}(\mathbb{K}^n)$ formé de toutes les fonctions $f : \mathbb{K}^n \rightarrow \mathbb{K}$. L'action est définie par la relation $(g \cdot f)(v) := f(g^{-1} \cdot v)$. Le sous-espace vectoriel $\text{Pol}(\mathbb{K}^n) \subset \mathcal{F}(\mathbb{K}^n)$ formé des fonctions polynomiales est une sous-représentation.

Définition 4.3 Soit (V, ρ) une représentation du groupe G . On note V^G la sous-représentation formée des vecteurs $v \in V$ vérifiant

$$g \cdot v = v, \quad \forall g \in G.$$

Les vecteurs de V^G sont appelés les invariants de l'action.

Voici quelques exemples :

1. \mathfrak{S}_n agissant sur \mathbb{K}^n : ici $(\mathbb{K}^n)^{\mathfrak{S}_n} = \mathbb{K}(1, \dots, 1)$.
2. $GL_n(\mathbb{K})$ agissant sur $M_n(\mathbb{K})$ par conjugaison : les matrices invariantes pour cette action sont de la forme λI_n avec $\lambda \in \mathbb{K}$.
3. \mathfrak{S}_n agissant sur $\mathbb{K}[X_1, \dots, X_n]$: les polynômes invariants pour cette action sont appelés les polynômes symétriques.

Définition 4.4 Soit $W \subset V$ une sous-représentation du groupe G . L'espace vectoriel quotient W/V est muni d'une action linéaire du groupe G , définie par la relation

$$g \cdot \bar{w} := \overline{g \cdot w}, \quad \forall (g, w) \in G \times W.$$

4.1.2 Morphismes entre deux représentations

Soient V_1 et V_2 deux représentations du groupe G , sur le même corps \mathbb{K} :

$$\rho_1 : G \rightarrow GL(V_1) \quad \text{et} \quad \rho_2 : G \rightarrow GL(V_2).$$

Définition 4.5 L'espace vectoriel $\text{hom}_{\mathbb{K}}(V_1, V_2)$ est muni d'une action linéaire du groupe G , qui est définie par la relation :

$$g \cdot f = \rho_2(g) \circ f \circ \rho_1^{-1}(g), \quad \forall f \in \text{hom}_{\mathbb{K}}(V_1, V_2), \forall g \in G.$$

Définition 4.6 On note $\text{hom}_G(V_1, V_2) \subset \text{hom}_{\mathbb{K}}(V_1, V_2)$ la sous-représentation formée des éléments invariants pour l'action de G . Les éléments de $\text{hom}_G(V_1, V_2)$ sont appelés des morphismes entre les représentations V_1 et V_2 .

Ainsi, une application \mathbb{K} -linéaire $f : V_1 \rightarrow V_2$ est un morphisme si pour tout $g \in G$, on a la relation :

$$f \circ \rho_1(g) = \rho_2(g) \circ f.$$

Définition 4.7 Deux représentations V_1 et V_2 sont dites isomorphes si $\exists f \in \text{hom}_G(V_1, V_2)$ qui soit bijectif. On note alors $V_1 \simeq V_2$.

Exemple 4.8 Soit $\pi : \mathbb{K}[X_1, \dots, X_n] \rightarrow \text{Pol}(\mathbb{K}^n)$ l'application canonique qui à un élément $P \in \mathbb{K}[X_1, \dots, X_n]$ associe la fonction polynomiale

$$(x_1, \dots, x_n) \mapsto P(x_1, \dots, x_n).$$

L'application π est un morphisme entre deux représentations de $GL_n(\mathbb{K})$: c'est un isomorphisme si et seulement si \mathbb{K} est un corps infini.

On termine cette section avec un résultat de factorisation.

Proposition 4.9 Soit $f \in \text{hom}_G(V_1, V_2)$. Alors

- $\text{Im}(f)$ est une sous-représentation de V_2 ,
- $\text{ker}(f)$ est une sous-représentation de V_1 ,
- Les représentations $V_1/\text{ker}(f)$ et $\text{Im}(f)$ sont isomorphes.

