Algèbre approfondie

Notes de cours
Master 2 Mathématiques 2013-2014

Julien Bichon
Département de Mathématiques
Université Blaise Pascal
Julien.Bichon@math.univ-bpclermont.fr

Les pages qui suivent constituent les notes de cours “Algèbre approfondie” du Master 2 Mathématiques. Bien sûr, il est probable que des coquilles ou erreurs se sont glissées dans ce document, merci de me les signaler !

Voici quelques références utiles.

•D. Dummit, R. Foote, Abstract algebra. Third edition, John Wiley & Sons, 2004.

• D. Guin, Algèbre (tome 1), Belin, 1997.

• D. Perrin, Cours d'algèbre, Ellipses, 1996.

•J. P. Serre, Représentations linéaires des groupes fini, Hermann, Paris, 1978.

•P. Tauvel, Mathématiques générales pour l'agrégation, Masson, Paris, 1997.

Table des matières

I Modules

Rappel : un **anneau** est un triplet $(A, +, \cdot)$ où A est un ensemble non vide et

$$+ : A \times A \longrightarrow A, \quad \cdot : A \times A \longrightarrow A$$

sont des lois (internes) sur A satisfaisant aux axiomes qui suivent.

1. $(A, +)$ est un groupe abélien. Le neutre est alors noté 0_A ou 0, et le symétrique d'un élément $a \in A$ est noté $-a$.
2. $(A, \cdot)$ est un monoïde, c'est-à-dire que la loi $\cdot$ est associative et possède un élément neutre, noté 1_A ou 1.
3. On a $\forall a, b, c \in A : a \cdot (b + c) = a \cdot b + a \cdot c$, et $(b + c) \cdot a = b \cdot a + c \cdot a$.

Dans ce chapitre on va étudier les **modules** sur un anneau. Cela permet
$\longrightarrow$ de généraliser des résultats d'algèbre linéaire (les modules sur les corps étant les espaces vectoriels),
$\longrightarrow$ d'obtenir des résultats structurels sur les anneaux (de la même manière, on obtient des résultats sur les groupes en les faisant opérer sur des ensembles).

Dans la suite A est un anneau.

A Définitions

Définition A.1. *Un A-**module** (à gauche) est un triplet $(M, +, .)$ où $(M, +)$ est un groupe abélien et $. : A \times M \longrightarrow M$ est une loi externe*

$$\begin{aligned} A \times M &\longrightarrow M \\ (a, x) &\longmapsto a.x \end{aligned}$$

vérifiant les axiomes suivants ($\forall a, b \in A$, $\forall x, y \in M$) :

1. $a.(x + y) = a.x + a.y$,
2. $(a + b).x = a.x + b.y$,
3. $(ab).x = a.(b.x)$,
4. $1.x = x$.

Exemples A.2.

1. A est un A-module, la loi externe étant la multiplication de A.
2. Pour $n \in \mathbb{N}^*$, A^n est un A-module, dont le groupe abélien sous-jacent est le groupe abélien produit A^n et la loi externe est donnée par
$$a.(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$$
3. Si A est un corps, un A-module est exactement un A-espace vectoriel.

4. $A = \mathbb{Z}$. Les $\mathbb{Z}$-modules sont exactement les groupes abéliens.
   En effet : Un $\mathbb{Z}$-module est en particulier un groupe abélien. Réciproquement si M est groupe abélien, on définit une loi externe
   $$\begin{aligned} \mathbb{Z} \times M &\longrightarrow M \\ (n, x) &\longmapsto n.x \end{aligned}$$
   de la manière suivante. Si $n \geq 0$, on pose $n.x = \underbrace{x + \ldots + x}_{n \text{ fois}}$ et si $n \leq 0$, on pose $n.x = -((-n).x)$. On vérifie que cela munit bien M d'une structure de $\mathbb{Z}$-module (exercice).
5. Si I est un ensemble et M est un A-module, notons M^I l'ensemble des applications $I \longrightarrow M$. Alors on vérifie que M^I est un A-module, pour les lois suivantes ($f, g \in M^I$, $a \in A$).
   – $(f + g)(x) := f(x) + g(x)$,
   – $(a.f)(x) := a.f(x)$.

La notion de module est donc une (vaste) généralisation des notions de groupe abélien et d'espace vectoriel. Un certain nombre de constructions et résultats sur les espaces vectoriels se généralisent sans problème aux modules, alors que d'autres résultats ne se généraliseront pas (comme par exemple l'existence d'une base).

Définition A.3. *Soient M et N des A-modules. Une **application A-linéaire de M vers N**, ou encore un **morphisme de A-modules de M vers N**, est une application $f : M \longrightarrow N$ telle que $\forall x, y \in M$, $\forall a \in A$, on a*

1. $f(x + y) = f(x) + f(y)$,
2. $f(a.x) = a.f(x)$.

*L'ensemble des applications A-linéaire de M vers N est noté $\mathrm{Hom}_A(M, N)$, avec de plus quand $M = N$, $\mathrm{Hom}_A(M, M) = \mathrm{End}_A(M)$. Un **isomorphisme de A-modules**, ou encore un **isomorphisme A-linéaire**, est une application A-linéaire bijective.*

On vérifiera que la composée de deux applications A-linéaires est encore une application A-linéaire, et que la bijection inverse d'un isomorphisme A-linéaire est encore A-linéaire.

Exemples A.4.
1. Soit $a \in A$. L'application $f_a : A \longrightarrow A$, $b \longmapsto ba$, est une application A-linéaire.
2. Soit $n \in \mathbb{N}^*$ et $i \in \{1, \ldots n\}$. La i-ème projection $p_i : A^n \longrightarrow A$ est une application A-linéaire.
3. Si M et N sont des $\mathbb{Z}$-modules, un morphisme de $\mathbb{Z}$-modules $M \longrightarrow N$ est exactement un morphisme de groupes (vérifier).

Proposition A.5. Soient M et N des A-modules.

1. L'ensemble $\mathrm{Hom}_A(M,N)$ est naturellement un groupe abélien avec pour $f,g \in \mathrm{Hom}_A(M,N)$,
$$(f+g)(x) := f(x)+g(x), \forall x \in M$$
2. Si de plus A est commutatif, alors $\mathrm{Hom}_A(M,N)$ est un A-module avec pour $a \in A$, $f \in \mathrm{Hom}_A(M,N)$,
$$(a.f)(x) := a.f(x), \forall x \in M$$
3. $\mathrm{End}_A(M)$ est un anneau, avec pour multiplication la composition des applications A-linéaires.

Preuve. Exercice. □

Le résultat suivant est une reformulation très utile de la définition de A-module. On pourra le comparer à la situation analogue de la formulation d'une opération d'un groupe G sur un ensemble X en termes d'un morphisme de groupes $G \to S_X$.

Proposition A.6. Soit $M = (M,+)$ un groupe abélien. Il est équivalent de se donner

1. une structure de A-module sur M,
2. un morphisme d'anneaux $\varphi : A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$.

Preuve. Supposons d'abord que M est un A-module, avec loi externe $A \times M \longrightarrow M$ $(a,x) \longmapsto a.x$. Soit alors l'application $l_a : M \longrightarrow M$, $l_a(x) = a.x$, qui est un morphisme de groupes. Ceci définit donc une application

$$\begin{aligned} \varphi : A &\longrightarrow \mathrm{End}_{\mathbb{Z}}(M) \\ a &\longmapsto l_a \end{aligned}$$

On vérifie que φ est un morphisme d'anneaux.

Réciproquement, si $\varphi : A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$ est un morphisme d'anneaux, on définit une loi externe sur M

$$\begin{aligned} A \times M &\longrightarrow M \\ (a,x) &\longmapsto a.x := \varphi(a)(x) \end{aligned}$$

et on vérifie que $(M,+,.)$ est bien un A-module. □

Le résultat suivant est très utile pour transporter une structure de module sur un anneau donné vers un autre anneau.

Proposition A.7. Soient A et B des anneaux et soit $f : A \longrightarrow B$ un morphisme d'anneaux ($f(1_A) = 1_B$ et $\forall a,b \in A$, $f(ab) = f(a)f(b)$). Soit M un B-module. Alors f induit une structure de A-module sur M, définie par : $\forall a \in A$, $\forall x \in M$, $a.x := f(a).x$.

Preuve. Exercice. □

Exemple A.8. Si $A \subset B$ est un sous-anneau, alors la multiplication de B induit par restriction une structure de A-module sur B.

B Sous-modules

Les concepts introduits dans ce paragraphe sont des adaptations directes du cas des espaces vectoriels.

Définition B.1. *Soit M un A-module. On dit qu'un sous-ensemble N de M est un* ***sous-A-module*** *de M (ou plus simplement un* ***sous-module*** *de M) si*

1. $0 \in N$,
2. $\forall x, y \in N$, *on a* $x + y \in N$,
3. $\forall a \in A, \forall x \in N$, *on a* $a.x \in N$.

Un sous-module est donc en particulier un sous-groupe.

Exemple B.2.

1. Soit M un A-module : $\{0\}$ et M sont des sous-modules de M.
2. Les sous-modules du A-module A sont exactement les idéaux à gauche de A.
3. Soit M un A-module et $x \in M$. Alors $Ax = \{a.x,\ a \in A\}$ est un sous-module de M (à vérifier).
4. Soit M un $\mathbb{Z}$-module. Les sous-modules de M sont exactement ses sous-groupes.
5. Si I est un ensemble et M est un A-module, notons $M^{(I)}$ l'ensemble des applications $I \longrightarrow M$ à support fini, c'est-à-dire les applications nulles en dehors d'un ensemble fini. Alors $M^{(I)}$ est un sous-module de M^I.

Un sous-A-module est un A-module, pour les lois induites.

Proposition B.3. Soient M et N des A-modules et $f : M \longrightarrow N$ une application A-linéaire.

1. Si $M' \subset M$ est un sous-module, alors $f(M')$ est un sous-module de N. En particulier $\mathrm{Im}(f) = f(M)$ est un sous-module de N.
2. Si $N' \subset N$ est un sous-module, alors $f^{-1}(N')$ est un sous-module de M. En particulier $\mathrm{Ker}(f) = f^{-1}(\{0\})$ est un sous module de M.

Preuve. Exercice. □

Exemple B.4. Soit $(a_1, \ldots, a_n) \in A^n$. Alors

$$M = \{(x_1, \ldots, x_n) \in A^n \mid x_1 a_1 + \cdots + x_n a_n = 0\}$$

est un sous-module de A^n. En effet l'application

$$\begin{aligned} f : A^n &\longrightarrow A \\ (x_1, \ldots, x_n) &\longmapsto x_1 a_1 + \cdots + x_n a_n \end{aligned}$$

est A-linéaire (vérifier), et $M = \mathrm{Ker}(f)$.

Définition-Proposition B.5. Soient I un ensemble et $(M_i)_{i\in I}$ une famille de A-modules. Alors les lois produit munissent $\prod_{i\in I} M_i$ d'une structure de A-module :

$$(x_i) + (y_i) = (x_i + y_i),\ a.(x_i) = (a.x_i)$$

Le A-module obtenu, noté encore $\prod_{i\in I} M_i$, est appelé le A-**module produit** des $(M_i)_{i\in I}$.

Preuve. Exercice. □

Exemple B.6. Si $M_i = M$ pour tout i, le A-module $\prod_i M_i$est l'ensemble des suites d'éléments de M indexées par I. Il s'identifie au A-module M^I déjà défini des applications $I \longrightarrow M$.

Définition-Proposition B.7. Soit $(M_i)_{i\in I}$ une famille de A-modules. On note

$$\bigoplus_{i\in I} M_i = \{(x_i) \in \prod_{\in I} M_i \mid \exists J \subset I \text{ fini tq } x_i = 0 \text{ pour } i \notin J\}$$

Alors $\bigoplus_{i\in I} M_i$ est un sous-module de $\prod_{i\in I} M_i$, appelé **somme directe des** $(M_i)_{i\in I}$.

Preuve. Exercice. □

Exemple B.8. Si $M_i = M$ pour tout i, le A-module $\oplus_{i\in I} M_i$ est l'ensemble des suites d'éléments de M indexées par I et à support fini. Il s'identifie au A-module $M^{(I)}$ des applications à support fini $I \longrightarrow M$.

Définition B.9. *Soient M un A-module et $(M_i)_{i\in I}$ une famille de sous-modules de M. On dira (abusivement) que M est **somme directe des** $(M_i)_{i\in I}$, et on notera $M = \bigoplus_{i\in I} M_i$, si l'application A-linéaire*

$$\begin{aligned} \bigoplus_{i\in I} M_i &\longrightarrow M \\ (x_i) &\longmapsto \sum_{i\in I} x_i \end{aligned}$$

est un isomorphisme.

On a la reformulation immédiate suivante, qui est souvent la plus utile.

Proposition B.10. Soient M un A-module et $(M_i)_{i\in I}$ une famille de sous-modules de M. Alors $M = \bigoplus_{i\in I} M_i$ si et seulement si tout élément $x \in M$ s'écrit $x = \sum_{i\in I} x_i$, pour un unique $(x_i) \in \bigoplus_{i\in I} M_i$.

Un résultat important pour les espaces vectoriels est l'existence de supplémentaires pour les sous-espaces vectoriels (conséquence du théorème de la base incomplète). Au niveau des modules, on a la caractérisation suivante pour les sous-modules qui admettent un supplémentaire.

Proposition B.11. Soient M un A-module et $M' \subset M$ est un sous-module. il existe un sous A-module $M'' \subset M$ tel que $M = M' \oplus M''$ (un supplémentaire) si et seulement si il existe une projection $p \in \mathrm{End}_A(M)$ (c'est-à-dire $p \circ p = p$) telle que $M' = p(M)$. Dans ce cas on a alors $M'' = \mathrm{Ker}(p)$.

Preuve. Si $M = M' \oplus M''$, il existe pour tout $x \in M$, des éléments uniques $x' \in M'$ et $x'' \in M''$ tels que $x = x' + x''$. Soit $p : M \longrightarrow M$ l'application définie par $p(x) = x'$. On voit facilement que p est A-linéaire, que p est une projection et que $\mathrm{Ker}(p) = M''$.

Réciproquement s'il existe une projection $p \in \mathrm{End}_A(M)$ telle que $M' = p(M)$, on prend $M'' = \mathrm{Ker}(p)$, et on vérifie que l'application A-linéaire $M' \oplus M'' \longrightarrow M$, $(x', x'') \longmapsto x' + x''$, est un isomorphisme (car $\forall x \in M$, on a $x = p(x) + (x - p(x))$.

L'exemple suivant montre alors que le résultat d'existence d'un supplémentaire pour un sous-espace vectoriel n'est plus vrai en général pour les modules.

Exemple B.12. Soit $n > 1$. Il n'existe de pas de sous-module M du $\mathbb{Z}$-module $\mathbb{Z}$ tel que $\mathbb{Z} = n\mathbb{Z} \oplus M$.

En effet : si un tel M existe, il existe une projection $p \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z})$ telle que $p(\mathbb{Z}) = n\mathbb{Z}$. Mais on a alors $n\mathbb{Z} = p(\mathbb{Z}) = p \circ p(\mathbb{Z}) = p(n\mathbb{Z}) = np(\mathbb{Z}) = n^2\mathbb{Z}$, ce qui implique $n = 0$ ou $n = \pm 1$. □

Le résultat suivant est lui aussi souvent utile.

Proposition B.13. Soient M un A-module et $M_1, \ldots, M_n$ une famille A-modules. Les assertions suivantes sont équivalentes.

1. $M \cong M_1 \oplus \cdots \oplus M_n$.
2. Il existe, pour tout $i \in \{1, \ldots, n\}$, des applications A-linéaires $u_i : M_i \longrightarrow M$ et $p_i : M \longrightarrow M_i$ telles que
$$p_i \circ u_j = \delta_{ij} \mathrm{id}_{M_i}, \quad \mathrm{id}_M = \sum_{i=1}^{n} u_i \circ p_i$$

Preuve. Notons pour tout i, $p_i : M_1 \oplus \cdots \oplus M_n \longrightarrow M_i$ la i-ème projection, et $u_i : M_i \longrightarrow M_1 \oplus \cdots \oplus M_n$ la i-ème injection. Ces applications A-linéaires vérifient

$$p_i \circ u_j = \delta_{ij} \mathrm{id}_{M_i}, \quad \mathrm{id}_{M_1 \oplus \ldots \oplus M_n} = \sum_{i=1}^{n} u_i \circ p_i$$

(1) $\Rightarrow$ (2). Soit $f : M \longrightarrow M_1 \oplus \cdots \oplus M_n$ un isomorphisme A-linéaire. Alors les applications A-linéaires $v_i = f^{-1} \circ u_i$ et $q_i = p_i \circ f$ vérifient les conditions demandées et on a le résultat.

(2) $\Rightarrow$ (1) Supposons qu'il existe des applications A-linéaires $v_i : M_i \longrightarrow M$ et $q_i : M \longrightarrow M_i$ telles que $q_i \circ v_j = \delta_{ij} \mathrm{id}_{M_i}$, $\mathrm{id}_M = \sum_{i=1}^{n} v_i \circ q_i$. On vérifie alors que l'application A-linéaire

$$\begin{aligned} \bigoplus_{i \in I} M_i &\longrightarrow M \\ (x_i) &\longmapsto \sum_{i \in I} v(x_i) \end{aligned}$$

est un isomorphisme. □

Définition-Proposition B.14. Soient M un A-module et $(M_i)_{i\in I}$ un famille de sous-modules de M. Alors

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

est un sous-module de M, appelé la somme des sous-modules $(M_i)_{i\in I}$.

Preuve. Exercice. □

Exemple B.15. Soient M un A-module et N et P des sous-modules de M. On a $M = N \oplus P \iff [M = N + P \text{ et } N \cap P = \{0\}]$.

Définition-Proposition B.16. Soient M un A-module et $(M_i)_{i\in I}$ un famille de sous-modules de M. Alors $\bigcap_{i\in I} M_i$ est un sous-module de M.
Si $S \subset M$, notons $A.S$ (ou AS) l'intersection de tous les sous-modules de M contenant S : c'est le plus petit sous-module de M contenant S, et on dit que AS est **le sous-module engendré par** S. On a

$$A.S = \sum_{x\in S} Ax$$

L'ensemble $A.S$ est **l'ensemble des combinaisons linéaires (à coefficients dans A) des éléments de** S. Si $M = A.S$, on dit S est une **partie génératrice de** M, ou encore **engendre** M. Un A**-module de type fini** est un A-module engendré par une partie finie.

Preuve. Exercice. □

Remarque. La définition s'applique aussi dans le cas où la partie S est vide, avec alors $A.S = \{0\}$.

Exemple B.17. Le A-module A^n est de type fini, engendré par la partie $\{e_1, \ldots, e_n\}$, où $e_i = (0, \ldots, 0 \underbrace{,1,}_{i-\text{eme place}} 0, \ldots, 0)$.

Exemple B.18. Soient M un A-module et $(M_i)_{i\in I}$ un famille de sous-modules de M. Alors le sous-module de M engendré par $\cup_{i\in I} M_i$ est $\sum_{i\in I} M_i$ (vérifier).

C Modules quotients

Rappel. Soient $M = (M, +)$ un groupe abélien et $N \subset M$ un sous-groupe. Considérons la relation $\mathcal{R}_N$ définie sur M par

$$x\mathcal{R}_N y \iff x - y \in N$$

La relation $\mathcal{R}_N$ est une relation d'équivalence, on note M/N l'ensemble des classes d'équivalences et $p : M \longrightarrow M/N$ la surjection canonique (on note aussi $p(x) = \overline{x}$, etc). Alors il

existe une unique structure de groupe (abélien) sur M/N telle que la surjection canonique soit un morphisme de groupes (de telle sorte que $\overline{x+y} = \overline{x} + \overline{y}$, le neutre est $\overline{0} = p(0)$).

Proposition C.1. Soient $M = (M, +)$ un A-module et $N \subset M$ un sous-module. Il existe sur M/N une unique structure de A-module telle que la surjection canonique $p : M \longrightarrow M/N$ soit A-linéaire.

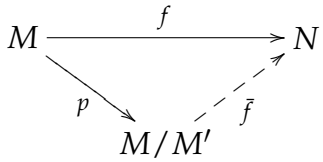
Preuve. Il reste à construire la loi externe $A \times M/N \longrightarrow M/N$. Soit $x, y \in M$ tels que $x - y \in N$. Alors $a.(x-y) \in N$ car N est un sous-module. Ainsi $a.x - a.y = a.x + a.(-y) = a.(x-y) \in N$. Ce calcul montre que l'on peut définir une application

$$\begin{aligned} A \times M/N &\longrightarrow M/N \\ (a, p(x)) &\longmapsto a.p(x) = p(a.x) \end{aligned}$$

On vérifie que muni de cette loi, le groupe abélien M/N est bien un A-module. La surjection canonique est A-linéaire par construction de la structure de A-module, et il est clair que cette propriété assure l'unicité de cette structure. □

Théorème C.2 (de factorisation et d'isomorphisme pour les A-modules)**.** Soient M et N des A-modules et $f : M \longrightarrow N$ une application A-linéaire.

1. Soit $M' \subset M$ un sous-module. Si $f(M') = 0$, alors il existe une unique application A-linéaire $\overline{f} : M/M' \longrightarrow N$ telle que $\overline{f} \circ p = f$ ($p : M \longrightarrow M/M'$ est la surjection canonique).



2. f induit un isomorphisme de A-modules $M/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$

Preuve. 1. Soient $x, y \in M$ tels que $x - y \in M'$. Alors $f(x-y) = 0$, d'où $f(x) = f(y)$. Ce calcul montre que l'on peut définir une application $\overline{f} : M/M' \longrightarrow N$, $\overline{f}(p(x)) = f(x)$. On vérifie que $\overline{f}$ est A-linéaire, et par construction $\overline{f} \circ p = f$. L'unicité provient de la surjectivité de p.

2. On applique la constuction précedente à $M' = \mathrm{Ker}(f)$ pour obtenir une application A-linéaire $\overline{f} : M/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f)$. Le théorème d'isomorphisme pour les groupes assure que f est un isomorphisme de groupes, et est donc un isomorphisme A-linéaire. □

Exemple C.3. Soit $(a_1, \ldots, a_n) \in A^n$ et soit $M = \{(x_1, \ldots, x_n) \in A^n \mid x_1a_1 + \cdots + x_na_n = 0\}$: c'est un sous-module de A^n. Alors les A-modules A^n/M et $Aa_1 + \cdots + Aa_n$ sont isomorphes.