4.1.3 Somme et produit tensoriel

Considérons deux représentations V et W d'un groupe G (définies sur un corps \mathbb{K}). On peut alors construire d'autres représentations de G :

- Le produit cartésien $V \times W : g \cdot (v, w) := (g \cdot v, g \cdot w), \quad \forall (v, w) \in V \times W.$
- Le produit tensoriel $V \otimes_{\mathbb{K}} W : g \cdot (v \otimes w) := g \cdot v \otimes g \cdot w, \quad \forall (v, w) \in V \times W.$
- Le dual $V^* = \text{hom}_{\mathbb{K}}(V, \mathbb{K}) : \langle g \cdot \xi, v \rangle := \langle \xi, g^{-1} \cdot v \rangle, \quad \forall (v, \xi) \in V \times V^*.$
- $\text{hom}_{\mathbb{K}}(V, W)$

À tout couple $(\xi, w) \in V^* \times W$, on associe l'application linéaire $\rho(\xi, w) \in \text{hom}_{\mathbb{K}}(V, W)$ définie par la relation

$$\rho(\xi, w)(v) := \langle \xi, v \rangle w, \quad \forall v \in V.$$

L'application $\rho : V^* \times W \rightarrow \text{hom}_{\mathbb{K}}(V, W)$ est un morphisme entre deux représentations de G . De plus, comme ρ est bilinéaire, elle se factorise en un morphisme

$$\bar{\rho} : V^* \otimes_{\mathbb{K}} W \longrightarrow \text{hom}_{\mathbb{K}}(V, W). \quad (8)$$

Proposition 4.10 *Si V et W sont deux représentations de dimension finies, le morphisme $\bar{\rho}$ détermine un isomorphisme*

$$V^* \otimes_{\mathbb{K}} W \simeq \text{hom}_{\mathbb{K}}(V, W).$$

On utilise le produit tensoriel dans le cadre plus général suivant. Soient E une représentation d'un groupe G_1 et F une représentation d'un groupe G_2 (toutes deux définies sur un corps \mathbb{K}). Alors $E \otimes_{\mathbb{K}} F$ est une représentation de $G_1 \times G_2$: l'action linéaire de $(g_1, g_2) \in G_1 \times G_2$ sur $E \otimes_{\mathbb{K}} F$ est définie par la relation

$$(g_1, g_2) \cdot (e \otimes f) := g_1 \cdot e \otimes g_2 \cdot f, \quad \forall (e, f) \in E \times F.$$

4.1.4 Représentations irréductibles

Définition 4.11 *Une représentation V d'un groupe G est dite irréductible si les seules sous-représentations de V sont $\{0\}$ et V .*

On a un critère élémentaire pour savoir si une représentation $\rho : G \rightarrow GL(V)$ est irréductible. À tout vecteur $v \in V$, on associe le sous espace vectoriel $E(v)$ engendré par la famille $g \cdot v, g \in G$. On voit que $E(v) \subset V$ est une sous-représentation.

Lemme 4.12 *Une représentation V d'un groupe G est irréductible si et seulement si*

$$E(v) = V$$

pour tout $v \in V$ non-nul.

Considérons l'action du groupe $\mathbb{Z}/n\mathbb{Z}$ sur \mathbb{R}^2 à travers le morphisme $\rho : \mathbb{Z}/n\mathbb{Z} \rightarrow GL_2(\mathbb{R})$:

$$\rho(\bar{k}) = \begin{pmatrix} \cos(\frac{2k\pi}{n}) & -\sin(\frac{2k\pi}{n}) \\ \sin(\frac{2k\pi}{n}) & \cos(\frac{2k\pi}{n}) \end{pmatrix} = \rho(\bar{1})^k.$$

On voit que (\mathbb{R}^2, ρ) est une représentation irréductible de $\mathbb{Z}/n\mathbb{Z}$. Considérons maintenant la cas de \mathbb{C}^2 muni de la même action ρ . Dans ce cas, (\mathbb{C}^2, ρ) n'est pas une représentation irréductible de $\mathbb{Z}/n\mathbb{Z}$, car la droite $\mathbb{C}(i, 1)$ est une sous-représentation de \mathbb{C}^2 .

Considérons maintenant l'action du groupe symétrique \mathfrak{S}_n sur \mathbb{K}^n . On a $\mathbb{K}^n = E_1 \oplus E_2$ où $E_1 = \mathbb{K}(1, \dots, 1)$ et $E_2 = \{x_1 + \dots + x_n = 0\}$ sont deux sous-représentations. On vérifie que E_1 et E_2 sont toutes deux des représentations irréductibles de \mathfrak{S}_n .

4.1.5 Lemme de Schur

Dans cette partie on suppose que le corps \mathbb{K} est algébriquement clos.

Soient V, W deux représentations irréductibles **de dimension finies** d'un groupe G (définies sur le corps \mathbb{K}). Nous nous intéressons au \mathbb{K} -espace vectoriel $\text{hom}_G(V, W)$.

Lemme 4.13 (Lemme de Schur)

- Si V et W ne sont pas isomorphes, alors $\text{hom}_G(V, W) = \{0\}$.
- Si $V \simeq W$, alors $\dim \text{hom}_G(V, W) = 1$.

Preuve : Supposons tout d'abord que V et W ne sont pas isomorphes et considérons $f \in \text{hom}_G(V, W)$. Comme le morphisme f n'est pas bijectif, nous pouvons considérer deux cas :

- Soit $\ker(f) \neq \{0\}$. Comme $\ker(f)$ est une sous-représentation de V , et que V est irréductible, on doit avoir $\ker(f) = V$.
- Soit $\text{Image}(f) \neq W$. Comme $\text{Image}(f)$ est une sous-représentation de W , et que W est irréductible, on doit avoir $\text{Image}(f) = \{0\}$.

Dans les deux cas, on obtient $f = 0$.

Supposons maintenant qu'il existe un isomorphisme $h : V \rightarrow W$ entre les deux représentations. L'application $g \mapsto h \circ g$ définit alors un isomorphisme entre les espaces vectoriel $\text{hom}_G(V, V)$ et $\text{hom}_G(V, W)$. Il nous suffit alors de montrer que $\dim \text{hom}_G(V, V) = 1$.

Soit $g \in \text{hom}_G(V, V)$. Comme le corps \mathbb{K} est algébriquement clos et que le \mathbb{K} -espace vectoriel V est de dimension fini, il existe $\lambda \in \mathbb{K}$ tel que le sous-espace propre $\ker(g - \lambda Id_V)$ est non-nul. Sachant que $g - \lambda Id_V$ appartient à $\text{hom}_G(V, V)$, on voit que $\ker(g - \lambda Id_V)$ est une sous-représentation de V . Cette dernière étant irréductible, on a $\ker(g - \lambda Id_V) = V$, i. e. $g = \lambda Id_V$. On vient de montrer que $\text{hom}_G(V, V) = \mathbb{K}Id_V$. \square

4.2 Le cas des groupes finis

Dans toute la suite G désigne un groupe fini. De plus les représentations de G que l'on considère sont des espaces vectoriels **complexes** de dimension finies.

4.2.1 L'algèbre $\mathbb{C}[G]$

On note $\mathbb{C}[G]$ l'ensemble des fonctions sur G à valeurs complexes. C'est un espace vectoriel complexe qui admet pour base canonique la famille de fonctions $\{\delta_g, g \in G\}$:

$$\delta_g(x) = \begin{cases} 1 & \text{si } x = g \\ 0 & \text{si } x \neq g. \end{cases}$$

On munit $\mathbb{C}[G]$ du produit de convolution $\star : \mathbb{C}[G] \times \mathbb{C}[G] \rightarrow \mathbb{C}[G]$, qui est défini par la relation

$$\lambda \star \mu(g) := \sum_{h \in G} \lambda(h) \mu(h^{-1}g).$$

Le produit \star définit une loi associative sur $\mathbb{C}[G]$ qui admet δ_1 comme élément neutre : $\delta_1 \star \mu = \mu \star \delta_1 = \mu$ pour tout $\mu \in \mathbb{C}[G]$.