En effet : L'application

$$\begin{aligned} f : A^n &\longrightarrow A \\ (x_1, \ldots, x_n) &\longmapsto x_1a_1 + \cdots + x_na_n \end{aligned}$$

est A-linéaire, avec $\mathrm{Ker}(f) = M$ et $\mathrm{Im}(f) = Aa_1 + \cdots + Aa_n$: le théorème d'isomorphisme donne le résultat.

II Modules libres

Dans ce chapitre on étudie une classe importante de modules : les modules libres, qui sont les modules admettant une base. On verra que si l'anneau de base n'est pas corps, il n'existe pas nécessairement une base.

Dans la suite A est un anneau non nul.

A Définition et exemples

Définition A.1. *Soit M un A-module et $(x_i)_{i\in I} \in M^I$ une famille d'éléments de M.*

1. *On dit que la partie $\{x_i\}_{i\in I}$ **engendre** M, ou est **une partie génératrice de** M, lorsque M est engendré par la partie $\{x_i\}_{i\in I}$, c'est-à-dire lorsque $M = \sum_{i\in I} Ax_i$.*
2. *On dit que la partie $\{x_i\}_{i\in I}$ est **libre**, ou encore **linéairement indépendante**, lorsque*

$$\forall (a_i)_{i\in I} \in A^{(I)},\ \sum_{i\in I} a_i x_i = 0 \Longrightarrow a_i = 0,\ \forall i \in I$$

3. *On dit que la partie $\{x_i\}_{i\in I}$ est une **base de** M si elle est libre et génératrice.*

Ainsi, **la partie $\{x_i\}_{i\in I}$ est une base de M si tout élément de M s'écrit de manière *unique* sous la forme $\sum_{i\in I} a_i x_i$ pour $(a_i) \in A^{(I)}$.**

Remarque : on peut formuler les définitions précédentes pour la famille $(x_i)_{i\in I}$ de M, on parle alors de famille libre, famille génératrice.

Définition A.2. *On dit qu'un A-module est **libre** s'il possède une base.*

Par convention on dira que le module nul est libre (avec $\emptyset$ pour base).

Exemple A.3.

1. Pour $n \in \mathbb{N}^*$, le A-module A^n est libre, et la partie $\{e_1, \dots, e_n\}$, où $e_i = (0, \dots, 0, \underbrace{1}_{\text{place } i}, 0, \dots, 0)$, est une base de A^n (la base canonique). On fait de plus la convention $A^0 = \{0\}$, c'est bien un module libre.
2. Soit I un ensemble. Le A-module $A^{(I)}$ des fonctions à support fini $I \longrightarrow A$ est libre. Pour $i \in I$, notons e_i la fonction caractéristique du singleton $\{i\}$. Alors $\{e_i\}_{i\in I}$ est une base de $A^{(I)}$.

   Preuve. Si $f \in A^{(I)}$, Soit $J \subset I$ le support de $f : J = \{i \in I \mid f(i) \neq 0\}$. On vérifie alors que $f = \sum_{i\in J} f(i)e_i$, ce qui montre que la partie $\{e_i\}_{i\in I}$ engendre $A^{(I)}$. Soit $(a_i)_{i\in I} \in A^{(I)}$ tel que $\sum_{i\in I} a_i e_i = 0$. Alors pour tout $i_0 \in I$, on a $0 = \sum_{i\in I} a_i e_i(i_0) = a_{i_0}$. Ceci montre que la partie $\{e_i\}_{i\in I}$ est libre. □

Le théorème qui suit est une propriété cruciale des modules libres.

Théorème A.4. Soit M un A-module libre de base $\{e_i\}_{i\in I}$. Soit N un A-module et x_i, $i \in I$, des éléments de N. Alors il existe une unique application A-linéaire $f : M \longrightarrow N$ telle que $\forall i \in I$, on a $f(e_i) = x_i$.

Preuve. Pour montrer l'unicité, supposons qu'il existe une telle application f. Soit $x \in M$: on a $x = \sum_{i\in I} a_i.e_i$ pour $(a_i) \in A^{(I)}$. Alors par linéarité de f on a $f(x) = \sum_{i\in I} a_i.f(e_i) = \sum_{i\in I} a_i.x_i$, et cela montre l'unicité.

On construit alors f de la manière suivante. Soit $x \in M$: x s'écrit de manière *unique* sous la forme $x = \sum_{i\in I} a_i.e_i$ pour $(a_i) \in A^{(I)}$. On pose alors $f(x) = \sum_{i\in I} a_i.x_i$. Ceci définit une application $f : M \longrightarrow N$ telle que $\forall \in I$, $f(e_i) = x_i$, et on vérifie sans problème que f est linéaire. □

Corollaire A.5. Si M est un A-module libre, il existe un ensemble I tel que les A-modules $A^{(I)}$ et M soient isomorphes.

Preuve. Soit $\{x_i\}_{i\in I}$ une base de M. On considère le A-module libre $A^{(I)}$, de base $\{e_i\}_{i\in I}$. Il existe, par le théorème précédent, des applications A-linéaires $f : A^{(I)} \longrightarrow M$ et $g : M \longrightarrow A^{(I)}$ telles que $\forall i \in I$, $f(e_i) = x_i$ et $g(x_i) = e_i$. Alors $\forall i \in I$, $g \circ f(e_i) = e_i$ et puisque $\{e_i\}_{i\in I}$ est une base de $A^{(I)}$, la linéarité de $g \circ f$ assure que $g \circ f = \mathrm{id}_{A^{(I)}}$. De même on voit que $f \circ g = \mathrm{id}_M$, et on a bien l'isomorphisme annoncé. □

Corollaire A.6. Tout A-module est quotient d'un module libre.

Preuve. Soit $\{x_i\}_{i\in I}$ une partie génératrice de M et soit $f : A^{(I)} \longrightarrow M$ l'unique application A-linéaire telle que $\forall i \in I$, $f(e_i) = x_i$. On a donc $x_i \in \mathrm{Im}(f)$, $\forall i \in I$, et $\sum_{i\in I} Ax_i = M \subset \mathrm{Im}(f)$, et ainsi f est surjective. Le théorème d'isomorphisme permet de conclure. □

Corollaire A.7. Soient M et N des A-modules et $f : M \longrightarrow N$ une application A-linéaire surjective. Si N est libre, il existe une application A-linéaire $s : N \longrightarrow M$ telle que $f \circ s = \mathrm{id}_N$.

Preuve. Soit $\{e_i\}_{i\in I}$ une base de N. Comme f est surjective, il existe, pour tout $i \in I$, $x_i \in M$ tel que $f(x_i) = e_i$. Soit $s : N \longrightarrow M$ l'unique application A-linéaire telle $\forall i \in I$, $s(e_i) = x_i$. On a alors $f \circ s(e_i) = e_i$, $\forall i \in I$, et donc $f \circ s = \mathrm{id}_N$ par linéarité (et le fait que $\{e_i\}_{i\in I}$ est une base de N). □

Corollaire A.8. Si A est un anneau intègre qui n'est pas un corps (par exemple $A = \mathbb{Z}$), alors il existe des A-modules non libres.

Preuve. L'anneau A est intègre et n'est pas un corps, il existe donc un élément $a \in A$ non nul tel que $I = Aa \subsetneq A$ et A/I est non nul. Supposons que le A-module A/I est libre. Soit $p : A \longrightarrow A/I$ la surjection canonique. Il existe, d'après le corollaire précédent, une application A-linéaire $s : A/I \longrightarrow A$ telle que $p \circ s = \mathrm{id}_{A/I}$. Comme $a \in I$, on a, en utilisant la linéarité de s, $0 = s(p(a)) = s(a.p(1)) = as(p(1))$. L'anneau A est intègre et $a \neq 0$, donc $s(p(1)) = 0$. Mais alors $p(1) = p \circ s(p(1)) = 0$, ce qui implique $1 \in I$ et $I = A$: on aboutit à une contradiction. □

B Le théorème de la base incomplète

On vient donc de voir qu'en toute généralité, il existe des modules non libres si A n'est pas un corps.

Théorème B.1 (de la base incomplète)**.** Supposons que A est un corps. Soient M un A-module, S une partie libre de M et X une partie génératrice de M. Alors il existe une base $\mathcal{B}$ de M telle que $S \subset \mathcal{B} \subset X$.

Preuve. Soit I l'ensemble des parties libres E de M telles que $S \subset E \subset X$: I est non vide car $S \in I$. On munit I de l'ordre induit par l'inclusion des parties de M. On voit facilement que I est ordonné *inductif* (toute partie non vide totalement ordonnée admet un majorant). On peut donc utiliser le lemme de Zorn : I possède un élément maximal, que l'on note $\mathcal{B}$. Montrons que $\mathcal{B}$ est une base de M : on sait déjà que c'est une partie libre, il reste à voir que c'est une partie génératrice de M. Tout élément de M est combinaison linéaire d'éléments de X, il suffit donc de voir que tout élément de X est combinaison linéaire d'éléments de $\mathcal{B}$. Soit $x \in X \setminus \mathcal{B}$. Alors la partie $\mathcal{B} \cup \{x\}$ n'est pas libre par maximalité de $\mathcal{B}$. Il existe donc $e_1, \ldots, e_n \in \mathcal{B}$, $a_1, \ldots, a_n \in A$ et $b \in B$ tels que $a_1.e_1 + \cdots + a_n.e_n + b.x = 0$, avec $b \neq 0$ (car $\mathcal{B}$ est libre). Alors $b.x = -\sum_{i=1}^n a_i.e_i = \sum_{i=1}^n (-a_i).e_i$. Comme A est un corps, $b \neq 0$ est inversible et on a

$$x = 1.x = (b^{-1}b).x = b^{-1}.(b.x) = b^{-1}.(\sum_{i=1}^n (-a_i).e_i) = \sum_{i=1}^n (-b^{-1}a_i).e_i$$

ce qui montre que x est combinaison linéaire d'éléments de $\mathcal{B}$. □

Corollaire B.2. Si A est un corps, tout A-espace vectoriel (A-module) possède une base.

Preuve. Soit M un A-espace vectoriel. Si M est nul il n'y a rien à montrer, sinon on prend $x \in M$, $x \neq 0$. La partie $\{x\}$ est libre car A est un corps, et on peut appliquer le théorème de la base incomplète (en prenant par exemple $X = M$ comme partie génératrice). □

C Rang d'un module libre

On se propose de démontrer le résultat suivant.

Théorème C.1. Soient A un anneau commutatif non nul et M un A-module libre. Toutes les bases de M ont le même cardinal.

On verra plus loin que le théorème n'est pas vrai si A n'est pas supposé commutatif. On va commencer par établir le résultat dans le cas où le module libre admet une base ayant un nombre fini d'éléments. On aura besoin de la notion suivante.

Définition C.2. *Soient $M_1, \ldots, M_n, V$ des A-modules. Une application $f : M_1 \times \cdots \times M_n \longrightarrow V$ est dite* ***n-linéaire*** *si pour chaque i et des éléments fixés $x_j \in M_j$, $j \neq i$, l'application*

$$M_i \longrightarrow V,\ x \longmapsto f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots x_n)$$

est A-linéaire. Quand $M_i = M$, $\forall i$ et $V = A$, on dit que $f : M^n \longrightarrow A$ est une ***forme n-linéaire sur*** *M.*

On dit qu'une forme n-linéaire $f : M^n \longrightarrow A$ est ***alternée*** *si pour tout $(x_1, \ldots, x_n) \in M^n$, alors $x_i = x_j$ avec $i \neq j$ entraine $f(x_1, \ldots, x_n) = 0$.*

Proposition C.3. Soit A un anneau commutatif (non nul) et soit M un A-module.

1. Si $f : M^n \longrightarrow A$ est une forme n-linéaire alternée, on a pour tout $\sigma \in S_n$ et tout $(x_1, \ldots, x_n) \in M^n$,
$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \varepsilon(\sigma) f(x_1, \ldots, x_n)$$
2. Si M admet une partie génératrice ayant $p < n$ éléments, alors toute forme n-linéaire alternée sur M est nulle.
3. Si M est un A-module libre ayant une base $\{e_1, \ldots, e_n\}$ à n éléments, il existe une unique forme n-linéaire alternée $\Delta : M^n \longrightarrow A$ telle que $\Delta(e_1, \ldots, e_n) = 1$

Preuve. 1. Supposons dans un premier temps que σ est une transposition : $\sigma = (i, j)$ avec $i < j$. Alors

$$f(x_1, \ldots, x_i + x_j, \ldots, x_j + x_i, \ldots, x_n) = 0$$
$$\Rightarrow f(x_1, \ldots, x_i, \ldots, x_i, \ldots, x_n) + f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) +$$
$$f(x_1, \ldots, x_j, \ldots, x_j, \ldots, x_n) + f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = 0$$
$$\Rightarrow f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = -f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = \varepsilon(\sigma) f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n)$$

Pour traiter le cas général, on remarque que l'on a une application

$$M^n \times S_n \longrightarrow M^n$$
$$((x_1, \ldots, x_n), \sigma) \longmapsto (x_1, \ldots, x_n).\sigma = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

qui vérifie $(x_1, \ldots, x_n).(\sigma\tau) = ((x_1, \ldots, x_n).\sigma).\tau, \forall \sigma, \tau \in S_n$ et $(x_1, \ldots, x_n).1 = (x_1, \ldots, x_n)$. Le groupe S_n est engendré par les transpositions et la signature est un morphisme de groupes, le résultat se montre donc sans difficulté par récurrence sur le nombre de transpositions dont la permutation σ est un produit, à partir de la première étape.

2. Supposons que $\{e_1, \ldots, e_p\}$ est une partie génératrice de M. Pour $(x_1, \ldots, x_n) \in M^n$, on écrit pour chaque i, $x_i = \sum_{j=1}^{p} a_{ji} e_j$. On a donc,

$$f(x_1, \ldots, x_n) = \sum_{j_1, \ldots, j_n} a_{j_1 1} \cdots a_{j_n n} f(e_{j_1}, \ldots, e_{j_n}) = 0$$

car f est n-linéaire et alternée et $p < n$.

3. Supposons que $\{e_1, \ldots, e_n\}$ est une partie génératrice de M. Pour $(x_1, \ldots, x_n) \in M^n$, on a, en reprenant les notations précédentes

$$f(x_1, \ldots, x_n) = \sum_{j_1, \ldots, j_n} a_{j_1 1} \cdots a_{j_n n} f(e_{j_1}, \ldots, e_{j_n})$$
$$= \sum_{\sigma \in S_n} a_{\sigma(1)1} \cdots a_{\sigma(n)n} f(e_{\sigma(1)}, \ldots, e_{\sigma(n)}) = \left(\sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n} \right) f(e_1, \ldots, e_n)$$

Il existe donc au plus une forme n-lineaire alternée $f : M^n \longrightarrow A$ telle que $f(e_1, \ldots, e_n) = 1$. Si maintenant $\{e_1, \ldots, e_n\}$ est une base de M, on définit une application

$$\Delta : M^n \longrightarrow A$$

en posant

$$\Delta(x_1,\dots,x_n)=\sum_{\sigma\in S_n}\varepsilon(\sigma)a_{\sigma(1)1}\cdots a_{\sigma(n)n}$$

où comme précedemment, on a, pour chaque i, $x_i=\sum_{j=1}^{p}a_{ji}e_j$. Il est clair que $\Delta(e_1,\dots,e_n)=1$ et on vérifie sans difficulté que Δ est n-linéaire. Soit $(x_1,\dots,x_n)\in M^n$ avec $x_i=x_j$ pour $i<j$. On a

$$\begin{aligned}\Delta(x_1,\dots,x_n)&=\sum_{\sigma\in S_n}\varepsilon(\sigma)a_{\sigma(1)1}\cdots a_{\sigma(n)n}\\&=\sum_{\sigma\in A_n}\varepsilon(\sigma)a_{\sigma(1)1}\cdots a_{\sigma(n)n}+\sum_{\sigma\in A_n(i,j)}\varepsilon(\sigma)a_{\sigma(1)1}\cdots a_{\sigma(n)n}\\&=\sum_{\sigma\in A_n}\varepsilon(\sigma)a_{\sigma(1)1}\cdots a_{\sigma(n)n}+\sum_{\sigma\in A_n}\varepsilon(\sigma(i,j))a_{\sigma(1)1}\cdots a_{\sigma(j)i}\cdots a_{\sigma(i)j}\cdots a_{\sigma(n)n}\\&=\sum_{\sigma\in A_n}\varepsilon(\sigma)a_{\sigma(1)1}\cdots a_{\sigma(n)n}+\sum_{\sigma\in A_n}-\varepsilon(\sigma)a_{\sigma(1)1}a_{\sigma(j)j}\cdots a_{\sigma(i)i}\cdots a_{\sigma(n)n}\\&=0\end{aligned}$$

Ceci montre que Δ est alternée. □

Preuve du théorème C.1. Etape 1. Supposons que M admet une base finie, et soit $(e_i)_{i\in I}$ une telle base. Soit $(f_j)_{j\in J}$ une autre base de M. Montrons que J est fini.

Pour tout $i\in I$, il existe un élément $(a_{ij})_{j\in J}\in A^{(J)}$ tel que

$$e_i=\sum_{j\in J}a_{ij}f_j$$

Notons $S_i\subset J$ le support (fini) de $(a_{ij})_{j\in J}$: $S_i=\{j\in J\mid a_{ij}\neq 0\}$. Soit $J'=\cup_{i\in I}S_i\subset J$. Soit M' le sous-module de M engendré par les f_j, $j\in J'$. Comme $\forall i\in I$, on a $e_i\in M'$, on a donc $M'=M$ et $J=J'$ (par l'indépendance linéaire des f_j) et donc J est fini.

Si $n=\mathrm{Card}(I)$ et $p=\mathrm{Card}(J)$ avec , il existe par la proposition précédente une forme n-linéaire alternée non nulle et on a nécessairement $p\geq n$, et l'argument symétrique montre que $p=n$.

Etape 2. Soient $(e_i)_{i\in I}$ et $(f_j)_{j\in J}$ deux bases de M. On peut supposer que I et J sont infinis. Montrons d'abord que $\mathrm{Card}(I)\leq\mathrm{Card}(J\times\mathbb{N})$. Pour tout $j\in J$, soit $(a_{ij})_{i\in I}\in A^{(I)}$ tels que $f_j=\sum_{i\in I}a_{ij}e_i$, et notons $S_j\subset I$ le support (fini) de $(a_{ij})_{i\in I}$: $S_j=\{i\in I\mid a_{ij}\neq 0\}$. Soit $I'=\cup_{j\in J}S_j$. Tous les f_j appartiennent à M', le sous module de M engendré par les e_i, $i\in I'$, donc $M'=M$. On a donc $I'=I$ (car pour $i\in I$, e_i est combinaison linéaire d'éléments $e_{i'}$, $i'\in I$, et par l'indépendance linéaire on a $i\in I'$) et ainsi

$$\mathrm{Card}(I)=\mathrm{Card}(I')=\mathrm{Card}(\cup_{j\in J}S_j)\leq\mathrm{Card}(J\times\mathbb{N})$$

L'inégalité de droite s'obtient en utilisant le lemme suivant.

Lemme C.4. Soit E un ensemble et $(E_j)_{j\in J}$ des parties de E. Alors $\mathrm{Card}(\cup_{j\in J}E_j)\leq\mathrm{Card}(J\times E)$. En particulier si les E_j sont finis, on a $\mathrm{Card}(\cup_{j\in J}E_j)\leq\mathrm{Card}(J\times\mathbb{N})$.

Preuve du lemme. Pour chaque $x\in\cup_{j\in J}E_j$, on choisit un élément $\tau(x)\in J$ tel que $x\in E_{\tau(x)}$. On construit ainsi une injection $(\cup_{j\in J}E_j)\hookrightarrow(J\times E)$ en associant à $x\in\cup_{j\in J}E_j$ le couple $(\tau(x),x)$. Si les E_j sont finis, on fixe pour tout j une injection $\nu_j:E_j\hookrightarrow\mathbb{N}$, et on obtient une application injective $\cup_{j\in J}E_j\hookrightarrow J\times\mathbb{N}$, $x\mapsto(\tau(x),\nu_{\tau(x)}(x))$. □

Comme J est infini, on a $\mathrm{Card}(J\times\mathbb{N})=\mathrm{Card}(J)$ (propriété vraie pour tout ensemble infini, admise si elle n'est pas déjà connue), et donc $\mathrm{Card}(I)\leq\mathrm{Card}(J)$. En échangeant les rôles de I et J, on obtient $\mathrm{Card}(J)\leq\mathrm{Card}(I)$ et le théorème de Cantor-Bernstein permet de conclure que $\mathrm{Card}(I)=\mathrm{Card}(J)$. □

Définition C.5. *Soit A un anneau commutatif non nul. Le cardinal d'une base d'un A-module libre est appelé le **rang** (ou **dimension** si A est un corps) du module.*

Exemple C.6. 1. Le A-module libre A^n est libre de rang n.

2. Si M et N sont des A-modules libres de rang respectifs m et n, alors $M \oplus N$ est libre de rang $m+n$.

Remarque. Si A est un corps non commutatif, il est également vrai que toutes les bases d'un A-module (A-espace vectoriel) ont même cardinal. Par contre le résultat n'est plus vrai si A n'est pas un corps, comme le montre l'exemple suivant.

Exemple C.7. Soit K un corps commutatif. Soit V un K-espace vectoriel ayant une base $(e_n)_{n\in\mathbb{N}}$ (par exemple $V = K^{(\mathbb{N})}$). Considérons l'anneau $A = \mathrm{End}_K(V)$ des endomorphismes K-linéaires de V. Alors A possède une base ayant un élément, ainsi qu'une base ayant deux éléments.

En effet : A est bien sûr un A-module libre avec une base à un élément ($1_A = \mathrm{id}_V$). Considérons maintenant les éléments u, v de $A = \mathrm{End}_K(V)$ définis par

$$u(e_i) = e_{2i},\ v(e_i) = e_{2i+1},\ \forall i \in \mathbb{N}$$

ainsi que les les éléments u', v' de A définis par

$$u'(e_i) = \begin{cases} e_{\frac{i}{2}} & \text{si } i \text{ est pair} \\ 0 & \text{si } i \text{ impair} \end{cases} \qquad v'(e_i) = \begin{cases} e_{\frac{i-1}{2}} & \text{si } i \text{ est impair} \\ 0 & \text{si } i \text{ est pair} \end{cases}$$

On vérifie alors que $u' \circ u = \mathrm{id}_V = v' \circ v = u \circ u' + v \circ v'$, et $u' \circ v = 0 = v' \circ u$. Montrons que (u', v') est une base du A-module A. Si $f \in A$, on a $f = f \circ \mathrm{id}_V = (f \circ u) \circ u' + (f \circ v) \circ v'$, ce qui montre que (u', v') engendre A. Si $f, g \in A$ vérifient $f \circ u' + g \circ v' = 0$, alors $f \circ u' \circ u = 0 = f$ et $g \circ v' \circ v = 0 = g$ (par les identités précédentes), donc (u', v') est une famille libre, et est donc une base du A-module A. □

On termine la section en mentionnant la non-généralisation d'autres résultats classiques sur les espaces vectoriels aux modules arbitraires.

Remarques.

1. Un sous-module d'un module libre n'est pas nécessairement libre.
2. Un sous-module d'un module de type fini n'est pas nécessairement de type fini.

En effet : 1. Considérons $A = \mathbb{Z}/n^2\mathbb{Z}$, $n \geq 2$. Pour $k \in \mathbb{Z}$, notons $\overline{k}$ sa classe dans A. Soit $M = \{\overline{kn},\ k \in \mathbb{Z}\} = \{\overline{0}, \overline{n}, \ldots, \overline{(n-1)n}\}$. C'est un idéal de A, c'est-à-dire un sous-module de A. Montrons qu'aucun élément de M n'est libre, ce qui montrera que M ne possède pas de base et donc n'est pas libre. Soit $x \in M : x = \overline{kn}$. Alors on a $\overline{n}.\overline{x} = \overline{nx} = \overline{n^2k} = \overline{0}$, avec $\overline{n} \neq 0$, ce qui montre que x n'est pas libre.

2. Soit K un corps et $A = K^{\mathbb{N}}$. Alors $M = A$ est un A-module de type fini, mais $K^{(\mathbb{N})}$ n'est pas un sous-module de type fini de A. Sinon, il existerait $f_1, \ldots, f_m \in K^{(\mathbb{N})}$ tels que $K^{(\mathbb{N})} = Af_1 + \cdots + Af_m$. Soit $J = \{k \in \mathrm{N},\ \exists i \in \{1, \ldots, m\} \text{ tq } f_i(k) \neq 0\}$. Alors J est fini car $f_1, \ldots f_m \in A^{(I)}$, et pour tout élément $f \in Af_1 + \cdots + Af_m$, on a $f(k) = 0$ pour $k \notin J$. Puisque J est fini, il existe donc f qui n'appartient pas à $Af_1 + \cdots + Af_m$, ce qui donne une contradiction. □

D Module de torsion

Pour un module M, on introduit un sous-ensemble (un sous-module si A est intègre et commutatif) qui permet à l'occasion de montrer qu'un module n'est pas libre.

Définition-Proposition D.1. Soit M un A-module. Le sous-ensemble de **torsion** de M est défini par

$$T(M) := \{x \in M \mid \exists a \in A \setminus \{0\} \text{ tq } a.x = 0\}$$

Si A est intègre et commutatif, alors $T(M)$ est un sous-module de M.

Preuve. Il est clair que $0 \in M$. Soient $x, y \in T(M)$: il existe $a, b \in A \setminus \{0\}$ tels que $a.x = 0 = b.y$. Alors $ab.(x+y) = 0$ car A commutatif, avec $ab \neq 0$ car A intègre. De plus $\forall c \in A$, on a $a.(c.x) = c.(a.x) = 0$, d'où $c.x \in T(M)$. □

Proposition D.2. Si A est un anneau intègre et M est un A-module libre, alors $T(M) = (0)$.

Preuve. Soit $\{e_i\}_{i\in I}$ une base de M et $x \in M : x = \sum_{i\in I} a_i.e_i$ pour $(a_i)_{i\in I} \in A^{(I)}$. Si $x \in T(M)$, soit $a \in A \setminus \{0\}$ tel que $a.x = 0$. Alors $\sum_{i\in I}(aa_i).e_i = 0$, donc $aa_i = 0$, pour tout i. L'anneau A est intègre, donc $a_i = 0$, $\forall i$, et $x = 0$. □

Exemple D.3.

1. Si M est un groupe abélien ($\mathbb{Z}$-module) fini, alors $T(M) = M$.
2. Si $M = A/I$ ($I \neq (0)$ idéal de A), alors $T(A/I) = A/I$ (ce qui redémontre que A/I n'est pas un module libre si A est intègre et commutatif).
3. Si $M = N \oplus P$, alors $T(M) = T(N) \oplus T(P)$.
4. On a $T(\mathbb{Q}) = (0)$, mais $\mathbb{Q}$ n'est pas un $\mathbb{Z}$-module libre.

On verra plus loin que si A est un anneau principal et si M est un A-module de type fini, alors M est libre si et seulement si $T(M) = (0)$.

III Algèbres

Dans ce chapitre A est un anneau commutatif.

A Definitions

Définition A.1. *Une A-**algèbre** est un anneau R qui est un A-module, les loi $+$ de R en tant que qu'anneau et en tant que A-module étant les mêmes, tel que $\forall a \in A, \forall x, y \in R$, on a*

$$(a.x)y = x(a.y) = a.(xy)$$

Exemple A.2.
1. Les $\mathbb{Z}$-algèbres sont exactement les anneaux.
2. Soit R un anneau et soit
$$Z(R) = \{x \in R \mid yx = xy, \forall y \in R\}$$
le centre de R (c'est un sous-anneau de R). Alors R est une $Z(R)$-algèbre, la structure de $Z(R)$-module étant induite par la multiplication de R. Plus généralement si A est un sous-anneau de $Z(R)$, alors R est une A-algèbre (vérifier). Encore plus généralement, tout morphisme d'anneaux $A \longrightarrow Z(R)$ induit une structure de A-algèbre sur A.
3. $M_n(A)$, l'ensemble des matrices $n \times n$ à coefficients dans A, est un A-module et un anneau, et est une A-algèbre (cet exemple sera étudié beaucoup plus en détail dans le chapitre suivant).
4. Si I est un ensemble, le A-module A^I est une A-algèbre, le produit étant donné par le produit ponctuel des fonctions (vérifier).
5. Si M est un A-module, alors $\mathrm{End}_A(M)$ est une A-algèbre.

Pour construire des exemples d'algèbres, il est souvent utile de reformuler la définition. Pour cela on utilisera le concept suivant.

Définition A.3. *Soient M, N, P des A-modules et $f : M \times N \to P$ une application. On dit que f est une application A-bilinéaire si c'est une application 2-linéaire, c'est-à-dire si f est A-linéaire en chaque variable :*

1. *$f(a.x+y,z) = a.f(x,z) + f(y,z)$, $\forall a \in A, \forall x, y \in M, \forall z \in N$;*
2. *$f(x, a.y+z) = a.f(x,y) + f(x,z)$, $\forall a \in A, \forall x \in M, \forall y, z \in N$.*

Définition A.4 (Algèbres, bis)**.** *Une A-**algèbre** est un A-module R muni d'une application A-bilinéaire*

$$\begin{aligned} R \times R &\longrightarrow R \\ (x, y) &\longmapsto xy \end{aligned}$$

telle que $\forall x, y, z \in R$, on a $(xy)z = x(yz)$ et il existe $1 \in R$ tel que $x1 = 1x = x$, $\forall x \in R$.

On vérifiera avec soin l'équivalence des deux définitions (si R est une algèbre au sens de la première définition, alors l'application bilinéaire de la deuxième définition est le produit de l'anneau, et réciproquement).

Les lemmes suivants seront très utiles pour construire des algèbres en utilisant la deuxième définition.

Lemme A.5. Soient M, N, P des A-modules. Supposons que M et N sont libres de bases respectives $\{e_i\}_{i\in I}$ et $\{e'_j\}_{j\in J}$. Soit $\{x_{ij}\}_{i\in I, j\in J}$ une famille d'éléments de P. Alors il existe une unique application A-bilinéaire $f : M \times N \to P$ telle que $f(e_i, e'_j) = x_{ij}$, $\forall i \in I, \forall j \in J$.

Preuve. Exercice. □

Lemme A.6. Soit R un A-module engendré par une famille $\{e_i\}_{i\in I}$. Soit $m : R \times R \longrightarrow R$, $(x, y) \longmapsto x \cdot y$ une application A-bilinéaire telle que

1. $e_i \cdot (e_j \cdot e_k) = (e_i \cdot e_j) \cdot e_k$, $\forall i, j, k \in I$
2. il existe $e \in R$ tel que $e_i \cdot e = e_i = e \cdot e_i$, $\forall i \in I$.

Alors m munit R d'une structure de A-algèbre (l'unité de l'anneau R est e).

Preuve. Il suffit de vérifier que $\forall x, y, z \in R$, on a $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ et $x \cdot e = e \cdot x = x$. Cela se fait sans difficulté à partir de la bilinéarité de m et des hypothèses. □

Exemple A.7. Soit I est un ensemble fini, et considérons l'unique application bilinéaire $A^I \times A^I \longrightarrow A^I$, $(e_i, e_j) \longmapsto \delta_{ij} e_i$. Elle munit le A-module libre A^I ($= A^{(I)}$ car I est fini) d'une structure de A-algèbre. Le produit correspond en fait au produit ponctuel des fonctions.

Définition A.8. *Si R et S sont des R-algèbres, un **morphisme de A-algèbres** $f : R \longrightarrow S$ est une application A-linéaire qui est aussi un morphisme d'anneaux.*

On vérifiera que la composée de deux morphismes de A-algèbres est encore un morphisme de A-algèbres. Bien sûr un isomorphisme de A-algèbres est un morphisme de A-algèbres bijectif, et on vérifiera que la bijection inverse d'un isomorphisme de A-algèbres est encore un isomorphisme de A-algèbres.

Plus généralement, les définitions, constructions et résultats sur les modules et anneaux ont des analogues évidents. Nous ne les énoncerons pas, mais citons tout de même les faits suivants.

$\rightsquigarrow$ **Sous-algèbres.** Une sous-algèbre est un sous-anneau qui est un sous-module.

$\rightsquigarrow$ **Idéaux dans une algèbre.** Si R est une A-algèbre et I est un idéal de R, alors I est automatiquement un sous A-module (vérifier), et on peut former la A-algèbre quotient R/I.

$\rightsquigarrow$ **Noyau d'un morphisme d'algèbres.** Le noyau d'un morphisme d'algèbres est un idéal, et on a un théorème d'isomorphisme pour les algèbres.

$\rightsquigarrow$ **Modules sur une algèbre.** Si R est une A-algèbre et M est un R-module, alors M est automatiquement un A-module. Plus généralement on a

Proposition A.9. Soit R une A-algèbre et soit M un A-module. Il est équivalent de se donner

1. une structure de R-module sur M,
2. un morphisme de A-algèbres $\varphi : R \longrightarrow \mathrm{End}_A(M)$.

La démonstration est laissée en exercice.

La structure de A-module d'un module sur une A-algèbre R peut s'avérer extrèmement utile pour l'étude des R-modules. Par exemple, si $A = k$ est un corps et si R est une k-algèbre de dimension finie (i.e. est de dimension finie comme k-espace vectoriel), alors si M est un R-module avec $0 < \dim_k(M) < \dim_k(R)$, on voit que M n'est pas un R-module libre.

B L'algèbre d'un monoïde

On présente dans cette section un construction très importante d'algèbre : l'algèbre d'un monoïde. Cette construction engloble non seulement les algèbres de polynômes, mais aussi bien d'autres exemples intéressants.

Soit $G = (G, \cdot)$ est un monoïde (la loi $\cdot : G \times G \longrightarrow G$ est associative et possède un élément neutre, noté 1). On considère le A-module libre $A^{(G)}$, avec sa base canonique $\{e_g\}_{g\in G}$.

Définition-Proposition B.1. Soit $G = (G, \cdot)$ un monoïde. Il existe sur $A^{(G)}$ une unique structure de A-algèbre dont la stucture sous-jacente de A-module est celle de $A^{(G)}$, et dont le produit $* : A^{(G)} \times A^{(G)} \longrightarrow A^{(G)}$ vérifie, $\forall g, h \in G$, $e_g * e_h = e_{gh}$. L'élément neutre multiplicatif est e_1. Le produit $*$ est appelé **produit de convolution**. La A-algèbre obtenue, notée $A[G]$, est appelée **la A-algèbre du monoïde G.**

Preuve. L'existence de l'application A-bilinéaire $* : A^{(G)} \times A^{(G)} \longrightarrow A^{(G)}$ est assurée par un lemme précédent ($A^{(G)}$ est un A-module libre de base $\{e_g\}_{g\in G}$). Les identités

$$(e_g * e_h) * e_s = e_g * (e_h * e_s),\ e_g * e_1 = e_g = e_1 * e_g,\ \forall g, h, s \in G$$

sont assurées par les propriétés du monoïde G, et on obtient bien la A-algèbre annoncée. □

L'application $i : A \longrightarrow A[G], a \longmapsto a.e_1$, est un morphisme d'anneaux injectif, qui permet d'identifier A à un sous-anneau de $A[G]$.

Théorème B.2 (Propriété universelle de l'algèbre d'un monoïde)**.** Soient R une A-algèbre, G un monoïde et $f : G \longrightarrow R$ une application multiplicative, c'est-à-dire que $f(xy) = f(x)f(y)$, $\forall x, y \in G$, et $f(1) = 1$. Alors il existe un unique morphisme de A-algèbres $\overline{f} : A[G] \longrightarrow R$ tel que $\overline{f}(e_g) = f(g)$, $\forall g \in G$.

Preuve. Comme $A[G]$ est un A-module libre de base $\{e_g\}_{g\in G}$, il existe une unique application A-linéaire $\overline{f} : A[G] \longrightarrow R$ tel que $\overline{f}(e_g) = f(g)$, $\forall g \in G$. On a $\overline{f}(e_1) = f(1) = 1$. Pour $x = \sum_{g\in G} x_g.e_g$ et $y = \sum_{g\in G} y_g.e_g$, on a $xy = \sum_{s\in G}(\sum_{gh=s} x_g y_h).e_s$, et donc

$$\overline{f}(xy) = \sum_{s\in G}(\sum_{gh=s} x_g y_h).f(s)$$

alors que

$$\overline{f}(x)\overline{f}(y) = \sum_{g,h\in G}(x_g y_h).(f(g)f(h)) = \sum_{g,h\in G}(x_g y_h).f(gh) = \sum_{s\in G}(\sum_{gh=s} x_g y_h).f(s)$$

et ainsi $\overline{f}$ est un morphisme d'algèbres. □

Remarque. La A-algèbre $A[G]$ est commutative si et seulement si le monoïde G est commutatif.

On décrira au chapitre VII la structure de l'algèbre $\mathbb{C}[G]$ lorsque G est un groupe fini. On utilisera le résultat suivant.

Proposition B.3. Soit G un groupe fini. Alors $Z(A[G])$, le centre de $A[G]$, est un A-module libre de rang égal au nombre de classes de conjugaison de G.

Preuve. Soit $\phi \in A[G]$. Alors puisque les $(e_g)_{g\in G}$ forment une base de $A[G]$, il est clair que $\phi \in Z(A[G]) \iff [\forall g \in G, e_g * \phi = e_g * \phi]$, d'où en multipliant à gauche par $e_{g^{-1}}$, $\phi \in Z(A[G]) \iff [\forall g \in G, e_g * \phi * e_{g^{-1}} = \phi]$ donc

$$\phi \in Z(A[G]) \iff \forall g \in G,\ \phi = \sum_{h\in G} \phi(h)e_h = e_g * \phi * e_{g^{-1}} = \sum_{y\in G} \phi(y)e_{gyg^{-1}} = \sum_{h\in G} \phi(g^{-1}hg)e_h$$

Ceci montre que $\phi \in Z(A[G]) \iff \forall g,h \in G,\ \phi(ghg^{-1}) = \phi(h)$ (ϕ est une fonction centrale sur G).

Soit C une classe de conjugaison de G. On pose $x_C = \sum_{g\in C} e_g$. Alors la fonction x_C est la fonction indicatrice de la classe de conjugaison C : $x_C(g) = 1$ si $g \in C$ et $x_C(g) = 0$ si $g \notin C$. Ainsi x_C est constante sur les classes de conjugaison, et est une fonction centrale, d'où $x_C \in Z(A[G])$. Soient $C_1, \dots, C_t$ les classes de conjugaison de G : $G = C_1 \amalg \dots \amalg C_t$. On sait donc que $Ax_{C_1} + \dots + Ax_{C_t} \subset Z(A[G])$. Montrons que $x_{C_1}, \dots, x_{C_t}$ est une base de $Z(A[G])$. Déjà ces éléments sont linéairement indépendants car les $(e_g)_{g\in G}$ le sont et les classes de conjugaison sont disjointes. Soit maintenant $\phi \in Z(A[G])$. Alors ϕ est une fonction centrale, et donc est constante sur les classes de conjuguaison de G. Si C est une classe de conjugaison de G, notons $\phi(C)$ la valeur de ϕ sur n'importe quel élément de C. On obtient alors

$$\phi = \sum_{g\in G} \phi(g)e_g = \sum_{i=1}^{t} \sum_{g\in C_i} \phi(g)e_g = \sum_{i=1}^{t} \sum_{g\in C_i} \phi(C_i)e_g = \sum_{i=1}^{t} \phi(C_i) \sum_{g\in C_i} e_g = \sum_{i=1}^{t} \phi(C_i)x_{C_i},$$

ce qui assure bien que $x_{C_1}, \dots, x_{C_t}$ est une partie génératrice de $Z(A[G])$, et donc une base de $Z(A[G])$ qui est donc un A-module libre de rang le nombre de classes de conjugaison de G. □

C Algèbres de polynômes

On va utiliser la construction du paragraphe précédent pour (re)définir une classe d'algèbres très importante : les algèbres de polynômes.

Soit $n \in \mathbb{N}^*$. Considérons le monoïde additif $\mathbb{N}^n$. Pour $i \in \{1, \dots, n\}$, notons $X_i = e_{(0,\dots,1,\dots,0)}$, où le 1 est situé à la i-ème place. Par définition du produit dans $k[\mathbb{N}^n]$, on a, pour $(i_1, \dots, i_n) \in \mathbb{N}^n$,

$$e_{(i_1,\dots,i_n)} = X_1^{i_1} \cdots X_n^{i_n}$$

avec bien sûr la convention $X_i^0 = 1 = e_{(0,\dots,0)}$. Les $X_1^{i_1} \cdots X_n^{i_n}$, $(i_1, \dots, i_n) \in \mathbb{N}^n$ forment donc une base du A-module libre $A[\mathbb{N}^n]$, et on écrit alors

$$A[\mathbb{N}^n] = A[X_1, \dots, X_n]$$

Définition C.1. *L'algèbre $A[X_1, \dots, X_n] = A[\mathbb{N}^n]$ est **l'algèbres des polynôme à n variables à coefficients dans** A. Les éléments de $A[X_1, \dots, X_n]$ sont appelés les **polynômes à coefficients dans** A.*

A s'identifie à un sous-anneau de $A[X_1, \dots X_n]$ (avec $a = a1$), et donc si B est un sous-anneau de A, il s'identifie à un sous-anneau de $A[X_1, \dots X_n]$, que l'on peut donc voir comme une B-algèbre.

La propriété universelle de $A[X_1, \dots, X_n]$ est la suivante.

Théorème C.2. Soient B une A-algèbre et $b_1, \dots, b_n \in B$ tels que $b_i b_j = b_j b_i$ pour tous i,j. Alors il existe une unique morphisme de A-algèbres

$$\varphi : A[X_1, \dots, X_n] \longrightarrow B$$

tel que $\varphi(X_i) = b_i$, $\forall i \in \{1, \dots n\}$. Pour $P \in A[X_1, \dots, X_n]$, on note $P(b_1, \dots, b_n) = \varphi(P)$.

Preuve. On considère d'abord l'application $\mathbb{N}^n \longrightarrow B$, $(i_1, \dots, i_n) \longmapsto b_1^{i_1} \cdots b_n^{i_n}$, qui est multiplicative car les b_i commutent deux à deux. On applique ensuite la propriété universelle de l'algèbre du monoïde $\mathbb{N}^n$. □

Corollaire C.3. Soient A et B des anneaux commutatifs et $f : A \longrightarrow B$ un morphisme d'anneaux. Alors il existe un unique morphisme d'anneaux $\tilde{f} : A[X_1, \dots, X_n] \longrightarrow B[X_1, \dots, X_n]$ tel que $\tilde{f}_{|A} = f$ et $f(X_i) = X_i$, pour tout i.

Preuve. On peut construire $\tilde{f}$ directement, ou bien utiliser le résultat précédent en munissant $B[X_1, \dots, X_n]$ de la structure de A-algèbre induite par la composition $A \to B \hookrightarrow B[X_1, \dots, X_n]$. □

Le résultat qui suit est très utile pour montrer des résultats par récurrence sur le nombre de variables.

Proposition C.4. Les A-algèbres $A[X_1, \dots, X_n]$ et $A[X_1, \dots, X_{n-1}][X_n]$ sont isomorphes.

Preuve. Il existe un unique morphisme de A-algèbres $f : A[X_1, \dots, X_n] \longrightarrow A[X_1, \dots, X_{n-1}][X_n]$ tel que $f(X_i) = X_i$, pour tout i. On vérifie que f est un isomorphisme (par exemple en remarquant que f envoie une base de $A[X_1, \dots, X_n]$ sur une base de $A[X_1, \dots, X_{n-1}][X_n]$). □

Proposition C.5. Soient A un anneau et I un idéal de A. Alors on a un isomorphisme d'anneaux $(A/I)[X] \cong A[X]/(A[X]I)$.

Preuve. La surjection canonique $p : A \longrightarrow A/I$ induit un morphisme d'annneaux $\tilde{p} : A[X] \longrightarrow A/I[X]$, $\sum_{i=0}^m a_i X^i \mapsto \sum_{i=0}^m p(a_i) X^i$. Il est clair que $\tilde{p}$ est surjectif, et on vérifie sans difficulté que $\mathrm{Ker}(\tilde{p}) = IA[X]$, l'idéal de $A[X]$ engendré par I, ce qui permet d'appliquer le théorème d'isomorphisme pour les anneaux. □

Définition C.6. 1. *Un monôme est un polynôme de la forme $aX_1^{i_1} \cdots X_n^{i_n}$, pour $a \in A$ $a \neq 0$ et $(i_1, \dots, i_n) \in \mathbb{N}^n$. Le **degré** du monôme $X_1^{i_1} \cdots X_n^{i_n}$ est défini par*

$$\deg(X_1^{i_1} \cdots X_n^{i_n}) = i_1 + \cdots + i_n$$

2. *Un **polynôme homogène de degré** $k \in \mathbb{N}$ est une combinaison linéaire de monômes de degré k.*

3. *Soit* $P \in A[X_1, \ldots, X_n]$, $P \neq 0$ *avec* $P = \sum_{i_1,\ldots,i_n} a_{(i_1,\ldots,i_n)} X_1^{i_1} \cdots X_n^{i_n}$. *Le* ***degré du polynôme*** *P est défini par*

$$\deg(P) = \max\{\deg(X_1^{i_1} \cdots X_n^{i_n}), a_{(i_1,\ldots,i_n)} \neq 0\}$$

Par ailleurs on pose $\deg(0) = -\infty$.