Le produit \star est distributif par rapport à la structure d'espace vectoriel de $\mathbb{C}[G]$: on a

$$(a\lambda + b\eta) \star \mu = a(\lambda \star \mu) + b(\eta \star \mu), \quad \forall a, b \in \mathbb{C}, \forall \lambda, \eta, \mu \in \mathbb{C}[G].$$

Idem pour le produit $\mu \star (a\lambda + b\eta)$. Ainsi $(\mathbb{C}[G], +, \star)$ est une \mathbb{C} -algèbre. On remarque que

$$\delta_g \star \delta_h = \delta_{gh} \tag{9}$$

pour tout $g, h \in G$. Ainsi $\mathbb{C}[G]$ est une algèbre abélienne si et seulement si le groupe G est abélien.

Le centre de $\mathbb{C}[G]$

Définition 4.14 On note $\mathcal{Z}[G]$ le centre de l'algèbre $\mathbb{C}[G]$.

On remarque que les conditions suivantes sont équivalentes :

- $\lambda \in \mathcal{Z}[G]$,
- $\lambda \star \delta_g = \delta_g \star \lambda, \forall g \in G$,
- $\lambda(hg) = \lambda(gh), \forall g, h \in G$,
- λ est une fonction constante sur les classes de conjugaison de G .

Si $\mathcal{C} \subset G$ est une classe de conjugaison, on note $\mathbf{1}_{\mathcal{C}} \in \mathcal{Z}[G]$ la fonction caractéristique de \mathcal{C} .

Lemme 4.15 Les fonctions $\mathbf{1}_C$, où C parcourt les classes de conjugaisons de G , forment une base de $\mathcal{Z}[G]$.

Structure de $\mathbb{C}[G]$ -modules

Définition 4.16 Soit V un espace vectoriel complexe. Une structure de $\mathbb{C}[G]$ -module sur V est la donnée d'un morphisme d'algèbres

$$\tilde{\rho} : \mathbb{C}[G] \longrightarrow \text{End}_{\mathbb{C}}(V),$$

telle que $\tilde{\rho}(\delta_1) = \text{Id}_V$.

Notons $\mathbb{C}[G]^\times$ l'ensemble des éléments inversibles de $\mathbb{C}[G]$: c'est un groupe par rapport à la loi \star . On remarque qu'un morphisme d'algèbres $\tilde{\rho} : \mathbb{C}[G] \rightarrow \text{End}_{\mathbb{C}}(V)$ induit un morphisme de groupe

$$\tilde{\rho} : \mathbb{C}[G]^\times \rightarrow \text{GL}(V)$$

car $\text{GL}(V) = (\text{End}_{\mathbb{C}}(V))^\times$. Les relations (9) montre que l'application $g \mapsto \delta_g$ est un morphisme de groupe entre G et $\mathbb{C}[G]^\times$.

Si on part d'un morphisme d'algèbres $\tilde{\rho} : \mathbb{C}[G] \longrightarrow \text{End}_{\mathbb{C}}(V)$, l'application $\rho : g \in G \mapsto \tilde{\rho}(\delta_g) \in \text{GL}(V)$ est un morphisme de groupe.

Réciproquement, considérons un morphisme de groupe $\rho : G \rightarrow \text{GL}(V)$. On détermine un morphisme d'algèbre $\tilde{\rho} : \mathbb{C}[G] \longrightarrow \text{End}_{\mathbb{C}}(V)$ en posant

$$\tilde{\rho} \left(\sum_{g \in G} \lambda(g) \delta_g \right) := \sum_{g \in G} \lambda(g) \rho(g).$$

Conclusion : on a montré que sur un espace vectoriel complexe, une structure de $\mathbb{C}[G]$ -module est équivalente à celle d'être une représentation de G .

La remarque qui suit sera utile plus tard.