Exemple C.7. $XY - X^2$ est un polynôme homogène de degré 2 de $A[X, Y]$

Proposition C.8. Soit $P \in A[X_1, \ldots, X_n]$ un polynôme de degré $d \geq 0$. Alors il existe des polynômes homogènes P_k , $0 \leq k \leq d$, de degrés respectifs k, tels que $P = P_0 + \cdots + P_d$. Cette écriture est unique.

Preuve. Il suffit d'utiliser le fait que les monômes forment une base. Les détails sont laissés en exercice. □

Proposition C.9. Soient $P, Q \in A[X_1, \ldots, X_n]$.

1. Si $P + Q \neq 0$, alors $\deg(P + Q) = \max(\deg(P), \deg(Q))$.
2. $\deg(PQ) \leq \deg(P) + \deg(Q)$, avec égalité si A est intègre.

Preuve. Exercice □

Corollaire C.10. Si A est un anneau intègre, alors $A[X_1, \ldots, X_n]$ est un anneau intègre.

Preuve. C'est une application directe des identités précédentes. □

Le résultat important suivant est l'existence d'une division euclidienne sur les anneaux de polynômes.

Théorème C.11. Soit A un anneau (non nul) et soient $F, P \in A[X]$ avec P de coefficient dominant inversible dans A. Alors il existe $Q, R \in A[X]$ tels que $F = PQ + R$ et $\deg(R) < \deg(P)$.

Preuve. Notons $\pi : A[X] \to A[X]/(P) = B$ la surjection canonique, $x = \pi(X)$, et

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

avec $a_n \in U(A)$ ($n \geq 0$). Dans B, on a $\pi(P) = 0$, donc

$$x^n = -(\pi(a_n^{-1} a_{n-1}) x^{n-1} + \cdots + \pi(a_n^{-1} a_1) x + \pi(a_n^{-1} a_0))$$

On en déduit facilement que pour tout $k \geq n$, x^k est combinaison linéaire (à coefficients dans $\pi(A)$) des x^i, $0 \leq i \leq n-1$, et qu'un élément quelconque de B est combinaison linéaire (à coefficients dans $\pi(A)$) des x^i, $0 \leq i \leq n-1$.

Soit $F \in A[X]$: on a $\pi(F) = \pi(b_{n-1}) x^{n-1} + \cdots + \pi(b_1) x + \pi(b_0)$, pour des éléments $b_0, \ldots, b_n \in A$. Posons $R = b_{n-1} X^{n-1} + \cdots + b_1 X + b_0 \in A[X]$. On a $\pi(F) = \pi(R)$, donc il existe $Q \in A[X]$ tel que $F = PQ + R$, avec $\deg(Q) < \deg(P)$. □

Bien sûr, le résultat est déjà bien connu quand A est un corps, et permet de montrer, entre autres résultats fondamentaux, qu'un polynôme non nul n'a qu'un nombre fini de racines. Nous ne rappelons pas ces résultats.

La version générale la division euclidienne est cependant utile dans diverses situations, en particulier pour les polynômes à plusieurs variables. Voila un exemple.

Proposition C.12. Soit A un anneau (non nul). Pour tout $(a_1, \dots, a_n) \in A^n$ et tout $P \in A[X_1, \dots, X_n]$, on a

$$P(a_1, \dots, a_n) = 0 \iff P \in (X_1 - a_1, \dots, X_n - a_n)$$

et $A[X_1, \dots, X_n]/(X_1 - a_1, \dots, X_n - a_n) \simeq A$. En particulier si $A = k$ est un corps, l'idéal $(X_1 - a_1, \dots, X_n - a_n)$ est maximal dans $k[X_1, \dots, X_n]$.

Preuve. L'implication $\Leftarrow$ est claire. Pour l'implication inverse, on procède par récurrence sur n, le cas $n = 1$ étant connu. Supposons le résultat montré au rang $n - 1$. Soit $P \in A[X_1, \dots, X_n]$. Par division euclidienne (dans $A[X_1, \dots, X_{n-1}][X_n]$), il existe $Q \in A[X_1, \dots X_n]$, $R \in A[X_1, \dots, X_{n-1}]$ tels que $P = (X_m - a_m)Q + R$. Alors si $P(a_1, \dots, a_n) = 0$, on a $R(a_1, \dots, a_{n-1}) = 0$, et l'hypothèse de récurrence permet de conclure. Considérons maintenant

$$\begin{aligned} \varphi : A[X_1, \dots, X_n] &\to A \\ P &\mapsto P(a_1, \dots, a_n) \end{aligned}$$

C'est un morphisme de A-algèbres surjectif, donc $I = \mathrm{Ker}(\varphi)$ est un idéal maximal, et d'après ce qui précède que $(X_1 - a_1, \dots, X_n - a_n) = I$, ce qui donne le résultat. □

IV Arithmétique dans les anneaux factoriels

Dans ce chapitre, tous les anneaux sont supposés commutatifs, et ainsi anneau = anneau commutatif. Un grand nombre des résultats du chapitre sont déjà connus du lecteur, dans le cadre des anneaux principaux. On se place ici dans le cadre plus général des anneaux factoriels. Le texte présenté ici, basé sur [Perrin], est essentiellement auto-contenu.

A Anneaux noethériens

Dans $\mathbb{Z}$, tout idéal est de la forme $n\mathbb{Z}$, engendré par un élément. Cette propriété est formalisée par la définition suivante.

Définition A.1. *Soient A un anneau et I un idéal de A. On dit que I est **principal** s'il est engendré par un élément : $I = Aa = (a)$ pour un $a \in I$.*
*Un **anneau principal** est un anneau intègre dont tout idéal est principal.*

Définition A.2. *Soient A un anneau et I un idéal de A. On dit que I est **de type fini** s'il est engendré par un nombre fini d'éléments : $I = (a_1, \dots, a_n) = Aa_1 + \cdots + Aa_n$ pour $a_1, \dots, a_n \in I$.*

Définition-Proposition A.3. Soit A un anneau. Les assertions suivantes sont équivalentes.

1. Tout idéal de A est de type fini.
2. Toute suite croissante $I_1 \subset I_2 \subset \cdots \subset I_n \subset I_{n+1} \subset \cdots$ d'idéaux de A est stationnaire : $\exists N$ tel que $\forall n \geq N$, on a $I_n = I_N$.
3. Tout ensemble non vide d'idéaux de A possède un élément maximal (pour l'inclusion).

Un anneau satisfaisant l'une de ces conditions est dit **noethérien**.

Preuve. (1) $\Rightarrow$ (2) La suite $(I_n)_{n\in\mathbb{N}^*}$ est croissante, donc $I = \cup_{n\in\mathbb{N}^*} I_n$ est un idéal de A, et $I = (a_1, \dots, a_l)$ pour $a_1, \dots, a_l \in I$. Soit $N \in \mathbb{N}^*$ tel que $a_1, \dots, a_l \in I_N$. Alors $I = (a_1, \dots, a_l) \subset I_N \subset I$. Donc si $n \geq N$, on a $I_n = I_N$.

(2) $\Rightarrow$ (3) Soit E une famille non vide d'idéaux de A. Supposons que E n'a pas d'élément maximal. Soit $I_1 \in E$. Comme E n'a pas d'élément maximal, il existe $I_2 \in E$ tle que $I_1 \subsetneq I_2$. De même I_2 n'est pas maximal donc il existe $I_3 \in E$ tel que $I_2 \subsetneq I_3$. On construit ainsi par récurrence une suite $(I_n)_{n\geq 1}$ d'idéaux de A telle que $\forall n$, $I_n \subsetneq I_{n+1}$: cette suite n'est pas stationnaire.

(3) $\Rightarrow$ (1) Soit I un idéal de A et soit E l'ensemble des idéaux de J de A qui sont inclus dans I et sont de type fini. E est non vide car $(0) \in E$. Soit J un élément maximal de E. Si $J \subsetneq I$, soit $a \in I \setminus J$. Alors $J \subsetneq J + (a)$, avec $J + (a)$ idéal de type fini inclus dans I, ce qui contredit la maximalité de J. Donc $J = I$ et I est de type fini. $\square$

Un anneau principal est bien sûr noethérien. D'autres exemples sont fournis par le résultat suivant.

Proposition A.4. Soit $f : A \to B$ un morphisme d'anneaux surjectif. Si A est noethérien, alors B est noethérien.

Preuve. Soit J un idéal de B. Alors $f^{-1}(J)$ est un idéal de l'anneau noethérien A, il existe donc $a_1, \ldots, a_n \in A$ tels que $f^{-1}(J) = (a_1, \ldots, a_n)$. On a alors $J = f(f^{-1}(J)) = (f(a_1), \ldots, f(a_n))$ (surjectivité de f) et donc J est de type fini. □

On prendra garde qu'un sous-anneau d'un anneau noethérien n'est pas nécessairement noethérien.

La source principale d'anneaux noethériens est le théorème suivant.

Théorème A.5 (de la base finie de Hilbert)**.** Soit A un anneau noethérien. Alors l'anneau $A[X]$ est noethérien.

Preuve. Supposons $A[X]$ non noethérien : il existe un idéal I de $A[X]$ qui n'est pas de type fini. Soit $f_1 \in I$ de plus bas degré (≥ 0) possible. Soit $f_2 \in I \setminus (f_1)$ de plus bas degré possible, $f_3 \in I \setminus (f_1, f_2)$ de plus bas degré possible... On construit ainsi une suite $(f_k)_{k\geq 1}$ d'éléments de I telle que f_k soit de plus bas degré possible dans $I \setminus (f_1, \ldots, f_{k-1})$. Soit a_k le coefficient dominant de f_k et soit $n_k = \deg(f_k) \geq 0$. On a

$$n_1 \leq n_2 \leq n_3 \leq \cdots \leq n_k \leq n_{k+1} \leq \cdots \quad \text{et} \quad (a_1) \subset (a_1, a_2) \subset \cdots \subset (a_1, \ldots, a_k) \subset (a_1, \ldots, a_{k+1}) \subset \cdots$$

Supposons qu'il existe k tel que $(a_1, \ldots, a_k) = (a_1, \ldots, a_k, a_{k+1})$. Il existe alors $b_1, \ldots, b_k \in A$ tels que $a_{k+1} = \sum_{i=1}^{k} b_i a_i$, et écrivons pour tout $i \leq k$, $f_i = a_i X^{n_i} + Q_i$, avec $\deg(Q_i) < n_i$. Soit

$$g = f_{k+1} - \sum_{i=1}^{k} b_i X^{n_{k+1}-n_i} f_i = f_{k+1} - (\sum_{i=1}^{k} b_i a_i) X^{n_{k+1}} - \sum_{i=1}^{k} b_i Q_i$$

Alors $\deg(g) < n_{k+1}$ et $g \in I \setminus (f_1, \ldots, f_k)$: contradiction. On a donc $(a_1, \ldots, a_k) \subsetneq (a_1, \ldots, a_k, a_{k+1})$ pour tout k, ce qui montre que A n'est pas noethérien. □

Exemple A.6. $\mathbb{Z}[X]$ est noethérien (mais n'est pas principal, on le verra plus loin).

Un récurrence immédiate donne :

Corollaire A.7. Soit A un anneau noethérien. Alors l'anneau $A[X_1, \ldots, X_n]$ est noethérien.

En combinant le corrollaire et une proposition précédente, on obtient :

Corollaire A.8. Soient A un anneau noethérien et soit I un idéal de $A[X_1, \ldots, X_n]$. L'anneau quotient $A[X_1, \ldots, X_n]/I$ est noethérien.

B Divisibilité

Dans la suite A est un anneau. On note $U(A)$ le groupe multiplicatif des éléments inversibles de A.

Définition B.1. *Soient $a, b \in A$. On dit que a **divise** b, et on écrit $a|b$, s'il existe $c \in A$ tel que $b = ca$.*

Proposition B.2. Soient $a, b \in A$. Alors $a|b \iff (b) \subset (a)$

Preuve. Exercice □

Définition B.3. *Soient $a, b \in A$. On dit que a est b sont **associés**, et on note $a \sim b$, si $a|b$ et $b|a$, c'est-à-dire si $(a) = (b)$.*

Il est clair que la relation d'"association" est une relation d'équivalence sur A.

Exemple B.4. Dans $\mathbb{Z}$, $m \sim n \iff m = \pm n$.

Proposition B.5. Soient A un anneau intègre et $a, b \in A$. Alors $a \sim b$ si et seulement s'il existe $u \in U(A)$ tel que $a = ub$.

Preuve. Exercice □

On suppose dans la suite que A est un anneau intègre.

Définition B.6. *Soit $p \in A$. On dit que p est **irréductible** si*

1. *$p \notin U(A)$;*
2. *Si $p = ab$, alors $a \in U(A)$ ou $b \in U(A)$.*

Remarque B.7.

1. 0 n'est pas irréductible.
2. Dans un corps il n'y pas d'élément irréductible.
3. Si $p, q \in A$ sont irréductibles, alors $p|q \iff p \sim q$.

Exemples B.8.

1. Pour $n \in \mathbb{Z}$, on a n irréductible $\iff |n|$ est un nombre premier.
2. Dans $k[X]$, avec k un corps, $X - a$ est irréductible ($a \in k$).

Proposition B.9. Soit $p \in A^*$. Alors (p) premier $\Rightarrow$ p irréductible.

Preuve. Supposons (p) premier. Alors $(p) \subsetneq A$, donc $p \notin U(A)$. Suposons que $p = ab$, avec $a, b \in A$. Alors $ab \in (p)$, cet idéal étant premier, donc $a \in (p)$ ou $b \in (p)$. Si $a \in (p)$, alors il existe $x \in A$ tel que $a = px = abx$, d'où $b \in U(A)$ (A intègre et $a \neq 0$ car $p \neq 0$). □

Remarque B.10. La réciproque de la proposition précédente n'est pas vraie. En effet, soit $A = \mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}, a, b \in \mathbb{Z}\}$. On vérifie, en utilisant $N : A \to \mathbb{N}$, $\alpha \mapsto \alpha\overline{\alpha}$, que $U(A) = \{\pm 1\}$. On vérifie également, toujours en utilisant N, que 3 est irréductible dans A, mais que l'idéal (3) n'est pas premier dans A, car $9 = (2 + i\sqrt{5})(2 - i\sqrt{5}) \in (3)$, alors que $2 + i\sqrt{5} \notin (3)$ et $2 - i\sqrt{5} \notin (3)$.

Théorème B.11. Soient A un anneau principal et $p \in A^*$. Alors

$$(p) \text{ maximal} \iff (p) \text{ premier} \iff p \text{ irreductible}$$

Preuve. Un idéal maximal est premier, et la propriété (p) premier $\Rightarrow$ p irréductible a été vue. Supposons p irréductible. Déjà $(p) \subsetneq A$ car $p \notin U(A)$. Soit I un idéal de A tel que $(p) \subset I$. Comme A est principal, il existe $a \in I$ tel que $I = (a)$, et on a $p \in (a)$, d'où $p = ab$. Alors $a \in U(A)$ ou $b \in U(A)$. Dans le premier cas $I = A$ et dans le deuxième $I = (p)$: on en déduit que (p) est maximal. □

Définition B.12. *Soient $a, b \in A$. On dit que a et b sont premiers entre eux si*

$$\forall d \in A,\ d|a \text{ et } d|b \Rightarrow d \in U(A)$$

Proposition B.13 (Théorème de Bezout)**.** Soient $a, b \in A$. Alors $(a) + (b) = A \Rightarrow a$ et b sont premiers entre eux. Si A est principal, alors $(a) + (b) = A \iff a$ et b sont premiers entre eux.

Preuve. Si $(a) + (b) = A$, il existe $u, v \in A$ tels que $1 = au + bv$. Donc si $a = dx$ et $b = dy$, on a $1 = d(xu + yv)$ et $d \in U(A)$, et a et b sont premiers entre eux.

Supposons A principal et a, b premiers entre eux. Soit $d \in A$ tel que $(a) + (b) = (d)$. Alors $a|d$ et $b|d$, donc $d \in U(A)$ et $(a) + (b) = A$. □

Remarque B.14. Si l'anneau n'est pas principal, on n'a pas l'équivalence. Par exemple, si k est un corps, les éléments X et Y de $k[X, Y]$ sont premiers entre eux, mais $(X) + (Y) \subsetneq (X, Y)$.

C Anneaux factoriels

Définition C.1 (Anneau factoriel, première définition)**.** *Un **anneau factoriel** est un anneau intègre A satisfaisant les deux conditions suivantes.*

(E) Tout élément $a \in A^*$ s'écrit

$$a = up_1 \cdots p_r$$

avec $u \in U(A)$ et $p_1, \ldots, p_r$ irréductibles.

(U) Cette écriture est unique : si $a = up_1 \cdots p_r = vq_1 \cdots q_s$ avec $u, v \in U(A)$ et $p_1, \ldots, p_r, q_1, \ldots q_s$ irréductibles, on a $r = s$ et il existe $\sigma \in S_r$ tels que $\forall i$, $p_i \sim q_{\sigma(i)}$.

Il est souvent utile d'introduire une reformulation de cette définition. On fixe $\mathcal{P}$ un ensemble de représentants des irréductibles de A pour la relation $\sim$. Il existe donc pour tout irréductible $q \in A$, un unique $p \in \mathcal{P}$ tel que $q \sim p$, et donc pour $q, p \in \mathcal{P}$, $q \sim p \iff q = p$ (Par exemple quand $A = \mathbb{Z}$, $\mathcal{P}$ est l'ensemble des nombres premiers).

Définition C.2 (Anneau factoriel, deuxième définition)**.** *Un **anneau factoriel** est un anneau intègre A satisfaisant les deux conditions suivantes.*

(E') Tout élément $a \in A^*$ s'écrit

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

avec $u \in U(A)$ et les $v_p(a) \in \mathbb{N}$ nuls sauf pour un nombre fini d'éléments de $\mathcal{P}$.

*(U') Cette écriture est unique. L'entier $v_p(a)$ s'appelle **la valuation p-adique de** A.*

Il est clair que les axiomes (E) et (E') sont équivalents, et qu'en présence de (E) et (E'), les axiomes (U) et (U') sont équivalents. On utilisera ces divers axiomes de manière interchangeable.

Proposition C.3. Soient A un anneau factoriel et $a, b \in A^*$. Pour $p \in \mathcal{P}$, on a $v_p(ab) = v_p(a) + v_p(b)$ et

$$a|b \iff \forall p \in \mathcal{P},\ v_p(a) \leq v_p(b)$$

Preuve. Ecrivons

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)} \quad \text{et} \quad b = v \prod_{p \in \mathcal{P}} p^{v_p(b)}$$

avec $u, v \in U(A)$. Alors

$$ab = uv \prod_{p \in \mathcal{P}} p^{v_p(a)+v_p(b)}$$

et l'axiome U' donne $v_p(ab) = v_p(a) + v_p(b)$ pour tout $p \in \mathcal{P}$. Si $\forall p \in \mathcal{P}$, $v_p(a) \leq v_p(b)$, soit $c = \prod_{p \in \mathcal{P}} p^{v_p(b)-v_p(a)}$. On a $vu^{-1}ac = b$, donc $a|b$. Réciproquement si $ac = b$ pour un $c \in A$, alors $\forall p \in \mathcal{P}$ on a $v_p(b) = v_p(a) + v_p(c)$, d'où $v_p(b) \geq v_p(a)$. □

Le résultat suivant montre qu'en fait la condition (E) est assez peu contraignante.

Proposition C.4. Soit A un anneau intègre et noethérien. Alors A vérifie (E).

Preuve. Soit F l'ensemble des idéaux de A de la forme (a), $a \in A^*$ ne s'écrivant pas sous la forme $a = up_1 \cdots p_r$ avec u inversible et $p_1, \ldots, p_r$ irréductible. On doit montrer que F est vide. Supposons au contraire que F est non vide. Comme A est noethérien, il existe $a \in A^*$ tel que (a) soit un élément maximal de F. Alors a n'est ni inversible ni irréductible. Il existe donc $b, c \in A$, $b, c \notin U(A)$ tels que $a = bc$. On a $(a) \subset (b)$ et $(a) \subset (c)$, et de plus $(a) \subsetneq (b)$ et $(a) \subsetneq (c)$. En effet si par exemple $(a) = (b)$ on a $a = ub$ pour $b \in U(A)$, car A est intègre. Comme aussi $a = bc$, on obtient $c \in U(A)$, une contradiction. La maximalité de (a) dans F implique $(b) \notin F$ et $(c) \notin F$. Il existe donc $u, v \in U(A)$, $p_1, \ldots p_r, q_1, \ldots q_s$ des irréductibles de A tels que

$$b = up_1 \cdots p_r, \quad c = vq_1 \cdots q_s$$

et donc $a = uvp_1 \cdots p_r q_1 \cdots q_s$, et $(a) \notin F$: contradiction. Donc $F = \emptyset$ et A vérifie (E). □

Lemme C.5. Soit A un anneau intègre. Les assertions suivantes sont équivalentes.

1. A vérifie le lemme d'Euclide : si $p \in A$ est irréductible et $p|ab$, alors $p|a$ ou $p|b$.
2. Dans A, pour $p \in A^*$, p irréductible $\iff$ (p) premier.

Preuve. (1) $\Rightarrow$ (2) Soit $p \in A^*$ irréductible. Alors $(p) \subsetneq A$ car $p \notin U(A)$. Si $ab \in (p)$, on a $p|ab$, donc le lemme d'Euclide donne $p|a$ ou $p|b$, c'est-à-dire $a \in (p)$ ou $b \in (p)$. Donc (p) et premier.

(2) $\Rightarrow$ (1) Soit $p \in A$ irréductible tel que $p|ab$. Alors $ab \in (p)$. Comme (p) est premier, on a $a \in (p)$ ou $b \in (p)$, c'est-à-dire que $p|a$ ou $p|b$. □

Théorème C.6. Soit A un anneau intègre vérifiant l'axiome (E). Les assertions suivantes sont équivalentes.

1. A vérifie (U), c'est-à-dire A est factoriel.
2. A vérifie le lemme d'Euclide : si $p \in A$ est irréductible et $p|ab$, alors $p|a$ ou $p|b$.
3. Dans A, pour $p \in A^*$, p irreductible $\iff$ (p) premier.
4. A vérifie le lemme de Gauss : si $a|bc$ et a est premier avec b, alors $a|c$.

Preuve. Le lemme précédent assure que $(2) \iff (3)$.

Montrons $(4) \Rightarrow (2)$. Soit p irréductible tel que $p|ab$. Supposons que p ne divise pas a, et montrons que p est premier avec a. Soit $d \in A$ tel que $d|a$ et $d|p$: il existe $\alpha, \beta \in A$ tels que $a = \alpha d$ et $p = \beta d$. Si $d \notin U(A)$, comme p est irréductible on a $\beta \in U(A)$ et $a = \alpha\beta^{-1}p$ et $p|a$: contraire à l'hypothèse. Donc $d \in U(A)$ et a et p sont premiers entre eux. On applique alors le lemme de Gauss : $p|b$.

Montrons $(2) \Rightarrow (1)$. Notons tout d'abord que le lemme d'Euclide, s'il est vrai dans A, se généralise directement à : si p irréductible divise $a_1 \cdots a_n$, alors il existe i tel que $p|a_i$. Soit $a \in A$, $a \neq 0$, avec

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)} = v \prod_{p \in \mathcal{P}} p^{w_p(a)}$$

où $u, v \in U(A)$ et $v_p(a), w_p(a) \in \mathbb{N}$. Soit $q \in \mathcal{P}$ tel que $v_q(a) > 0$. Alors q divise le troisième membre, et alors le lemme d'Euclide assure que q divise $q^{w_q(a)}$, c'est-à-dire $w_q(a) > 0$. On a donc

$$uq^{v_q(a)-1} \prod_{p \in \mathcal{P}, p \neq q} p^{v_p(a)} = vq^{w_q(a)-1} \prod_{p \in \mathcal{P}, p \neq q} p^{w_p(a)}$$

On réitère le procédé jusqu'à trouver $v_q(a) = w_q(a)$, pour tout $q \in \mathcal{P}$, et finalement on a $u = v$.

Il reste à voir que $(1) \Rightarrow (4)$. Supposons que $a|bc$ et que a est premier avec b. On doit montrer que $a|c$, c'est-à-dire que pour tout $p \in \mathcal{P}$, on a $v_p(a) \leq v_p(c)$. Supossons au contraire qu'il existe $p \in \mathcal{P}$ tel que $v_p(a) > v_p(c)$. Comme $a|bc$, on a $v_p(a) \leq v_p(bc) = v_p(b) + v_p(c)$, donc $v_p(b) \geq v_p(a) - v_p(c) > 0$. Ainsi $p|b$ et $p|a$. Cela contredit que a et b sont premiers entre eux (p non inversible car irréductible). □

Corollaire C.7. Un anneau principal est factoriel.

Preuve. Un anneau principal est intègre et noethérien, donc vérifie (E), et vérifie la condition (3) du théorème, il est donc factoriel. □

Exemples C.8. 1. $\mathbb{Z}$ est factoriel car principal.

2. $\mathbb{Z}[i\sqrt{5}]$ est intègre (car inclus dans $\mathbb{C}$) et noethérien (car c'est un quotient de $\mathbb{Z}[X]$) mais n'est pas factoriel car il contient des éléments irréductibles qui engendrent des idéaux non premiers.

Définition C.9. *Soient A un anneau intègre et $a_1, \ldots, a_n$ des éléments de A.*

*Un **PGCD** des éléments $a_1, \ldots, a_n$ est un élément δ de A vérifiant*

1. *$\delta | a_i$, $\forall i \in \{1, \ldots, n\}$,*
2. *Si $b | a_i$, $\forall i \in \{1, \ldots, n\}$, alors $b | \delta$.*

Un tel élément, s'il existe, est noté $\mathrm{PGCD}(a_1, \ldots, a_n)$*. Il n'est défini qu'à multiplication par un inversible près.*

*Un **PPCM** des éléments $a_1, \ldots, a_n$ est un élément μ de A vérifiant*

1. *μ est un multiple de a_i, $\forall i \in \{1, \ldots, n\}$ ($a_i | \mu$),*
2. *Si b est un multiple de a_i, $\forall i \in \{1, \ldots, n\}$, alors b est un multiple de μ ($\mu | b$).*

Un tel élément, s'il existe, est noté $\mathrm{PPCM}(a_1, \ldots, a_n)$*. Il n'est défini qu'à multiplication par un inversible près.*

Théorème C.10. Toute famille $a_1, \ldots, a_n$ d'un anneau factoriel A admet un PGCD et un PPCM.

Preuve. Ecrivons, pour tout i,

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

avec u_i inversible. Posons, pour tout $p \in \mathcal{P}$,

$$d_p = \min(v_p(a_1), \ldots, v_p(a_n)), \quad m_p = \max(v_p(a_1), \ldots, v_p(a_n))$$

Soit alors

$$d = \prod_{p \in \mathcal{P}} p^{d_p} \quad \text{et} \quad m = \prod_{p \in \mathcal{P}} p^{m_p}$$

On vérifie sans problème que d est un PGCD de $a_1, \ldots, a_n$, et que m est un PPCM de $a_1, \ldots, a_n$. □

Proposition C.11. Soient A un anneau factoriel et $a_1, \ldots, a_n \in A$.

1. $a_1, \ldots, a_n$ sont premiers entre eux si et seulement si $\mathrm{PGCD}(a_1, \ldots, a_n) = 1$.
2. On a $\mathrm{PGCD}(a_1, a_2)\mathrm{PPCM}(a_1, a_2) \sim a_1 a_2$.
3. Pour $b \in A$, on a $\mathrm{PGCD}(ba_1, \ldots, ba_n) \sim b\mathrm{PGCD}(a_1, \ldots, a_n)$.
4. Si $d = \mathrm{PGCD}(a_1, \ldots, a_n)$, soient $b_1, \ldots, b_n \in A$ tels que $a_i = db_i$, $\forall i$. Alors on a $\mathrm{PGCD}(b_1, \ldots, b_n) = 1$.

Preuve. La première affirmation est immédiate, dès que l'on connait l'existence d'un PGCD. Les affirmations 2 et 3 se déduisent facilement des constructions explicites du PGCD et du PPCM dans la preuve du théorème précédent. Enfin l'affirmation 4 se déduit directement de la troisième. □

Remarque C.12. Si A est un anneau factoriel, on a $(a) \cap (b) = (c)$ où $c = \mathrm{PPCM}(a, b)$, mais on n'a pas en général $(a) + (b) = (d)$ où $d = \mathrm{PGCD}(a, b)$. Par exemple dans $k[X, Y]$ (k corps), qui est factoriel, on a $(X) + (Y) = (X, Y) \subsetneq k[X, Y]$ et $\mathrm{PGCD}(X, Y) = 1$.

Théorème C.13 (Bezout)**.** Soient A un anneau principal et $a_1, \ldots, a_n \in A$.

1. Pour $d \in A$, on a $d = \text{PGCD}(a_1, \ldots, a_n) \iff (a_1) + \cdots + (a_n) = (d)$.
2. $a_1, \ldots, a_n$ sont premiers entre eux si et seulement si $(a_1) + \cdots + (a_n) = A$.

La preuve est laissée en exercice.

Proposition C.14. Soit A un anneau factoriel et $K = \text{Fr}(A)$ son corps de fractions. Alors tout élément $x \in K^*$ s'écrit sous la forme $x = \frac{p}{q}$ avec $p, q \in A^*$ premiers entre eux.

Preuve. Voir l'appendice pour la construction du corps des fractions. La preuve est une conséquence directe de la proposition C.11 et des règles de calcul dans K.□

D Anneaux euclidiens

On montre que $\mathbb{Z}$ est principal en utilisant la division euclidienne. Ceci mène à la définition suivante.

Définition D.1. *Un **anneau euclidien** est un anneau intègre A muni d'une application $\nu : A^* \longrightarrow \mathbb{N}$, appelée stathme euclidien, telle que*

$$\forall a, b \in A^*, \text{ il } \textit{existe } q, r \in A \text{ tels que } a = bq + r, \text{ avec } r = 0 \text{ ou } \nu(r) < \nu(b)$$

Exemple D.2. $\mathbb{Z}$ est un anneau euclidien avec $\nu(n) = |n|$, $\forall n \in \mathbb{Z}$.

L'autre exemple fondamental d'anneau euclidien est celui des anneaux de polynômes à une variable à coefficients dans un corps. Le résultat provient de l'existence d'une division "euclidienne" dans un contexte plus général, établi dans le chapitre précédent.

Théorème D.3. Si k est un corps, alors $k[X]$ est un anneau euclidien (avec $\nu(P) = \deg(P)$ pour stathme).

Théorème D.4. Un anneau euclidien est principal.

Preuve. Soit I un idéal de A. Si $I = (0)$, I est principal, on peut donc supposer $I \neq (0)$. Soit alors $a \in I$, $a \neq 0$, tel que $\nu(a) \in \mathbb{N}$ soit minimal. On a $(a) \subset I$, et montrons que $(a) = I$. Soit $x \in I$. Il existe $q, r \in A$ tels que $x = aq + r$ et $r = 0$ ou $\nu(r) < \nu(a)$. On a $r = x - aq \in I$ avec $r = 0$ ou $\nu(r) < \nu(a)$ si $r \neq 0$. Le deuxième cas qui contredit la minimalité de $\nu(a)$, donc $r = 0$ et $x \in (a)$. □

Exemple D.5. Si k est un corps, alors $k[X]$ est principal.

Proposition D.6. Soit A un anneau. Alors $A[X]$ est principal $\iff$ A est un corps.

Preuve. Le Sens $\Leftarrow$ a été vu. Réciproquement, supposons $A[X]$ principal. En particulier A est intègre, et le polynôme X est un élément irréductible de $A[X]$. L'idéal (X) est donc maximal, et ainsi l'anneau quotient $A[X]/(X) \simeq A$ est un corps. □

Le résultat suivant est une source utile d'exemples d'anneau euclidiens.

Proposition D.7. Soient K un sous-corps de $\mathbb{C}$ et A un sous-anneau de K. On suppose :

1. $N(z) = |z|^2 \in \mathbb{N}, \forall z \in A$;
2. $\forall z \in K$, il existe $q \in A$ tel que $N(z-q) < 1$.

Alors l'anneau A est euclidien.

Preuve. Montrons que A est euclidien avec stahme N. A est un anneau intègre car c'est un sous-anneau du corps K. Soient $a, b \in A$ avec $b \neq 0$. Soit $z = b^{-1}a \in K$, et soit $q \in A$ tel que $N(z-q) < 1$ Soit $r = a - bq \in A$. On a $a = bq + r$ et $N(r) = N(a-bq) = N((z-q)b) = N(b)N(z-q) < N(b)$, d'où le résultat. □

Exemple D.8. $\mathbb{Z}[i]$ est un anneau euclidien. Cet anneau est appelé l'anneau des entiers de Gauss. On utilise le fait qu'il est factoriel pour montrer le théorème des deux carrés, qui décrit exactement les entiers qui sont somme de deux carres d'entiers.

On peut montrer qu'il existe des anneaux principaux non euclidiens : voir [Perrin]. On montrera dans le paragraphe qui suit que si A est factoriel, alors $A[X]$ est aussi factoriel. Il existe donc des anneaux factoriels non principaux, par exemple $\mathbb{Z}[X]$.

Les principaux résultats obtenus sont résumés dans le tableau suivant.

Résumé des principaux résultats d'arithmétique dans les anneaux

$\rightsquigarrow$ Euclidien $\Longrightarrow$ Principal $\Longrightarrow$ Factoriel

$\rightsquigarrow$ Dans un anneau factoriel A
- Pour $p \in A^*$, p irréductible $\iff$ (p) premier.
- PGCD et PPCM existent.
- A factoriel $\Longrightarrow$ $A[X]$ factoriel.

$\rightsquigarrow$ Dans un anneau principal A
- Pour $p \in A^*$, p irréductible $\iff$ (p) premier $\iff$ (p) maximal.
- $A[X]$ principal $\iff$ A est un corps.
- Théorème de Bezout : pour $a, b \in A$, $(a) + (b) = (d)$ où $d = \mathrm{PGCD}(a, b)$.

E Le théorème de Gauss

Le but du paragraphe est de montrer le résultat suivant.

Théorème E.1 (Gauss)**.** Si A est un anneau factoriel, alors $A[X]$ est un anneau factoriel.

Le concept suivant va jouer un rôle essentiel dans la preuve.

Définition E.2. *Soit A un anneau factoriel et soit $P \in A[X]$, $P = a_n X^n + \cdots + a_1 X + a_0$. **Le contenu de** P, noté $c(P)$, est défini comme étant le* PGCD *de $a_0, \ldots, a_n$. Cet élément n'est défini qu'à multiplication par un inversible près. On dit que P est **primitif** si $c(P) \sim 1$.*

Il est clair que pour $P \in A[X]$ et $a \in A$, on a $c(aP) \sim ac(P)$. On remarque aussi que tout $P \in A[X]$ s'écrit $P = c(P)\tilde{P}$, avec $\tilde{P} \in A[X]$ primitif.

Avant de démontrer le théorème de Gauss, on a besoin de résultats intermédiaires : trois lemmes et une proposition.

Lemme E.3. Soient $P, Q \in A[X]$. Alors on a $c(PQ) \sim c(P)c(Q)$.

Preuve. Supposons dans un premier temps que P et Q sont primitifs. Si $c(PQ) \not\sim 1$, comme A est factoriel, il existe $p \in A$ irréductible qui divise $c(PQ)$. Ecrivons $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{j=0}^{m} b_j X^j$. Comme $c(P) \sim 1$ et $c(Q) \sim 1$, il existe $i_0, j_0 \in \mathbb{N}$ tels que

$$i < i_0 \Rightarrow p | a_i \text{ et } p \not| a_{i_0}, \quad j < j_0 \Rightarrow p | b_j \text{ et } p \not| b_{j_0}$$

Comme p divise $c(PQ)$, il divise tous les coeffcients de PQ, en particulier le coefficient $i_0 + j_0$

$$c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \sum_{i+j=i_0+j_0, i<i_0 \text{ ou } j<j_0} a_i b_j$$

Ainsi p divise $a_{i_0} b_{j_0}$, et donc par le lemme d'Euclide $p | a_{i_0}$ ou $p | b_{j_0}$: contradiction. Donc $c(PQ) \sim 1$.

On revient au cas général : on peut écrire $P = c(P)\tilde{P}$ et $Q = c(Q)\tilde{Q}$ avec $\tilde{P}$ et $\tilde{Q}$ primitifs. Alors

$$c(PQ) = c(c(P)c(Q)\tilde{P}\tilde{Q}) \sim c(P)c(Q)c(\tilde{P}\tilde{Q}) \sim c(P)c(Q)$$

par le premier cas. □

Lemme E.4. Soit A un anneau factoriel et $K = \mathrm{Fr}(A)$.

1. Soit $P \in K[X]$. Alors on peut écrire $P = \frac{a}{b}\tilde{P}$, où $a \in A$, $b \in A^*$, a et b sont premiers entre eux, et $\tilde{P} \in A[X]$ est primitif.
2. Soit $P \in A[X]$ avec $P = QR$ pour $Q, R \in K[X]$. Alors il existe $\tilde{Q}, \tilde{R} \in A[X]$ tels que $P = \tilde{Q}\tilde{R}$ et $\deg(\tilde{Q}) = \deg(Q)$ et $\deg(\tilde{R}) = \deg(R)$.

Preuve. Ecrivons $P = \sum_{i=0}^{m} \frac{a_i}{b_i} X^i$, et soit b un multiple commun de $b_0, \ldots, b_m$. On a alors $P = \frac{1}{b} \sum_{i=0}^{m} a'_i X^i$ pour des $a'_0, \ldots, a'_m \in A$. Si $a = \mathrm{PGCD}(a'_0, \ldots, a'_m)$, on a bien $P = \frac{a}{b}\tilde{P}$ avec $\tilde{P} \in A[X]$ primitif, et quite à simplifier la fraction $\frac{a}{b}$, on peut supposer a, b premier entre eux.

Soit maintenant $P \in A[X]$ avec $P = QR$ pour $Q, R \in K[X]$. Ecrivons $Q = \frac{a}{b}\tilde{Q}$ et $R = \frac{c}{d}\tilde{R}$, avec $a, c \in A$, $b, d \in A^*$, et $\tilde{Q}, \tilde{R} \in A[X]$ primitifs. Alors $bdc(Q) \sim ac$, donc $\frac{ac}{bd} \in A$, et on a bien $P = (\frac{ac}{bd}\tilde{Q})\tilde{R}$, avec les deux termes dans $A[X]$. L'assertion sur les degrés est immédiate. □

Lemme E.5. Soit A un anneau factoriel et $K = \mathrm{Fr}(A)$. Soit $P \in A[X]$ irréductible dans $A[X]$. Le morphisme d'anneau $\bar{i} : A[X]/(PA[X]) \longrightarrow K[X]/(PK[X])$ induit par l'injection $i : A \hookrightarrow K$, est injectif.

Preuve. Soit $Q \in A[X]$ tel que $Q \in PK[X]$ (la classe de Q appartient à $\mathrm{Ker}(\bar{i})$). Soit $R \in K[X]$ tel que $Q = PR$. Ecrivons $R = \frac{a}{b}\tilde{R}$ comme dans le lemme précédent et $Q = c\tilde{Q}$ avec $c = c(Q)$, $c(\tilde{Q}) \sim 1$. Alors

$$cb\tilde{Q} = bQ = bPR = aP\tilde{R} \Rightarrow c(cb\tilde{Q}) = c(aP\tilde{R}) \Rightarrow cb \sim ac(P) \sim a$$

(P irréductible dans $A[X] \Rightarrow c(P) \sim 1$). Ainsi $b|a$ et $\frac{a}{b} \in A$, d'où $R \in A[X]$ et $Q = PR \in PA[X]$. □

Proposition E.6. Soit A un anneau factoriel et $K = \mathrm{Fr}(A)$. Les polynômes $P \in A[X]$, irréductibles dans $A[X]$, sont

1. Les constantes $p \in A$ irréductibles dans A ;
2. Les polynômes $P \in A[X]$ de degré ≥ 1 primitifs et irréductibles dans $K[X]$.

Preuve. (a) On vérifie d'abord que ces éléments sont bien irréductibles dans $A[X]$. Soit $p \in A$ un irréductible de A. Alors $p \notin U(A[X]) = U(A)$, et si $p = P(X)Q(X)$, alors $\deg(P) = 0 = \deg(Q)$, donc $P(X) \in A$ et $Q(X) \in A$, et donc $p \in U(A) = U(A[X])$ ou $Q \in U(A) = U(A[X])$: p est bien irréductible dans $A[X]$.

Soit $P \in A[X]$ de degré ≥ 1 primitif et irréductible dans $K[X]$. P n'est pas inversible dans $A[X]$ car de degré ≥ 1. Si $P(X) = Q(X)R(X)$, avec $Q, R \in A[X]$, c'est aussi une écriture dans $K[X]$, donc $\deg(Q) = 0$ ou $\deg(R) = 0$. Par exemple $Q = a \in A^*$, et $P = aR$. Alors $1 = c(P) \sim ac(R)$, donc $a \in U(A) = U(A[X])$. Donc P est bien irréductible dans $A[X]$.

(b) On montre maintenant que ce sont les seuls éléments irréductibles de $A[X]$. Soit $P \in A[X]$, irréductible dans $A[X]$. Si $\deg(P) = 0$, on a $P = a \in A$, qui est irréductible dans A.

Supposons donc $\deg(P) \geq 1$. Alors $c(P) \sim 1$. Montrons que P est irréductible dans $K[X]$. On sait déjà qu'il est non inversible. Supposons que $P = QR$, avec $Q, R \in K[X]$. Alors par le deuxième lemme il existe $\tilde{Q}, \tilde{R} \in A[X]$ tels que $P = \tilde{Q}\tilde{R}$, $\deg(\tilde{Q}) = \deg(Q)$ et $\deg(\tilde{R}) = \deg(R)$. Comme P est irréductible dans $A[X]$, on a $\tilde{Q}$ ou $\tilde{R}$ inversible dans $A[X]$, en particulier $\deg(\tilde{Q}) = 0 = \deg(Q)$ ou $\deg(\tilde{R}) = 0 = \deg(R)$, donc Q ou R est inversible dans $K[X]$. □

Preuve du théorème de Gauss. 1) Montrons tout d'abord que tout polynôme primitif non nul $P \in A[X]$ s'écrit comme produit d'un inversible et d'irréductibles de $A[X]$. On procède par récurrence sur P. Si $\deg(P) = 0$, alors $P \in U(A)$ (P primitif), ce qui donne le résultat.

Supposons que $\deg(P) = n > 0$ et le résultat montré pour les polynômes primitifs de degré $< n$. Si P irréductible, on a le résultat. Sinon, comme P n'est pas inversible, on a $P = fg$ avec $f, g \in A[X]$ non inversibles primitifs. Si $0 < \deg(f) < \deg(P)$ et $0 < \deg(g) < \deg(P)$, l'hypothèse de récurrence donne le résultat. Si on a $\deg(f) = \deg(P)$ et $\deg(g) = 0$, alors $g = a \in A$, et $P = af$. On a $1 = c(P) \sim ac(f)$, donc $g = a \in U(A)$, impossible. On a donc le résultat.

Si $P \in A[X]$ est non nul, alors $P = c(P)\tilde{P}$ avec $\tilde{P} \in A[X]$ primitif. la factorialité de A, le fait que les irréductibles de A le sont encore dans $A[X]$ et le cas primitif assurent que l'axiome (E) est vérifié dans A.

2) $A[X]$ étant intègre et l'axiome (E) étant démontré dans $A[X]$, il reste à voir que pour $P \in A[X]$, alors P irréductible entraine (P) idéal premier de $A[X]$. Soit donc $P \in A[X]$ irréductible.

Supposons $P = p \in A$. On a un isomorphisme d'anneaux $A/(p)[X] \simeq A[X]/(p)$ (voir chapitre 3). Comme p est irréductible dans A et A est factoriel, alors (p) est un idéal premier de A et $A/(p)$ est intègre, ainsi que $A/(p)[X]$ et $A[X]/(p)$. Donc $(p) = pA[X]$ est un idéal premier de $A[X]$.

Supposons maintenant que $\deg(P) \geq 1$. Alors $c(P) = 1$ et P est irréductible dans $K[X]$ (proposition précédente). Alors $K[X]$ factoriel implique que $K[X]/PK[X]$ intègre. Le dernier lemme assure que $A[X]/PA[X]$ est isomorphe à un sous-anneau de $K[X]/PK[X]$, donc est lui-même intègre, et ainsi $PA[X]$ est un idéal premier. □

Une récurrence immédiate à partir du théorème de Gauss donne le résultat suivant.

Corollaire E.7. Si A est un anneau factoriel, alors $A[X_1, \ldots, X_n]$ est un anneau factoriel.