Lemme 4.17 Soit $\tilde{\rho} : \mathbb{C}[G] \longrightarrow \text{End}_{\mathbb{C}}(V)$ le morphisme associé à une représentation V . Pour tout $\phi \in \mathcal{Z}[G]$, on a $\tilde{\rho}(\phi) \in \text{hom}_G(V, V)$.

Preuve : Comme $\tilde{\rho}(\lambda) = \sum_{g \in G} \phi(g) \rho(g)$, on voit que

$$\rho(h) \tilde{\rho}(\phi) \rho(h)^{-1} = \sum_{g \in G} \phi(g) \rho(hgh^{-1}) = \sum_{g \in G} \phi(h^{-1}gh) \rho(g) = \tilde{\rho}(\lambda)$$

car ϕ est une fonction constante sur les classes de conjugaison de G . \square

Représentation régulière de G

L'action par translation à gauche de G sur lui-même permet de munir l'espace vectoriel $\mathbb{C}[G]$ d'une représentation de G , appelée représentation régulière. Celle-ci est déterminée par les relations suivantes

$$(h \cdot_r \lambda)(x) = \lambda(h^{-1}x), \quad \forall \lambda \in \mathbb{C}[G], \quad \forall h, x \in G.$$

On remarque par exemple que

$$h \cdot_r \delta_g = \delta_{hg}, \quad \forall h, g \in G.$$

Soit (V, ρ) une représentation irréductible de G et $v \in V - \{0\}$. On considère l'application linéaire

$$T_v : \mathbb{C}[G] \longrightarrow V$$

définie par $T_v(\lambda) = \sum_{h \in G} \lambda(h) \rho(h)(v)$.

Lemme 4.18 T_v est un morphisme surjectif entre la représentation régulière et V . Cela implique que $\dim V \leq n$.

Preuve : T_v est un morphisme car $T_v(g \cdot_r \lambda) = \rho(g)(T_v(\lambda))$.

Par définition, l'image de T_v est égal à l'espace vectoriel $E(v)$ engendré par la famille $\rho(h)(v), h \in G$. Comme (V, ρ) est une représentation irréductible de G , on a $E(v) = V$ (voir le Lemme 4.12). Conclusion : T_v est un morphisme surjectif. \square

4.2.2 Projection sur les invariants

A toute représentation E de G , on associe l'application linéaire $\pi_E \in \text{End}_{\mathbb{C}}(E)$:

$$\pi_E(v) = \frac{1}{|G|} \sum_{g \in G} g \cdot v, \quad v \in E.$$

Lemme 4.19 π_E est un projecteur sur le sous-espace vectoriel E^G :

- $\pi_E \circ \pi_E = \pi_E$.
- $\text{Image}(\pi_E) = E^G$.

On peut voir aussi π_E comme un morphisme surjectif entre E et la sous-représentation E^G .

Voici une application importante du lemme précédent.

Proposition 4.20 Soit (V, ρ_V) une représentation de G et $W \subset V$ une sous-représentation. Alors il existe une sous-représentation $W' \subset V$ telle que

$$W \oplus W' = V.$$

Preuve : Considérons l'action linéaire de G sur $E := \text{hom}_{\mathbb{C}}(V, V)$. D'après le lemme précédent, on a un morphisme surjectif $\pi : E \rightarrow E^G = \text{hom}_G(V, V)$ défini par

$$\pi(A) = \frac{1}{|G|} \sum_{g \in G} \rho_V(g) \circ A \circ \rho_V(g)^{-1}, \quad A \in \text{hom}_{\mathbb{C}}(V, V).$$

Soit $p \in \text{hom}_{\mathbb{C}}(V, V)$ un projecteur sur W . L'image $\tilde{p} = \pi(p) \in \text{hom}_G(V, V)$ est encore un projecteur sur W . Comme il vérifie les relations

$$\tilde{p}(g \cdot v) = g \cdot \tilde{p}(v), \quad \forall g \in G, \forall v \in V,$$

le sous-espace vectoriel $W' := \ker(\tilde{p})$ est une sous-représentation satisfaisant $W \oplus W' = E$. \square

4.2.3 Décomposition en facteurs irréductibles

Soit (E, ρ) une représentation de G (de dimension finie). Le résultat qui suit se démontre par récurrence sur la dimension de E , au moyen de la proposition 4.20.

Proposition 4.21 *Il existe des sous-représentations $E_j \subset E$, $j = 1, \dots, n$, telles que*

- E_j est irréductible, $\forall j = 1, \dots, n$.
- $E = E_1 \oplus \dots \oplus E_n$.

Appliquons ce résultat à la représentation régulière $\mathbb{C}[G]$.

Définition 4.22 *On note $\mathbb{V}_1, \dots, \mathbb{V}_\ell$ une liste de sous-représentations irréductibles de la représentation régulière satisfaisant la condition suivante : pour toute sous-représentation irréductible E de la représentation régulière, il existe un unique j tel que $E \simeq \mathbb{V}_j$.*

Proposition 4.23 *$\mathbb{V}_1, \dots, \mathbb{V}_\ell$ correspond à la liste de “toutes” les représentations irréductibles de G . En d'autres termes, pour toute représentation irréductible V du groupe G , il existe un unique j tel que $V \simeq \mathbb{V}_j$.*

Preuve : Soit V une représentation irréductible du groupe G . Le choix d'un vecteur $v \in V$ non-nul détermine un morphisme surjectif $T_v : \mathbb{C}[G] \rightarrow V$ (voir Lemme 4.18). Considérons une décomposition

$$\mathbb{C}[G] = \bigoplus_{k=1}^n E_k$$

en sous-représentations irréductibles. Comme T_v est surjectif, un des morphismes $T_v|_{E_k} : E_k \rightarrow V$ est non-nul. D'après le Lemme de Schur cela implique que $V \simeq E_k$. Ainsi, il existe un unique j tel que $V \simeq \mathbb{V}_j$. \square

Dans la suite, lorsque E est une représentation et $m \in \mathbb{N}$, on utilisera la notation suivante

$$mE = \begin{cases} \{0\} & \text{si } m = 0, \\ \underbrace{E \oplus \dots \oplus E}_{m \text{ fois}} & \text{si } m \geq 1. \end{cases}$$

On peut préciser la proposition 4.21 de la manière suivante.

Proposition 4.24 *Soit E une représentation de G (de dimension finie). Alors*

$$E \simeq \bigoplus_{j=1}^{\ell} m_j \mathbb{V}_j$$

avec $m_j = \dim \text{hom}_G(\mathbb{V}_j, E)$.

Dans l'isomorphisme $E \simeq \bigoplus_{j=1}^{\ell} m_j \mathbb{V}_j$, chaque entier m_j correspond à la multiplicité de la représentation irréductible \mathbb{V}_j dans la représentation E .

4.2.4 Caractère d'une représentation

Si V est un espace vectoriel complexe de dimension finie, nous avons l'application linéaire "trace"

$$\text{Tr} : \text{End}_{\mathbb{C}}(V) \rightarrow \mathbb{C}$$

qui est définie de la manière suivante. Considérons une base e_1, \dots, e_n de V et la base duale e_1^*, \dots, e_n^* de V^* : alors pour tout $A \in \text{End}_{\mathbb{C}}(V)$, on pose

$$\text{Tr}(A) = \sum_{k=1}^n \langle e_k^*, A(e_k) \rangle.$$

Un petit calcul permet de vérifier que la somme de droite ne dépend pas du choix de la base.

Définition 4.25 *Le caractère d'une représentation $\rho : G \rightarrow GL(V)$ est la fonction $\chi_V : G \rightarrow \mathbb{C}$ définie par*

$$\chi_V(g) := \text{Tr}(\rho(g)), \quad g \in G.$$

Voici quelques propriétés de la fonction caractère :

- $\chi_V(1) = \dim V$.
- $\chi_V(g) \leq \dim V$, pour tout $g \in G$.
- $\chi_V(g) = \dim V$ si et seulement si $\rho(g)$ est une homothétie.
- $\dim(V^G) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)$.
- $\chi_V \in \mathcal{Z}[G]$.
- $\chi_V = \chi_W$ si $V \simeq W$.