Pour finir le paragraphe, on propose une application des divers résultats rencontrés dans le chapitre. Si $P \in k[X,Y]$ (k corps), on dit que l'ensemble $V(P) = \{(x,y) \in k^2 \mid P(x,y) = 0\}$ est une courbe algébrique plane. On va montrer que l'intersection de deux courbes algébriques planes sans composante commune est finie, ce qui est formalisé par le résultat suivant.

Proposition E.8. Soient $P, Q \in k[X,Y]$ premiers entre eux. Alors l'ensemble $V(P) \cap V(Q)$ est fini.

On commence par un lemme.

Lemme E.9. Soit A un anneau factoriel de corps de fractions K, et soient $P, Q \in A[X]$. Si P et Q sont premiers entre eux dans $A[X]$, alors ils sont premiers entre eux dans $K[X]$.

Preuve. Soit $D \in K[X]$ un diviseur commun à P et Q dans $K[X]$: on a $P = DR$ et $Q = DS$ pour $R, S \in K[X]$. On sait alors par un lemme précédent (et sa preuve) qu'il existe $\tilde{D}$, $\tilde{R}$, $\tilde{S} \in A[X]$ tels que $P = \tilde{D}\tilde{R}$ et $Q = \tilde{D}\tilde{S}$ avec préservation des degrés en passant à $\tilde{}$. Comme P, Q sont premiers dans $A[X]$ on a $\deg(\tilde{D}) = 0 = \deg(D)$, d'où $D \in k^* = U(k[X])$. □

Preuve de la proposition. Posons

$$U = \{x \in k \mid \exists y \in k \text{ tq } P(x,y) = 0 = Q(x,y)\}, V = \{y \in k \mid \exists x \in k \text{ tq } P(x,y) = 0 = Q(x,y)\}$$

On a $V(P) \cap V(Q) \subset U \times V$, il suffit donc de voir que U et V sont finis.

Comme P et Q sont premiers entre eux dans $k[X,Y] = k[X][Y]$, le lemme assure qu'ils le sont aussi dans $k(X)[Y]$, qui est principal, il existe donc $A, B \in k(X)$ tel que $1 = AP + BQ$. Soit $D \in k[X]$ (non nul) tel que $DA, DB \in k[X]$. On a alors $D = (DA)P + (DB)Q$. Si $x \in U$, on a $D(x) = 0$, et cela montre, comme D est non nul et n'a donc qu'un nombre fini de racines, que U est fini. Le raisonnement symétrique montre que V est fini, et on a donc le résultat. □

F Critères d'irréductibilité des polynômes

On démontre dans ce paragraphe divers critères d'irréductibilité des polynômes. La première chose à faire est de s'intéresser à leurs racines. On rappelle tout d'abord le résultat bien connu suivant. La preuve est laissée en exercice.

Proposition F.1. Soit k un corps.

1. Les polynômes $(X - a)$, $a \in k$, sont irréductibles dans $k[X]$.
2. Soit $P \in k[X]$ irréductible de degré > 1. Alors P n'a pas de racine dans k.
3. Soit $P \in K[X]$ avec $\deg(P) = 2, 3$. Alors P est irréductible $\iff$ P n'a pas de racine dans k.

Rappelons qu'un corps k est **algébriquement clos** si tout polynôme non constant $P \in k[X]$ admet une racine dans k. Le résultat qui suit est une conséquence immédiate du précédent.

Proposition F.2. Soit k un corps algébriquement clos. Les polynômes irréductibles de $k[X]$ sont les polynômes de la forme $\lambda(X-a)$, $\lambda, a \in k$, $\lambda \neq 0$.

Proposition F.3 (test des racines entières)**.** Soit A un anneau factoriel et $K = \mathrm{Fr}(A)$. Soit $P \in A[X]$, $P = a_n X^n + \cdots + a_1 X + a_0$. Soit $\frac{p}{q} \in K$, avec p et q premiers entre eux, une racine de P. Alors $p|a_0$ et $q|a_n$.

Preuve. On a $0 = a_n \frac{p^n}{q^n} + \cdots + a_1 \frac{p}{q} + a_0$, d'où $-a_0 q^n = p(a_n p^{n-1} + \cdots + a_1 q^{n-1})$ et $p|a_0 q^n$. Le lemme de Gauss assure alors que $p|a_0$. D'autre part $-a_n p^n = q(a_{n-1} p^{n-1} + \cdots + a_1 p q^{n-1} + a_0 q^{n-1})$ et donc à nouveau par le lemme de Gauss on a $q|a_n$. □

Exemple F.4. Soit $P = X^3 - X + 1 \in \mathbb{Z}[X]$. D'après la proposition précédente, les seules racines possibles de P dans $\mathbb{Q}$ sont 1 et -1, qui ne sont pas racines. Ainsi P est irréductible dans $\mathbb{Q}[X]$ (il est de degré 3), et aussi dans $\mathbb{Z}[X]$ car il est primitif.

Théorème F.5 (Critère d'Eisenstein)**.** Soit A un anneau factoriel et $K = \mathrm{Fr}(A)$. Soit $P \in A[X]$, $P = a_n X^n + \cdots + a_1 X + a_0$ ($n = \deg(P) \geq 2$), et soit $p \in A$, irréductible. On suppose :

1. $p \not| a_n$;
2. $p|a_i$, $i = 0, \ldots n-1$;
3. $p^2 \not| a_0$.

Alors P est irréductible dans $K[X]$ (et aussi dans $A[X]$ si $\mathrm{PGCD}(a_n, \ldots, a_0) = 1$).

Preuve. Supposons que P n'est pas irréductible dans $K[X]$: il existe alors $Q, R \in A[X]$ tels que $P = QR$ et $0 < \deg(Q) < \deg(P)$ et $0 < \deg(R) < \deg(P)$ (voir un lemme dans le paragraphe précédent). Posons

$$Q = \sum_{i=0}^{q} b_i X^i,\ R = \sum_{j=0}^{r} c_j X^j,\ b_i, c_j \in A,\ q, r \in \mathbb{N},\ q + r = n$$

Comme A est factoriel, on a p irréductible $\Rightarrow$ (p) premier $\Rightarrow$ l'anneau $B = A/(p)$ est intègre. Projetons l'égalité $P = QR$ dans $B[X]$, on a

$$\overline{a_n} X^n = (\sum_{i=0}^{q} \overline{b_i} X^i)(\sum_{j=0}^{r} \overline{c_j} X^j)$$

On a $\overline{a_n} \neq 0$ dans B, donc $\overline{b_q} \neq 0$ et $\overline{c_q} \neq 0$. Cette égalité dans $B[X]$ est encore vraie dans $L[X]$, où L est le corps des fractions de l'anneau intègre B. Comme $L[X]$ est factoriel et X est irréductible dans $L[X]$, l'unicité de la décomposition en produit d'irréductibles donne en particulier $\overline{b_0} = \overline{0} = \overline{c_0}$, donc $p|b_0$ et $p|c_0$, donc $p^2|b_0 c_0 = a_0$: c'est une contradiction. □

Exemples F.6.

1. Soit p un nombre premier. Alors le polynôme $P(X) = X^{p-1} + X^{p-1} + \cdots + X + 1$ est irréductible dans $\mathbb{Q}[X]$, et aussi dans $\mathbb{Z}[X]$ (étudier $P(X+1)$).
2. Soit $a \in \mathbb{Z}$ tel qu'il existe p premier satisfaisant $p|a$ et $p^2 \not| a$. Alors pour $n \geq 1$, le polynôme $X^n - a$ est irréductible dans $\mathbb{Q}[X]$.

3. $P(X) = X^5 - 4X + 2$ est irréductible dans $\mathbb{Q}[X]$.
4. Pour $n \geq 1$, $X^n - Y$ est un élément irréductible de $\mathbb{Z}[X, Y]$.

Théorème F.7 (Critère d'irréductibilité par réduction)**.** Soit A un anneau factoriel et $K = \mathrm{Fr}(A)$. Soit I un idéal maximal de A et $L = A/I$. Soit $P \in A[X]$, $P = a_n X^n + \cdots + a_1 X + a_0$ ($n = \deg(f) \geq 2$). Notons $\overline{P}$ la réduction de P modulo I : $\overline{P} \in L[X]$. On suppose que $a_n \notin I$. Si $\overline{P}$ est irréductible dans $L[X]$, alors P est irréductible dans $K[X]$.

Preuve. Supposons que P n'est pas irréductible dans $K[X]$: il existe alors $Q, R \in A[X]$ tels que $P = QR$ et $0 < \deg(Q) < \deg(P)$ et $0 < \deg(R) < \deg(P)$ (voir un lemme dans le paragraphe précédent). Posons

$$Q = \sum_{i=0}^{q} b_i X^i,\ R = \sum_{j=0}^{r} c_j X^j,\ b_i, c_j \in A,\ q, r \in \mathbb{N},\ q + r = n$$

Notons $\overline{P} \in L[X]$ la réduction de P modulo I. On a $\overline{P} = \overline{QR}$ dans $L[X]$, et $\overline{a_n} \neq \overline{0}$ implique que $\overline{b_q} \neq 0$ et $\overline{c_r} \neq \overline{0}$. Comme P est irréductible dans $L[X]$, alors $\overline{Q}$ ou $\overline{R}$ est de degré 0, et Q ou R est de degré 0 dans $A[X]$: contradiction. □

Exemple F.8. $135X^3 + 222X^2 - 124X + 424678$ est irréductible dans $\mathbb{Q}[X]$ (réduire modulo 3).

On consultera [Perrin] pour d'autres critères d'irréductibilité.

G Polynômes cyclotomiques et applications

Dans ce paragraphe on étudie une classe importante de polynômes à coefficients entiers : les polynômes cyclotomiques. On montre leur irréductibilité et on présente quelques applications.

G.1 Généralités

Soit $n \in \mathbb{N}^*$ et soit $\mu_n = \{z \in \mathbb{C} : z^n = 1\}$ le groupe des racines n-ièmes de l'unité. On rappelle que μ_n est un groupe cyclique d'ordre n et qu'une racine n-ième de l'unité ω est dite primitive si ω engendre le groupe μ_n. L'ensemble des racines primitives n-ièmes est noté μ_n^*. Rappelons également que si $\omega \in \mu_n^*$ et $k \in \mathbb{Z}$, alors $\omega^k \in \mu_n^*$ si et seulement si $\mathrm{PGCD}(k, n) = 1$, et que $|\mu_n^*| = \varphi(n)$ où φ est la fonction indicatrice d'Euler.

Si $\omega \in \mu_n^*$, on se propose de déterminer le degré $[\mathbb{Q}(\omega) : \mathbb{Q}]$ (les corps du type $\mathbb{Q}(\omega)$ sont appelés **corps cyclotomiques**). Il faut donc trouver le polynôme minimal de ω sur $\mathbb{Q}$.

Définition G.1. *Pour $n \in \mathbb{N}^*$, Le n-**ième polynôme cyclotomique** $\Phi_n(X) \in \mathbb{C}[X]$ est défini par*

$$\Phi_n(X) = \prod_{\xi \in \mu_n^*} (X - \xi)$$

On constate que

$$\Phi_1(X) = X - 1,\ \Phi_2(X) = X + 1,\ \Phi_3(X) = X^2 + X + 1,\ \Phi_4(X) = X^2 + 1$$

et si p est un nombre premier

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$$

Proposition G.2. On a
$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Preuve. Ces deux polynômes ont même coefficient dominant et les mêmes racines, qui sont simples. On en déduit donc qu'ils sont égaux. □

Proposition G.3. On a $\Phi_n(X) \in \mathbb{Z}[X]$.

Preuve. On procède par récurrence, le résultat étant clair pour $n = 1, 2, 3$, et connu pour n premier. Supposons $n > 3$ et le résultat montré pour les entiers $< n$. Si n est premier on connait déjà le résultat. Sinon on a $X^n - 1 = \prod_{d|n, d<n} \Phi_d(X)\Phi_n(X)$. Par hypothèse de récurrence $B(X) = \prod_{d|n, d<n} \Phi_d(X)$ appartient à $\mathbb{Z}[X]$. Il existe alors $Q, R \in \mathbb{Z}[X]$ tels que $X^n - 1 = QB + R$ avec $R = 0$ ou $\deg(R) < \deg(B)$. Alors comme $X^n - 1 = \Phi_n B$, on a $B(\Phi_n - Q) = R$. Si $\Phi_n \neq Q$, on trouve $\deg(R) \geq \deg(B)$, une contradiction. Donc $\Phi_n = Q \in \mathbb{Z}[X]$. □

Théorème G.4. Pour tout $n \in \mathrm{N}^*$, le polynôme $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$ (et donc aussi dans $\mathbb{Z}[X]$), et est le polynôme minimal de tout racine primitive n-ième de l'unité $\omega \in \mu_n^*$. Ainsi on a $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$.

Preuve. On commence par un lemme.

Lemme G.5. Soient A un anneau factoriel et $K = \mathrm{Fr}(A)$. Soit $P \in A[X]$ un polynôme unitaire. On suppose que $P = QR$ où $Q, R \in K[X]$ et Q est unitaire. Alors $Q, R \in A[X]$ et que R est unitaire.

Preuve du lemme. Exercice, cela se démontre en utilisant les techniques du paragraphe E. □

Soit ω une racine primitive n-ième de l'unité et soit $f \in \mathbb{Q}[X]$ le polynôme minimal de ω sur $\mathbb{Q}$. Le lemme assure que $f \in \mathbb{Z}[X]$ et que $X^n - 1 = f(X)h(X)$ où $h(X) \in \mathbb{Z}[X]$ est un polynôme unitaire.

On a $\Phi_n(\omega) = 0$ donc $f | \Phi_n$ dans $\mathbb{Q}[X]$. On veut montrer que $f = \Phi_n$. Il suffit pour cela de voir que toute racine primitive n-ième de l'unité est une racine de f (en effet, les racines de Φ_n étant simples, on aura alors $\Phi_n | f$ et $f = \Phi_n$ sera irréductible).

Pour un entier $k \in \mathbb{N}$, notons $l(k)$ la longueur de k, c'est-à-dire le nombre de facteurs premiers intervenant dans sa décomposition en produit de nombres premiers. Si ω' est une racine primitive n-ième de l'unité, il existe $k \in \mathbb{N}^*$ premier avec n tel que $\omega' = \omega^k$. Montrons par récurrence sur $l(k)$ que ω' est une racine de f.

Le cas $l(k) = 0$ ($k = 1$) est immédiat. Supposons donc que $l(k) = 1$, c'est-à-dire que $k = p$ est un nombre premier ne divisant pas n. Supposons que ω^p n'est pas une racine de f. Alors $h(\omega^p) = 0$, et donc ω est une racine de $h(X^p)$. Il existe donc (lemme) $g \in \mathbb{Z}[X]$ tel que $h(X^p) = f(X)g(X)$. Dans $\mathbb{F}_p[X] = \mathbb{Z}/p\mathbb{Z}[X]$, on a $P(X^p) = P(X)^p$ pour tout polynôme $P \in \mathbb{F}_p[X]$. On obtient donc dans $\mathbb{F}_p[X]$, $\overline{h}(X^p) = \overline{h}(X)^p = \overline{f}(X)\overline{g}(X)$. Soit $\psi \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{f}(X)$. Alors ψ divise $\overline{h}(X)^p$, et comme il est irréductible, il divise $\overline{h}(X)$. Ainsi ψ^2 divise $\overline{f}(X)\overline{h}(X) = X^n - \overline{1}$, et $X^n - \overline{1}$ a

une racine multiple, ce qui n'est pas vrai car $(X^n - \overline{1})' = nX^{n-1}$ est non nul et n'admet que 0 pour racine ($p \not| n$) : on donc une contradiction, et ω^p est une racine de f.

Supposons maintenant que $l(k) > 1$ et le résultat montré pour tous les entiers k' premiers avec n tels $l(k') < l(k)$. On peut écrire $k = pk'$ où p est un nombre premier ne divisant pas n, k' est un entier premier avec n tel que $l(k') < l(k)$. Alors $\omega^{k'}$ est une racine primitive n-ième de l'unité, et est par hypothèse de récurrence, une racine de f, qui est donc son polynôme minimal. Le cas $l(k) = 1$ assure alors que $(\omega^{k'})^p$ est une racine de f, ce qui donne le résultat. □

G.2 Le théorème de Wedderburn

On se propose maintenant de démontrer le résultat suivant.

Théorème G.6 (Wedderburn)**.** Tout corps fini est commutatif.

On commence par un lemme élémentaire.

Lemme G.7. Soient $q, d, n \in \mathbb{N}^*$ avec $q \geq 2$. Alors $(q^d - 1)|(q^n - 1) \iff d|n$.

Preuve. Supposons d'abord que $n = ad$ avec $a \in \mathbb{N}^*$. Alors

$$(q^d)^a - 1 = (q^d - 1)(1 + q^d + \ldots + q^{d(a-1)}) \quad (*)$$

ce qui montre que $(q^d - 1)|(q^n - 1)$. Réciproquement, supposons que $(q^d - 1)|(q^n - 1)$: alors $d \leq n$ et on peut écrire $n = ad + r$ avec $a \in \mathbb{N}^*$ et r un entier tel que $0 \leq r < d$ (division euclidienne de n par d). il existe donc $\lambda \in \mathbb{N}^*$ tel que

$$q^n - 1 = q^{ad+r} - 1 = \lambda(q^d - 1). \quad (**)$$

On retranche alors $(*)$ à $(**)$ pour trouver que $q^d - 1$ divise $q^{ad+r} - q^{ad} = q^{ad}(q^r - 1)$. Comme q et $q^d - 1$ sont premiers entre eux (Bezout par exemple), on a aussi que q^{ad} et $q^d - 1$ sont premiers entre eux, et ainsi si $r \neq 0$, on a $(q^d - 1)|(q^r - 1)$ par le lemme de Gauss, et donc $d \leq r$: contradiction. Donc $r = 0$ et $d|n$. □

Lemme G.8. Soient $n, q \in \mathbb{N}^*$ avec $n, q \geq 2$.
i) Soit $d \in \mathbb{N}^*$ tel que $d|n$ et $d < n$. Alors $\Phi_n(q)$ divise $\frac{q^n-1}{q^d-1}$ (cf. lemme précédent).
ii) On a $|\Phi_n(q)| > q - 1$.

Preuve. i) On a

$$q^n - 1 = \prod_{m|n} \Phi_m(q) \quad \text{et} \quad q^d - 1 = \prod_{m|d} \Phi_m(q).$$

Donc en divisant ces expressions on obtient

$$\frac{q^n - 1}{q^d - 1} = \prod_{m|n, m\not|d} \Phi_m(q).$$

Ainsi puisque $d < n$, on trouve que $\Phi_n(q)$ divise $\frac{q^n-1}{q^d-1}$.

ii) Pour $\xi \in \mu_n^*$, comme $n > 1$, on a toujours $|q - \xi| > q - 1$ pour un entier $q \geq 2$ (faire un dessin). Ainsi si $\Phi_n(X) = (X - \xi_1) \ldots (X - \xi_l)$, on a

$$|\Phi_n(q)| = |q - \xi_1| \ldots |q - \xi_l| > (q - 1)^l \geq q - 1. \square$$

Démonstration du théorème de Wedderburn. Soit K un corps fini et soit Z son centre :

$$Z = \{a \in K \mid ax = xa,\ \forall x \in K\}.$$

Alors Z est un sous-corps de K (facile à vérifier), commutatif et de cardinal $q \geq 2$ ($0, 1 \in Z$). Comme k est un Z-espace vectoriel de dimension finie, on a donc $|K| = q^n$ pour un entier $n \in \mathbb{N}^*$. Alors K est commutatif $\iff n = 1$.

Le groupe multiplicatif K^* opère sur lui même par automorphismes intérieurs :

$$\begin{aligned} K^* \times K^* &\longrightarrow K^* \\ (a, x) &\longmapsto axa^{-1} \end{aligned}$$

Pour $x \in K^*$, posons

$$K_x = \{a \in K \mid ax = xa\}.$$

Il est facile de vérifier que K_x est un sous-corps de K, qui contient Z, et donc il existe $d_x \in \mathbb{N}$ tel que $K_x = q^{d_x}$. De plus il est clair que $K_x^* = \mathrm{Stab}_{K^*}(x)$. Par conséquent $q^{d_x} - 1 = |K_x^*|$ divise $|K^*| = q^n - 1$. on peut appliquer le premier lemme : on a $d_x | n$. Considérons l'orbite $\Omega(x)$ de x. On a $|\Omega(x)| = \frac{q^n - 1}{q^{d_x} - 1}$.

Supposons maintenant que le corps K n'est pas commutatif : il existe alors des éléments $x \in K^*$ tels que $x \notin Z$, ce qui revient à dire que l'orbite $\Omega(x)$ n'est pas réduite à un point ou encore que $d_x < n$. On écrit alors l'équation aux classes :

$$|K^*| = q^n - 1 = |Z^*| + \sum_{i=1}^{r} |\Omega(x_i)| = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{d_{x_i}} - 1}$$

où les x_i sont des représentants des orbites distinctes non réduites à un point. La partie i) du deuxième lemme assure alors que $\Phi_n(q)$ divise $q - 1$ et donc que $|\Phi_n(q)| \leq q - 1$, ce qui contredit la partie ii) de ce même lemme. On conclut donc que K est commutatif. □

G.3 Version faible du théorème de la progression arithmétique

On va montrer maintenant le résultat suivant, toujours en utilisant les polynômes cyclotomiques.

Théorème G.9. Soit $n \geq 2$ un entier. Il existe une infinité de nombre premiers p tels que $p \equiv 1 \bmod n$.

C'est un cas particulier du théorème de la progression arithmétique de Dirichlet, qui affirme que si $a, n \in \mathbb{N}^*$ sont premiers entre eux, alors il existe une infinité de nombres premiers p tels que $p \equiv a \bmod n$.

Lemme G.10. Soit $n \geq 2$ et soit p un nombre premier tel que $p \not| n$. Soit $a \in \mathbb{Z}$. Alors

$$p | \Phi_n(a) \iff [\overline{a} \in U(\mathbb{Z}/p\mathbb{Z}) \text{ et } \overline{a} \text{ est d'ordre } n \text{ dans } U(\mathbb{Z}/p\mathbb{Z})]$$

Preuve. Supposons que $a^n \equiv 1 \pmod p$. Alors p divise $a^n - 1 = \prod_{d|n} \Phi_d(a)$ et p étant premier, il existe d un diviseur de n tel que $p | \Phi_d(a)$. Alors $p | (a^d - 1)$ d'où $a^d \equiv 1 \pmod p$. Donc si $\overline{a} \in U(\mathbb{Z}/p\mathbb{Z})$ et $\overline{a}$ est d'ordre n dans $U(\mathbb{Z}/p\mathbb{Z})$, on a $p | \Phi_n(a)$ (si le d trouvé précedemment est $< n$, on a $o(\overline{a}) < n$). Cela démontre le sens $\Leftarrow$ du théorème.