Voici d'autres propriétés relatives aux opérations "somme" et "produit tensoriel".

Lemme 4.26 *Soient V et W deux représentations de G . Alors*

- $\chi_{V \oplus W} = \chi_V + \chi_W$.
- $\chi_{V \otimes W} = \chi_V \chi_W$.
- $\chi_{V^*} = \overline{\chi_V}$.
- $\chi_{\text{hom}(V, W)} = \overline{\chi_V} \chi_W$

Munissons l'espace vectoriel $\mathbb{C}[G]$ du produit hermitien

$$\langle \lambda, \mu \rangle := \frac{1}{|G|} \sum_{g \in G} \lambda(g) \overline{\mu(g)}.$$

On a le lemme crucial suivant.

Lemme 4.27 *Soient V et W deux représentations de G .*

1. $\langle \chi_V, \chi_W \rangle = \dim(\text{hom}_G(W, V))$.
2. Si V et W sont irréductibles, on a

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & \text{si } V \simeq W, \\ 0 & \text{sinon.} \end{cases}$$

3. V est irréductible si et seulement si $\langle \chi_V, \chi_V \rangle = 1$.
4. $V \simeq W$ si et seulement si $\chi_V = \chi_W$.

Preuve : Le premier point découle du calcul suivant

$$\begin{aligned} \langle \chi_V, \chi_W \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_W(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{V \otimes W^*}(g) \\ &= \dim(V \otimes W^*)^G. \end{aligned}$$

Maintenant, sachant que $V \otimes W^* \simeq \text{hom}(W, V)$, on voit que $(V \otimes W^*)^G \simeq \text{hom}_G(W, V)$.

Le deuxième point découle du premier point et du lemme de Schur.

Pour le troisième point, on utilise la proposition 4.24. Nous avons une décomposition $V \simeq \bigoplus_{j=1}^{\ell} m_j \mathbb{V}_j$ avec $m_j = \dim \text{hom}_G(\mathbb{V}_j, V)$. Comme les produits hermitiens $\langle \chi_{\mathbb{V}_i}, \chi_{\mathbb{V}_j} \rangle$ sont nuls si $i \neq j$ et égaux à 1 si $i = j$, on obtient

$$\langle \chi_V, \chi_V \rangle = \sum_{j=1}^{\ell} (m_j)^2. \quad (10)$$

C'est maintenant clair que $\langle \chi_V, \chi_V \rangle = 1$ si et seulement si V est irréductible.

Le dernier point vient du fait que dans la décomposition $V \simeq \bigoplus_{j=1}^{\ell} m_j \mathbb{V}_j$, les multiplicités $m_j \in \mathbb{N}$ sont déterminés par les relations

$$m_j = \langle \chi_V, \chi_{\mathbb{V}_j} \rangle .$$

Cela entraîne que si $\chi_V = \chi_W$, alors $V \simeq W$.

4.2.5 Premier pas vers la classification des représentations irréductibles

On a montré à la section 4.2.3 que G admet un nombre fini de représentations irréductibles $\mathbb{V}_1, \dots, \mathbb{V}_\ell$, et celles-ci apparaissent toutes dans la représentation régulière $\mathbb{C}[G]$: on a

$$\mathbb{C}[G] \simeq \bigoplus_{j=1}^{\ell} n_j \mathbb{V}_j, \quad (11)$$

avec $n_j \geq 1$ pour tout j .

Un calcul direct nous donne le caractère de la représentation régulière :

$$\chi_{\mathbb{C}[G]}(g) = \begin{cases} |G| & \text{si } g = 1, \\ 0 & \text{si } g \neq 1. \end{cases}$$

Cela permet de voir que les multiplicités n_j satisfont les relations :

$$n_j = \langle \chi_{\mathbb{C}[G]}, \chi_{\mathbb{V}_j} \rangle = \dim \mathbb{V}_j.$$

En comparant les dimensions dans l'identité (11), on obtient une première relation

$$\boxed{|G| = \sum_{j=1}^{\ell} (\dim \mathbb{V}_j)^2}$$

Nous allons maintenant montrer que les caractères des représentations irréductibles $\mathbb{V}_1, \dots, \mathbb{V}_\ell$ définissent une base de l'espace vectoriel $\mathcal{Z}[G]$. On sait déjà que $(\chi_{\mathbb{V}_j})_{1 \leq j \leq \ell}$ est une famille libre puisqu'elle est orthogonale.

Pour s'assurer que $(\chi_{\mathbb{V}_j})_{1 \leq j \leq \ell}$ est une famille génératrice de $\mathcal{Z}[G]$, il suffit de montrer le lemme suivant.

Lemme 4.28 *Soit $\phi \in \mathcal{Z}[G]$, tel que $\langle \phi, \chi_{\mathbb{V}_j} \rangle = 0, \forall j$. Alors $\phi = 0$.*

Preuve : Soit $\phi \in \mathcal{Z}[G]$, tel que $\langle \phi, \chi_{\mathbb{V}_j} \rangle = 0, \forall j$.

Soit (E, ρ) une représentation de G et $\tilde{\rho} : \mathbb{C}[G] \longrightarrow \text{End}_{\mathbb{C}}(E)$ le morphisme d'algèbre associé. L'endomorphisme $\tilde{\rho}(\phi) \in \text{hom}_G(E, E)$ est défini par la relation

$$\tilde{\rho}(\phi) = \sum_{g \in G} \phi(g) \rho(g).$$

Considérons des sous-représentations $E_k \subset E$ irréductibles, $k = 1, \dots, n$, telles que $E = E_1 \oplus \dots \oplus E_n$. L'endomorphisme $\tilde{\rho}(\phi)$ laisse stable chaque sous-représentation E_k . Comme $\tilde{\rho}(\phi)|_{E_k} \in \text{hom}_G(E_k, E_k)$, il existe $a_k \in \mathbb{C}$ tel que

$$\tilde{\rho}(\phi)|_{E_k} = a_k \text{Id}_{E_k}.$$

En prenant la trace, on obtient

$$a_k = \frac{1}{\dim(E_k)} \text{Tr}(\tilde{\rho}(\phi)|_{E_k}) = \frac{1}{\dim(E_k)} \sum_{g \in G} \phi(g) \text{Tr}(\rho_{E_k}(g)) = \frac{|G|}{\dim(E_k)} \langle \phi, \chi_{E_k^*} \rangle.$$

Mais sachant qu'il existe j tel que $E_k^* \simeq \mathbb{V}_j$, on en déduit que $\langle \phi, \chi_{E_k^*} \rangle = \langle \phi, \chi_{\mathbb{V}_j} \rangle = 0$. On obtient que $a_k = 0, \forall k$.

On a donc montré que l'endomorphisme $\tilde{\rho}(\phi) \in \text{hom}_G(E, E)$ est nul pour n'importe quelle représentation E .

Appliquons ce résultat à la représentation régulière $E = \mathbb{C}[G]$. Rappelons que le morphisme $\rho_r : G \rightarrow GL(\mathbb{C}[G])$ satisfait la relation $\rho_r(g)(\delta_1) = \delta_g$. Ainsi le vecteur $\tilde{\rho}_r(\phi)(\delta_1)$ est égal à

$$\sum_{g \in G} \phi(g) \delta_g \in \mathbb{C}[G].$$

Comme $\tilde{\rho}_r(\phi) = 0$, on doit avoir $\sum_{g \in G} \phi(g) \delta_g = 0$. Cette dernière condition impose que $\phi = 0$. \square

Nous pouvons maintenant résumer ce que nous avons démontré concernant les représentations irréductibles complexes d'un groupe fini.

Théorème 4.29 *Soit G un groupe fini. Notons $\ell \geq 1$ le nombre de classes de conjugaison de G . Alors G admet exactement ℓ représentations irréductibles $\mathbb{V}_1, \dots, \mathbb{V}_\ell$ satisfaisant la relation*

$$|G| = \sum_{j=1}^{\ell} (\dim \mathbb{V}_j)^2.$$