On suppose maintenant que $p | \Phi_n(a)$. Alors $a^n \equiv 1 \pmod p$ donc $\overline{a} \in U(\mathbb{Z}/p\mathbb{Z})$. Soit k l'ordre de $\overline{a}$ dans $U(\mathbb{Z}/p\mathbb{Z})$. La preuve du sens $\Leftarrow$ assure que $p | \Phi_k(a)$. Supposons que $k < n$. On a

$$a^n - 1 = \Phi_n(a)\Phi_k(a)l$$

où $l \in \mathbb{Z}$, donc p^2 divise $a^n - 1$. De même comme $a + p \equiv a \pmod{p}$, on a $p^2|((a+p)^n - 1)$. Alors

$$(a+p)^n \equiv a^n + nap \equiv 1 + nap \pmod{p^2}$$

et alors p^2 divise nap, une contradiction car $p \not| n$ et $p \not| a$. On a donc $k = n$. □.

Lemme G.11. Soit $n \in \mathbb{N}^*$ et soit p un nombre premier tel que $p \not| n$. Alors

$$p \equiv 1 (\mathrm{mod}\ n) \iff \exists a \in \mathbb{Z} \text{ tel que } p|\Phi_n(a)$$

Preuve. Si $p \equiv 1 \pmod{n}$, alors $n|p-1$. Le groupe $U(\mathbb{Z}/p\mathbb{Z})$ est cyclique d'ordre $p-1$, il contient donc un élément d'ordre n. Soit donc $a \in \mathbb{Z}$ tel que $\overline{a} \in U(\mathbb{Z}/p\mathbb{Z})$ et $\overline{a}$ est d'ordre n dans $U(\mathbb{Z}/p\mathbb{Z})$. Le lemme précédent assure que $p|\Phi_n(a)$.

Réciproquement s'il existe $a \in \mathbb{Z}$ tel que $p|\Phi_n(a)$, le lemme précédent assure l'existence d'un élément d'ordre n dans $U(\mathbb{Z}/p\mathbb{Z})$, et par le théorème de Lagrange on a $n|p-1$. □

Preuve du théorème. Soient $p_1, \ldots, p_r$ des nombres premiers tels que $\forall i$, $p_i \equiv 1 \pmod{n}$. On va montrer qu'il existe un nombre premier p tel que $\forall i$, $p \neq p_i$, et $p \equiv 1 \pmod{n}$. Cela montrera le théorème.

On pose $M = np_1 \cdots p_r$ (si $r = 0$, $M = n$). On a $|\Phi_n(M)| > 1$ car $n \geq 2$, et il existe donc un nombre premier p tel que $p|\Phi_n(M)$.

Le coefficient constant de $\Phi_n(X) \in \mathbb{Z}[X]$ est ± 1. On a donc

$$\Phi_n(M) \equiv \Phi_n(0) \equiv \pm 1 \pmod{n}$$

et donc n et $\Phi_n(M)$ sont premiers entre eux (Bezout). Ainsi $p \not| n$, et puisque $p|\Phi_n(M)$, on peut appliquer le lemme : $p \equiv 1 \pmod{n}$.

De même on a

$$\Phi_n(M) \equiv \Phi_n(0) \equiv \pm 1 \pmod{p_i},\ \forall i$$

ce qui montre que $\forall i$, p_i ne divise pas $\Phi_n(M)$, et donc $\forall i$, on a $p_i \neq p$. □

V Matrices à coefficients dans un anneau commutatif

Dans ce chapitre A est un anneau commutatif.

A Matrices

Soient $n, p \in \mathbb{N}^*$. On note $\mathcal{M}_{n,p}(A)$ l'ensemble des matrices $n \times p$ à coefficients dans A. C'est un A-module, pour les lois usuelles ($\forall (a_{ij}), (b_{ij}) \in \mathcal{M}_{n,p}(A)$)

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$$

$$a.(b_{ij}) = (ab_{ij})$$

Pour $(i,j) \in \{1,\dots,n\} \times \{1,\dots,p\}$, on note $E_{ij} \in \mathcal{M}_{n,p}(A)$ la matrice dont tous les coefficients sont nuls à l'exception de celui situé sur la i-ème ligne et la j-ème colonne, qui vaut 1. Toute matrice $M = (a_{ij}) \in \mathcal{M}_{n,p}(A)$ s'écrit de manière unique sous la forme $M = \sum_{i,j} a_{ij}E_{ij}$. Ainsi $\mathcal{M}_{n,p}(A)$ **est un A-module libre de rang** np.

Le produit usuel des matrices définit pour $n, p, q \in \mathbb{N}^*$, une application A-bilinéaire

$$\mathcal{M}_{n,p}(A) \times \mathcal{M}_{p,q}(A) \longrightarrow \mathcal{M}_{n,q}(A)$$

$$\big(M = (a_{ik}), N = (b_{kj})\big) \longmapsto MN = \left(\sum_{k=1}^{p} a_{ik}b_{kj}\right)$$

Pour $i \in \{1,\dots,n\}, j, k \in \{1,\dots,p\}, l \in \{1,\dots,q\}$, on a

$$E_{ij}E_{kl} = \delta_{jk}E_{il},$$

et cette formule définit totalement, par bilinéarité, le produit des matrices.

Lorsque $n = p$, $\mathcal{M}_n(A) = \mathcal{M}_{n,n}(A)$ est une A-algèbre, dont la multiplication est le produit des matrices. La matrice identité (unité pour le produit des matrices) est notée I_n. C'est une algèbre non commutative si $n \geq 2$.

On pose

$$\mathrm{GL}_n(A) = U(\mathcal{M}_n(A)) = \{M \in \mathcal{M}_n(A) \mid \exists M' \in \mathcal{M}_n(A) \text{ tq } MM' = I_n = M'M\}.$$

C'est un groupe pour la multiplication des matrices. Les matrices suivantes seront très utiles dans la suite.

Définition-Proposition A.1. Soit $a \in A$ et $i, j \in \{1,\dots,n\}$, avec $i \neq j$. La matrice

$$F_{ij}(a) := I_n + aE_{ij}$$

est inversible, d'inverse $F_{ij}(-a)$.

La vérification est immédiate.

B Centre et idéaux d'une algèbre de matrices

Dans ce paragraphe on se propose d'étudier quelques propriétés des algèbres de matrices : calcul de leur centre et description des idéaux (quand A est un corps).

Proposition B.1. On a $Z(\mathcal{M}_n(A)) = \{aI_n, a \in A\}$, d'où un isomorphisme d'anneaux $Z(\mathcal{M}_n(A)) \cong A$.

Le résultat est une conséquence immédiate du résultat plus précis suivant.

Proposition B.2. Soit $M \in \mathcal{M}_n(A)$. Les assertions suivantes sont équivalentes.

1. Il existe $a \in A$ tel que $M = aI_n$.
2. M commute avec les matrices E_{ij}, $\forall i \neq j$.
3. M commute avec les matrices $F_{ij}(1)$, $\forall i \neq j$.

Preuve. Comme la matrice identité I_n commute avec toutes les matrices et $F_{ij}(1) = I_n + E_{ij}$, il est clair que $(1) \Rightarrow (2)$ et que $(2) \Leftrightarrow (3)$. Il reste à voir que $(2) \Rightarrow (1)$. Soit $M = \sum_{k,l} a_{k,l} E_{kl}$ vérifiant (2). Fixons $i \neq j$. On a $ME_{ij} = \sum_k a_{ki} E_{kj}$ et $E_{ij}M = \sum_l a_{jl} E_{il}$, d'où $a_{ii} = a_{jj}$, et si $k \neq i$ et $l \neq j$, $a_{ki} = 0 = a_{jl}$. Ceci est vrai pour tout $i \neq j$, d'où le résultat. □

Proposition B.3. Supposons que $A = k$ est un corps. Alors les seuls idéaux bilatères de $\mathcal{M}_n(k)$ sont (0) et $\mathcal{M}_n(k)$.

Preuve. Soit $I \neq (0)$ un idéal de $\mathcal{M}_n(k)$. Supposons dans un premier temps qu'il existe i, j tels que $E_{ij} \in I$. Alors pour tous k, l, on a $E_{kl} = E_{ki} E_{ij} E_{jl} \in I$. Comme I est automatiquement un sous k-espace vectoriel, on en déduit que $J = \mathcal{M}_n(k)$.

Soit maintenant $M = \sum_{kl} a_{kl} E_{kl} \in I$ non nulle : il existe i, j tels que $a_{ij} \neq 0$. On a $E_{ii} M E_{jj} = a_{ij} E_{ij} \in I$, d'où $E_{ij} = a_{ij}^{-1} a_{ij} E_{ij} \in I$. On est ramené au cas précédent. □

Exercice. Si $I \subset A$ est un idéal, on note $\mathcal{M}_n(I)$ les matrices à coefficients dans I. Vérifier que $\mathcal{M}_n(I)$ est un idéal de $\mathcal{M}_n(A)$, et que tout idéal de $\mathcal{M}_n(A)$ est de cette forme.

Par contre $\mathcal{M}_n(A)$ admet toujours des idéaux à gauche.

Proposition B.4. Pour $i \in \{1, \ldots, \}$, notons $J_i \subset \mathcal{M}_n(A)$ l'ensemble des matrices dont les termes sont nuls en dehors de la i-ème colonne. Alors J_i est un idéal à gauche de $\mathcal{M}_n(A)$. De plus, en tant que $\mathcal{M}_n(A)$-module, on a $\mathcal{M}_n(A) = J_1 \oplus \cdots \oplus J_n$.

Preuve. On a $J_i = \sum_{l=1}^n A E_{li}$, et la vérification est un calcul facile. □

C Déterminant

Soit $M = (a_{ij}) \in \mathcal{M}_n(A)$, on pose

$$\det(M) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}$$

C'est le **déterminant** de M. Ceci définit une application $\det : \mathcal{M}_n(A) \longrightarrow A$.

On se propose de montrer le résultat suivant.

Théorème C.1 (Cramer). Soit $M \in \mathcal{M}_n(A)$. Alors

$$M \in \mathrm{GL}_n(A) \iff \det(M) \in U(A).$$

Exercice. Montrer le résultat si $n = 2$.

Schéma de la preuve. On verra plus loin que pour $M, N \in \mathcal{M}_n(A)$, on a $\det(MN) = \det(M)\det(N)$. Puisque $\det(I_n) = 1$, on en déduit aisément que $M \in \mathrm{GL}_n(A) \Rightarrow \det(M) \in U(A)$. La réciproque sera démontrée plus loin, avec en plus une formule pour le calcul de l'inverse de M si $\det(M) \in U(A)$. □

Notation-convention.

1. Soit E est un A-module libre de rang n et soit $\mathbf{e} = (e_1, \dots, e_n)$ une base de E. On a vu (Proposition C.3 du chapitre II) qu'il existe une unique forme n-linéaire alternée $\Delta : E^n \longrightarrow A$ telle que $\Delta(e_1, \dots, e_n) = 1$. Pour $(x_1, \dots, x_n) \in E^n$, avec $\forall i$, $x_i = \sum_j a_{ji} e_j$, on a
$$\Delta(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n} = \det(M), \text{ avec } M = (a_{ij})$$
On notera $\det_{\mathbf{e}}(x_1, \dots, x_n)$ cet élément de A.
2. Une matrice $M \in \mathcal{M}_n(A)$ est notée $(C_1, \dots, C_n)$ où $C_1, \dots, C_n$ sont les colonnnes de M. Ainsi le A-module libre $\mathcal{M}_n(A)$ de rang n^2 est vu comme le produit de n copies du module libre $\mathcal{M}_{n,1}(A)$ (de rang n et de base $\mathcal{E} = (E_{11}, \dots, E_{n1})$). Avec cette convention, $\det : \mathcal{M}_n(A) \longrightarrow A$ est une forme n-linéaire alternée, et $\det(M) = \det_{\mathcal{E}}(C_1, \dots, C_n)$.

Proposition C.2. Pour $M, N \in \mathcal{M}_n(A)$, on a

$$\det({}^tM) = \det(M) \quad \text{et} \quad \det(MN) = \det(M)\det(N)$$

Preuve. Ecrivons $M = (a_{ij})$. Pour $\sigma \in S_n$, on a

$$a_{\sigma(1)1} \cdots a_{\sigma(n)n} = a_{1\sigma^{-1}(1)} \cdots a_{n\sigma^{-1}(n)}$$

d'où

$$\det({}^tM) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma^{-1}(1)1} \cdots a_{\sigma^{-1}(n)n} = \det(M)$$

car $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$ pour tout $\sigma \in S_n$. Soient $M_1, \dots, M_n$ les colonnes de M. Si $N = (b_{ij})$, alors MN est la matrice dont les colonnes sont $C_1, \dots, C_n$ où $C_j = \sum_{l=1}^n b_{lj} M_l$. Alors on a

$$\det(MN) = \det_{\mathcal{E}}(C_1, \dots, C_n) = \left(\sum_{\sigma \in S_n} \varepsilon(\sigma) b_{\sigma(1)1} \cdots b_{\sigma(n)n} \right) \det_{\mathcal{E}}(M_1, \dots, M_n) = \det(N)\det(M)$$

ce qui donne le résultat. □

Définition C.3. *Soit $M = (a_{ij}) \in \mathcal{M}_n(A)$. Pour $i, j \in \{1, \dots, n\}$, soit $M_{ij} \in \mathcal{M}_{n-1}(A)$ la matrice obtenue à patir de A en effaçant la ligne i et la colonne j. L'élément $(-1)^{i+j} \det(M_{ij})$ est appelé le* ***cofacteur*** *(i, j) de M. On note $\widetilde{M} \in \mathcal{M}_n(A)$ la matrice dont les coefficients sont les cofacteurs de A.*

Théorème C.4 (Développement d'un déterminant suivant les lignes ou les colonnes)**.** Soit $M = (a_{ij}) \in \mathcal{M}_n(A)$. Pour chaque $i \in \{1, \dots, n\}$, on a

$$\det(M) = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det(M_{ik}) = \sum_{k=1}^{n} (-1)^{i+k} a_{ki} \det(M_{ki})$$

La première formule est le développement de $\det(M)$ suivant la ligne i, la deuxième formule est le développement de $\det(M)$ suivant la colonne i.

Preuve. Soit $\mathbf{e} = (e_1, \dots, e_n)$ la base canonique de A^n. Notons, pour $1 \leq i \leq n$, $v_i = \sum_{k=1}^{n} a_{ki} e_k$. On a $\det(M) = \det_{\mathbf{e}}(v_1, \dots, v_n)$. Pour $1 \leq k \leq n$, notons $\mathbf{f}_k = (e_k, e_1, \dots, e_{k-1}, e_{k+1}, \dots e_n)$. Posons également, pour $1 \leq k, j \leq n$,

$$N_{kj} = \begin{pmatrix} 1 & a_{k1} & \dots & a_{k,j-1} & a_{k,j+1} & \cdots & a_{k,n} \\ 0 & & & & & & \\ \vdots & & & M_{kj} & & & \\ 0 & & & & & & \end{pmatrix}$$

On a $\det(M_{kj}) = \det(N_{kj})$. D'autre part on a $\det(N_{kj}) = \det_{\mathbf{f}_k}(e_k, v_1, \dots, \widehat{v_j}, \dots v_n)$. Posons

$$\begin{aligned} \alpha_{kj} &= \det_{\mathbf{e}}(v_1, \dots, v_{j-1}, e_k, v_{j+1}, \dots, v_n) \\ &= (-1)^{j-1} \det_{\mathbf{e}}(e_k, v_1, \dots, \widehat{v_j}, \dots, v_n) = (-1)^{j-1}(-1)^{k-1} \det_{\mathbf{f}_k}(e_k, v_1, \dots, \widehat{v_j}, \dots, v_n) \end{aligned}$$

La dernière identité est obtenue en utilisant le fait que pour $\sigma \in S_n$, si on note $\sigma.\mathbf{e}$ la base $(e_{\sigma(1)}, \dots, e_{\sigma(n)})$, on a $\det_{\sigma.\mathbf{e}}(v_1, \dots, v_n) = \varepsilon(\sigma) \det_{\mathbf{e}}(v_1, \dots, v_n)$. La multilinéarité du déterminant assure que

$$\det(M) = \det_e(v_1, \dots, v_n) = \sum_{k=1}^{n} a_{kj} \alpha_{kj} = \sum_{k=1}^{n} a_{kj} (-1)^{k+j} \det(M_{kj})$$

Ceci donne la deuxième formule, et la première est obtenue par transposition. □

Théorème C.5 (Formule pour l'inverse d'une matrice)**.** Soit $M = (a_{ij}) \in \mathcal{M}_n(A)$. On a

$$M {}^t\widetilde{M} = \det(M) I_n = {}^t\widetilde{M} M$$

et M est inversible si et seulement si $\det(M) \in U(A)$.

Preuve. Soient $1 \leq l \neq j \leq n$ Soit $N = (a'_{ki})$ la matrice obtenue à partir de M en remplaçant la colonne j par la colonne l : $a'_{ki} = a_{ki}$ si $i \neq j$ et $a'_{kj} = a_{kl}$. Comme N a deux colonnes identiques on a $\det(N) = 0$. D'autre part pour tout k on a $\det(M_{kj}) = \det(N_{kj})$. Alors la formule précédente donne

$$0 = \det(N) = \sum_{k=1}^{n} a'_{kj} (-1)^{k+j} \det(N_{kj}) = \sum_{k=1}^{n} a_{kl} (-1)^{k+j} \det(M_{kj})$$

Ceci, combiné avec la formule précédente pour $\det(M)$, donne $\det(M) I_n = {}^t\widetilde{M} M$. L'autre partie de la formule s'obtient par transposition. La dernière assertion est immédiate. □

D Application aux endomorphismes d'un module libre

De même que pour les application linéaires entre espaces vectoriels, les applications linéaires entre modules libres sont déterminées par les matrices associées.

Définition D.1. *Soient E et E' des A-modules libres de rangs respectifs n et p et de base respectives $\mathcal{B} = \{e_1, \ldots, e_n\}$ et $\mathcal{B}' = \{e'_1, \ldots, e'_n\}$. Soit $u \in \mathrm{Hom}_A(E, E')$. **La matrice de u relativement aux bases $\mathcal{B}$ et $\mathcal{B}'$** est la matrice $M_{\mathcal{B},\mathcal{B}'}(u) = (\alpha_{ji}) \in \mathcal{M}_{p,n}(A)$ définie par*

$$u(e_i) = \sum_{j=1}^{p} \alpha_{ji} e'_j, \forall i \in \{1, \ldots, n\}$$

Lorsque $E = E'$ et $\mathcal{B} = \mathcal{B}'$, on note $M_{\mathcal{B},\mathcal{B}}(u) = M_{\mathcal{B}}(u)$, c'est la matrice de u relativement à la base $\mathcal{B}$ (ou dans la base $\mathcal{B}$).

Réciproquement, la donnée d'une matrice $M \in \mathcal{M}_{p,n}(A)$ détermine une unique application linéaire $E \longrightarrow E'$.

Proposition D.2. Soient E et E' des A-modules libres de rangs respectifs n et p et de bases respectives $\mathcal{B}$ et $\mathcal{B}'$. L'application

$$\begin{aligned} \mathrm{Hom}_A(E, E') &\longrightarrow \mathcal{M}_{p,n}(A) \\ u &\longmapsto M_{\mathcal{B},\mathcal{B}'}(u) \end{aligned}$$

est un isomorphisme A-linéaire.

Preuve. Exercice □

Proposition D.3. Soient E, E' et E'' des A-modules libres de rangs respectifs n, p et r et de base respectives $\mathcal{B}$, $\mathcal{B}'$ et $\mathcal{B}''$. Pour $u \in \mathrm{Hom}_A(E, E')$ et $v \in \mathrm{Hom}_A(E', E'')$, on a

$$M_{\mathcal{B},\mathcal{B}''}(v \circ u) = M_{\mathcal{B}',\mathcal{B}''}(v) M_{\mathcal{B},\mathcal{B}'}(u)$$

Preuve. Exercice □

Corollaire D.4. Soient E et E' des A-modules libres de rangs respectifs n et p et de base respectives $\mathcal{B}$ et $\mathcal{B}'$. Soit $u \in \mathrm{Hom}_A(E, E')$. Alors u est un isomorphisme si et seulement si la matrice $M_{\mathcal{B},\mathcal{B}'}(u)$ est inversible (et dans ce cas nécessairement $n = p$).

Corollaire D.5. Soit E un A-module libre de rang n et de base $\mathcal{B}$. L'application

$$\begin{aligned} \mathrm{End}_A(E) &\longrightarrow \mathcal{M}_n(A) \\ u &\longmapsto M_{\mathcal{B}}(u) \end{aligned}$$

est un isomorphisme de A-algèbres. En particulier u est un isomorphisme si et seulement si $M_{\mathcal{B}}(u) \in \mathrm{GL}_n(A)$. Cette application induit en particulier un isomorphisme de groupes $\mathrm{Aut}_A(E) \cong \mathrm{GL}_n(A)$.

Soit E un A-module libre de rang n et de bases $\mathcal{B}$ et $\mathcal{B}'$. Soit $u \in \mathrm{End}_A(M)$. On a

$$M_{\mathcal{B}}(u) = M_{\mathcal{B}',\mathcal{B}}(\mathrm{id}_M) M_{\mathcal{B}'}(u) M_{\mathcal{B},\mathcal{B}'}(\mathrm{id}_M) = M_{\mathcal{B},\mathcal{B}'}(\mathrm{id}_M)^{-1} M_{\mathcal{B}'}(u) M_{\mathcal{B},\mathcal{B}'}(\mathrm{id}_M)$$

Ainsi on a $\det(M_{\mathcal{B}}(u)) = \det(M_{\mathcal{B}'}(u))$. Ce calcul légitime la définition suivante.

Définition D.6. *Soit E un A-module libre de rang fini et $u \in \mathrm{End}_A(E)$. Le déterminant de u est le déterminant de la matrice de u (relativement à n'importe quelle base de E).*

Théorème D.7. Soit E un A-module libre de rang fini et $u \in \mathrm{End}_A(E)$. Les assertions suivantes sont équivalentes.

1. u est un isomorphisme.
2. u est surjectif.
3. $\det(u) \in U(A)$.

Preuve. Le théorème C.5 et les considérations précédentes assurent que $(1) \iff (3)$ et on a bien sûr $(1) \Rightarrow (2)$. Si u est surjectif, comme E est libre, il existe par le chapitre II une application linéaire $v : E \longrightarrow E$ telle que $u \circ v = \mathrm{id}_E$, d'où $\det(u) \in U(A)$. □

Corollaire D.8. Si $A = K$ est un corps et E est un K-espace vectoriel de dimension finie, alors pour $u \in \mathrm{End}_K(E)$, les assertions suivantes sont équivalentes.

1. u est un isomorphisme.
2. u est surjectif.
3. u est injectif.
4. $\det(u) \neq 0$.

Preuve. Il reste à voir que si u est injectif alors il est surjectif. Si u est injectif, alors $u(E) \subset E$ est un sous-espace de dimension égale à celle de E, et ainsi $E = u(E)$ (compléter une base de $u(E)$ en une base de E...) □

Théorème D.9. Supposons que A est un anneau intègre. Soit E un A-module libre de rang fini et $u \in \mathrm{End}_A(E)$. Les assertions suivantes sont équivalentes.

1. u est injectif.
2. $\det(u) \neq 0$.

Preuve. Soit $(\mathcal{E}_1, \ldots, \mathcal{E}_n)$ une base de E et soit $M = (a_{ij}) \in \mathcal{M}_n(A)$ la matrice de u dans cette base. Soit $K = \mathrm{Fr}(A)$ le corps des fractions de A et soit $\widetilde{u} : K^n \longrightarrow K^n$ l'application K-linéaire dont la matrice dans la base canonique $(e_1, \ldots, e_n)$ est $M : \widetilde{u}(e_i) = \sum_{j=1}^n a_{ji}.e_j$ pour tout i. On a $\det(u) = \det(\widetilde{u})$. Alors $\det(u) \neq 0$ si et seulement si $\widetilde{u}$ est un isomorphisme. Un élément $\sum_{i=1}^n a_i.\mathcal{E}_i$ du noyau de u ($a_1, \ldots, a_n \in A$) fournit un élément $\sum_{i=1}^n a_i.e_i$ du noyau de $\widetilde{u}$. Donc si $\det(u) \neq 0$, alors u est injectif.

Réciproquement si $\det(u) = 0 = \det(\widetilde{u})$, soit $\sum_{i=1}^n \lambda_i.e_i \in \mathrm{Ker}(u)$ ($\lambda_1, \ldots, \lambda_n \in K$ non tous nuls). Soit $d \in A$ tel que $\forall i$, $d\lambda_i \in A$. Alors $\sum_{i=1}^n (d\lambda_i).\mathcal{E}_i \neq 0$ appartient au noyau de u, et u est non injectif. □

Exemple D.10. Soit $u : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$ l'application $\mathbb{Z}$-linéaire dont la matrice dans la base canonique est $\begin{pmatrix} 2 & 4 \\ 3 & 1 \end{pmatrix}$. Alors u est injective mais non surjective.

E Application : les entiers algébriques

Définition E.1. *Soit $A \subset B$ une extension d'anneaux (commutatifs), c'est-à-dire que B est un anneau et A un sous-anneau $B : A \subset B$. On dit qu'un élément $x \in B$ est **entier sur** A s'il existe un polynôme unitaire $P \in A[X]$ tel que $P(x) = 0$. On note*

$$\mathcal{O}_{B/A} = \{x \in B \mid x \text{ est entier sur } A\}$$

On se propose de montrer que $\mathcal{O}_{B/A}$ est un sous-anneau de B.

Lorsque A et B sont des corps, un élément entier sur A est exactement un élément algébrique sur A. Mais si A n'est pas un corps, la notion d'entier est plus restrictive : par exemple un élément de $\mathbb{Q}$ est entier sur $\mathbb{Z}$ si et seulement si il appartient à $\mathbb{Z}$. Plus généralement, on a le résultat suivant.

Proposition E.2. Soit A un anneau factoriel et soit $K = \mathrm{Fr}(A)$ le corps des fractions de A. Alors $\mathcal{O}_{K/A} = A$.

Preuve. Soit $x \in K$ entier sur A. On peut écrire $x = \frac{p}{q}$ avec $(p, q) \in A \times A^*$ premiers entre eux. Il existe $n \in \mathbb{N}^*$ et $a_0, \ldots, a_{n-1} \in A$ tels que

$$\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \ldots + a_1\frac{p}{q} + a_0 = 0$$

ce qui donne en multipliant par q^n

$$p^n = -(a_{n-1}p^{n-1}q + \ldots + a_1 pq^{n-1} + a_0 q^n)$$

et donc $q|p^n$, donc $q|p$ (lemme de Gauss), et donc $q \in U(A)$. Ainsi $x \in A$. □

Théorème E.3. Soit $A \subset B$ une extension d'anneaux et soit $x \in B$. Les assertions suivantes sont équivalentes.

1. x est entier sur A.
2. $A[x]$ est un A-module de type fini.
3. Il existe un sous-anneau R de B contenant x, tel que $A \subset R \subset B$ et qui est de type fini comme A-module.

Preuve. (1) $\Rightarrow$ (2) est laissé en exercice et (2) $\Rightarrow$ (3) est évident. Montrons (3) $\Rightarrow$ (1). Soient $w_1, \ldots, w_n$ une famille de générateurs de R comme A-module. Il existe des éléments a_{ij}, $1 \leq i, j \leq n$, tels que $\forall i$, $R \ni xw_i = \sum_{j=1}^n a_{ij}w_j$, c'est-à-dire que

$$\forall i,\ \sum_{j=1}^n (\delta_{ij}x - a_{ij})w_j = 0$$

Posons $\lambda_{ij} = \delta_{ij}x - a_{ij}$ et considérons la matrices $M = (\lambda_{ij}) \in \mathcal{M}_n(R)$. Les relations précédentes donnent

$$M \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

La relation ${}^t\tilde{M}M = \det(M)I_n$ assure alors que $\det(M)w_i = 0$, $\forall i$. Mais $w_1, \ldots, w_n$ engendrent R comme A-module, donc il existe $b_1, \ldots, b_n \in A$ tels que $1 = \sum_{i=1}^n b_i w_i$, et on en déduit que $\det(M) = 0$. Ainsi si $P = \det(\delta_{ij}X - a_{ij}) \in A[X]$, on a $P(x) = 0$ avec P unitaire : x est entier sur A. □

Corollaire E.4. Soit $A \subset B$ une extension d'anneaux. Alors $\mathcal{O}_{B/A}$ est un sous-anneau de B.

Preuve. Pour $x, y \in \mathcal{O}_{B/A}$, il est clair que $A[x, y]$ est un A-module de type fini, et ainsi par le théorème précédent on a $A[x, y] \subset \mathcal{O}_{B/A}$ et donc $x - y, xy \in \mathcal{O}_{B/A}$. Enfin on a $A \subset \mathcal{O}_{B/A}$, donc $1 \in \mathcal{O}_{B/A}$, ce qui assure que $\mathcal{O}_{B/A}$ est un sous-anneau de B. □

Définition E.5. *Soit R un anneau. On dit qu'un élément $x \in R$ est un **entier algébrique** s'il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(x) = 0$. On note $\mathcal{O}_R$ l'ensemble des entiers algébriques de R.*

Soit R un anneau et soit ϕ l'unique morphisme d'anneaux de $\mathbb{Z}$ dans R. Un élément $x \in R$ est entier algébrique et seulement s'il est entier sur $\phi(\mathbb{Z})$. Les résultats précédents donnent donc en particulier le résultat suivant.

Théorème E.6. Soit R un anneau (commutatif) et soit $x \in R$. Les assertions suivantes sont équivalentes.

1. x est entier algébrique.
2. $\mathbb{Z}[x]$ (le sous-anneau de R engendré par x) est un $\mathbb{Z}$-module de type fini.
3. Il existe un sous-anneau T de R contenant x, qui est de type fini comme $\mathbb{Z}$-module.

En particulier $\mathcal{O}_R$ est un sous anneau de R.

Exemple E.7. Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré. On peut montrer que

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\omega] = \mathbb{Z} \oplus \omega\mathbb{Z}$$

où

$$\omega = \begin{cases} \sqrt{d} & \text{si } d \equiv 2, 3 \bmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \bmod 4 \end{cases}$$

F Opération sur les lignes et colonnes d'une matrice

Définition F.1. *Etant donnée une matrice $M \in \mathcal{M}_{s,n}(A)$, on considère les opérations suivantes (dites **opérations élémentaires sur les lignes** de M) :*

(L1) *On ajoute à une ligne donnée un multiple (quelconque) d'une autre ligne de M.*

(L2) *On multiplie une ligne de M par un élément* inversible *de A.*

(L3) *On permute deux lignes de M.*

Remarque F.2. Considérons les matrices inversibles suivantes :

1. Pour $i \neq j$ et $\lambda \in A$, on note $F_{ij}(\lambda) \in \mathcal{M}_{s,s}(A)$ est la matrice dont les coefficients diagonaux sont égaux à 1 et dont les autres coefficients sont nuls sauf celui de la ligne i et de la colonne j qui est égal à λ. (voir le paragraphe A)
2. Pour $1 \leqslant i \leqslant s$ et $\alpha \in A$ avec α *inversible*, on note $E_i(\alpha) \in \mathcal{M}_{s,s}(A)$ la matrice diagonale dont les coefficients sont égaux à 1 sauf le i-ème qui est égal à α.

Alors **(L1)** revient à multiplier M à gauche par une matrice $F_{ij}(\lambda)$ et **(L2)** revient à multiplier M à gauche par une matrice $E_i(\alpha)$. Par ailleurs l'échange de deux lignes **(L3)** peut être obtenu à partir de 4 opérations **(L1)** ou **(L2)**.

Définition F.3. *On considère également les opérations suivantes (dites* ***opérations élémentaires sur les colonnes*** *de M) :*

(C1) *On ajoute à une colonne donnée un multiple (quelconque) d'une autre colonne de M.*

(C2) *On multiplie une colonne de M par un élément* inversible *de A.*

(C3) *On permute deux colonnes de M.*

Remarque F.4. Ces opérations reviennent à multiplier M à *droite* par les matrices $F_{ij}(\lambda)$ et $E_i(\alpha)$ de taille $n \times n$ définies comme ci-dessus.

Définition-Proposition F.5. Soient M et N dans $\mathcal{M}_{s,n}(A)$. On dit que N est **équivalente** à M si N peut être obtenue à partir de M en lui appliquant une succession d'opérations élémentaires sur les lignes et les colonnes. On note $M \sim N$. Ceci définit une relation d'équivalence sur $\mathcal{M}_{s,n}(A)$.

Rappelons qu'un anneau euclidien est un anneau intègre A muni d'une application (stathme) $\nu : A \setminus \{0\} \longrightarrow \mathbb{N}$ telle que pour tous $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que

$$a = bq + r, \text{ avec } r = 0 \text{ ou } \nu(r) < \nu(b)$$

Théorème F.6. Supposons que A est un anneau euclidien. Soit $R \in \mathcal{M}_{s,n}(A)$. Alors R est équivalente à une matrice de la forme $\mathrm{diag}(d_1, \ldots, d_t)$ avec $d_1 \mid d_2 \mid \ldots \mid d_t$ dans A où $t = \min(s, n)$.

On peut démontrer que la suite $(d_1, \ldots, d_n)$ du théorème est unique à multiplication près par un élément inversible de A, ce qui justifie le terme de *facteurs invariants* pour la matrice.

Démonstration. Notons ν le stathme de A. Cette démonstration permettra alors d'obtenir un algorithme pour passer de R à la matrice des facteurs invariants.

Notons $R = (a_{ij})_{1 \leqslant i \leqslant s, 1 \leqslant j \leqslant n}$.

1. Fixons i et j tels que $a_{ij} \neq 0$. Montrons que l'on peut remplacer tous les coefficients de la ligne i et de la colonne j (autres que a_{ij} lui-même) par les restes de leurs divisions euclidiennes par a_{ij}.
   Soit $k \neq j$. On a $a_{ik} = q_{ik}a_{ij} + r_{ik}$ avec $r_{ik} = 0$ ou $\nu(r_{ik}) < \nu(a_{ij})$. Si on soustrait q_{ik} fois la colonne j à la colonne k, et le coefficient de la ligne i et de la colonne k devient r_{ik}.
   On raisonne de même pour transformer la colonne j.
2. Notons $\mathcal{C}$ l'ensemble de tous les coefficients non nuls de toutes les matrices équivalentes à R. Soit $d_1 \in \mathcal{C}$ avec $\nu(d_1)$ minimal dans $\{\nu(x); x \in \mathcal{C}\}$, et supposons que d_1 soit l'un des coefficients de R (quitte à remplacer R par une matrice qui lui est équivalente). Quitte à permuter des lignes et/ou les colonnes de R, on peut supposer que d_1 est le coefficient de la première ligne et de la première colonne.
   On sait que l'on peut remplacer tous les coefficients de la première ligne et de la première colonne autres que d_1 par les restes de leurs divisions euclidiennes par d_1. Par minimalité de $\nu(d_1)$, tous ces restes sont nuls.
   On s'est donc ramenés à une matrice équivalente à R qui est de la forme $\begin{pmatrix} d_1 & 0 \\ 0 & R_1 \end{pmatrix}$ avec $R_1 \in \mathcal{M}_{s-1,n-1}(A)$.
   De plus, d_1 divise tous les coefficients de R_1. En effet, soit $2 \leqslant i \leqslant s$. Si on ajoute la première ligne de R à la i-ème, on a une matrice dont la i-ème ligne est $\begin{pmatrix} d_1 & a_{i2} & \cdots & a_{in} \end{pmatrix}$, et on sait d'après l'étape précédente que l'on peut remplacer tous les a_{ij} pour $j = 2, \ldots, n$ par le reste de la division euclidienne de a_{ij} par d_1. Par minimalité de $\nu(d_1)$ on en déduit que ces restes sont nuls, c'est-à-dire que $d_1 \mid a_{ij}$ pour tout $2 \leqslant j \leqslant n$.
3. On applique les deux étapes précédentes à R_1. Cela ne changera pas la première ligne et la première colonne de R, et on en déduit que R est équivalente à une matrice de la forme $\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & R_2 \end{pmatrix}$ avec $d_1 \mid d_2$ et d_2 divise tous les coefficients de R_2.
4. Par récurrence, on obtient une matrice $\mathrm{diag}(d_1 \ldots, d_t)$ équivalente à R avec $d_1 \mid d_2 \mid \ldots \mid d_t$ et $t = \min(s, n)$. □

Remarque F.7. On obtient l'algorithme suivant :

Etape 1 Soit d_1 le coefficient non nul de R avec $\nu(d_1)$ minimal. Par permutation des lignes et des colonnes on place le coefficient non nul de R dont l'image par ν est minimale en position $(1, 1)$.

Etape 2 On ajoute des multiples de la première colonne (*resp.* ligne) aux autres colonnes (*resp.* lignes) afin d'obtenir des coefficients nuls ou dont l'image par ν est strictement inférieure à a_{11} sur la première ligne (*resp.* colonne).

Etape 3 On répète les étapes **1** et **2** jusqu'à obtenir une matrice de la forme $\begin{pmatrix} a_{11} & 0 \\ 0 & R_1 \end{pmatrix}$.

Etape 4 Si a_{11} divise tous les coefficients de R_1 on répète les étapes précédentes sur R_1.

Etape 5 Si a_{11} ne divise pas a_{ij} avec $i \geqslant 2$ et $j \geqslant 2$, on ajoute la $i$me ligne à la première et on reprend à l'étape **1**.

Exemple F.8. $A = \mathbb{Q}[X]$ et $R = \begin{pmatrix} X & 0 & 0 \\ 0 & 1-X & 0 \\ 0 & 0 & (1-X)(1+X) \end{pmatrix}$. L'anneau A est bien eucli-

dien avec $\nu = \deg$.

Les opérations successives suivantes : $L_1 \to L_1 + L_2$; $C_2 \to C_2 + C_1$; $C_1 \leftrightarrow C_2$; $L_2 \to L_2 + (X-1)L_1$; $C_2 \to C_2 - XC_1$; $L_2 \to L_2 + L_3$; $C_3 \to C_3 + C_2$; $C_2 \leftrightarrow C_3$; $L_3 - (1+X)L_2$; $C_3 \to C_3 + XC_2$; $C_2 \to -C_2$ et $C_3 \to -C_3$ donnent la matrice $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X-1 & 0 \\ 0 & 0 & X(X-1)(X+1) \end{pmatrix}$ donc les facteurs invariants sont 1, $X-1$ et $X(X-1)(X+1)$.

On sait que $D = PRQ$ où P est donnée par les opérations sur les lignes et Q est donnée par les opérations sur les colonnes. Pour les trouver, on applique les opérations que l'on a faites sur les lignes de R à I_3 (pour P) et les opérations que l'on a faites sur les colonnes de R à I_3 (pour Q). On obtient

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 1-X & -X & -1 \\ (X-1)(X+1) & X(X+1) & X \end{pmatrix} \quad \text{et} \quad Q = \begin{pmatrix} 1 & 1-X & (1-X)(1+X) \\ 1 & -X & -X(1+X) \\ 0 & 1 & X \end{pmatrix}.$$

Exemple F.9. $A = \mathbb{Z}$ et $R = \begin{pmatrix} 7 & 8 & 9 \\ 4 & 5 & 6 \\ 1 & 2 & 3 \end{pmatrix}$. L'anneau $\mathbb{Z}$ est bien euclidien avec $\nu = |\ |$.

La suite d'opérations sur les lignes et les colonnes $L_1 \leftrightarrow L_3$; $L_2 \to L_2 - 4L_1$; $L_3 \to L_3 - 7L_1$; $C_2 \to C_2 - 2C_1$; $C_3 \to C_3 - 3C_1$; $L_2 \to -L_2$; $L_3 \to L_3 + 2L_2$ et $C_3 \to C_3 - 2C_2$ donne $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. On sait que $D = PRQ$ avec P et Q obtenues comme dans l'exemple précédent. En pratique, nous voulons souvent Q^{-1} plutôt que Q, et celle-ci est obtenue en effectuant les opérations sur les colonnes inverses et dans l'ordre inverse. On obtient $P = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 4 \\ 1 & -2 & 1 \end{pmatrix}$ et $Q^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$.

G Applications aux groupes linéaires

Une première application directe des opérations élémentaires sur les lignes et colonnes est de fournir des générateurs du groupe linéaire $\mathrm{GL}_n(A)$.

Théorème G.1. Si A est un anneau euclidien, le groupe $\mathrm{GL}_n(A)$ est engendré par les matrices
$$\{F_{ij}(\lambda),\ 1 \le i \ne j \le n,\ \lambda \in A\} \cup \{E_i(\alpha),\ 1 \le i \le n,\ \alpha \in U(A)\}$$

Preuve. Notons $X = \{F_{ij}(\lambda),\ 1 \le i \ne j \le n,\ \lambda \in k\} \cup \{E_i(\alpha),\ 1 \le i \le n,\ \alpha \in U(A)\}$. Pour $M \in \mathrm{GL}_n(A)$, les opérations élémentaires sur les lignes et les colonnes de M assurent l'existence de $P_1, \dots P_m, Q_1, \dots Q_r \in X$ et $d_1, \dots d_n \in U(A)$ tels que

$$P_1 \cdots P_m M Q_1 \cdots Q_r = \mathrm{diag}(d_1, \dots, d_n)$$

et puisque $\mathrm{diag}(d_1, \dots, d_n) \in \langle X \rangle$, on a bien $M \in \langle X \rangle$. □

Exemple G.2. Le groupe $\mathrm{GL}_2(\mathbb{Z})$ est engendré par les 4 matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

En fait, en utilisant les relations

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

on voit que $\mathrm{GL}_2(\mathbb{Z})$ est engendré par les 3 matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Le groupe $\mathrm{SL}_n(A)$ est défini par

$$\mathrm{SL}_n(A) = \{M \in \mathcal{M}_n(A) \mid \det(M) = 1\}$$

C'est un sous-groupe normal de $\mathrm{GL}_n(A)$ car $\det : \mathrm{GL}_n(A) \longrightarrow U(A)$ est un morphisme de groupes.

Proposition G.3. On a un isomorphisme de groupes $\mathrm{GL}_n(A) \cong \mathrm{SL}_n(A) \rtimes U(A)$.

Preuve. Soit H le sous-groupe de $\mathrm{GL}_n(A)$ formé par les matrices $E_1(a) = \mathrm{diag}(\mathrm{a}, 1, \ldots, 1)$, $a \in U(A)$. On voit facilement que $H \cap \mathrm{SL}_n(A) = \{1\}$, $\mathrm{GL}_n(A) = H\mathrm{SL}_n(A)$, et puisque $\mathrm{SL}_n(A) \lhd \mathrm{GL}_n(A)$, la caractérisation des produits semi-directs assure que $\mathrm{GL}_n(A) \cong \mathrm{SL}_n(A) \rtimes H$, et on a le résultat car $H \cong U(A)$. □

Théorème G.4. Si A est un anneau euclidien, le groupe $\mathrm{SL}_n(A)$ est engendré par les matrices

$$\{F_{ij}(\lambda),\ 1 \leq i \neq j \leq n,\ \lambda \in A\}$$

Preuve. Les matrices en question sont bien sûr dans $\mathrm{SL}_n(A)$. Deux matrices $M, N \in \mathrm{SL}_n(A)$ sont dites fortement équivalentes si elles peuvent être obtenues l'une à partir de l'autre seulement à partir des opérations (L1) et (C1). Il s'agit donc de montrer qu'à partir d'un matrice quelconque de $\mathrm{SL}_n(A)$ est fortement équivalente à la matrice identité. Les opérations d'échange (L3) et (C3) ne sont pas autorisées en général. Néanmoins on peut échanger deux colonnes C_i et C_j au signe près, via la suite d'opérations (C1) suivante :

$$(C_i, C_j) \to (C_i + C_j, C_j) \to (C_i + C_j, -C_i) \to (C_j, -C_i)$$

Bien sûr on peut faire la même chose pour les lignes.

En reprenant point par point la preuve du théorème F.6, on voit alors qu'une matrice de $\mathrm{SL}_n(A)$ est fortement équivalente à une matrice du type $\mathrm{diag}(d_1, \ldots, d_n)$ avec $d_1 \cdots d_n = 1$. En effet l' étape 1 n'utilisent que les opérations (L1)-(C1), alors que dans l'étape 2, on peut utiliser la remarque précédente sur l'échange au signe près des lignes et colonnes (dans un anneau euclidien A on peut toujours remplacer le stathme ν par un stathme ν' tel que $\nu'(ua) = \nu'(a)$, $\forall u \in U(A)$, en posant $\nu'(a) = \min\{\nu(ua), u \in U(A)\}$). Finalement on voit sans difficulté qu'une matrice de $\mathrm{SL}_n(A)$ est fortement équivalente à I_n. □

Exemple G.5. Le groupe $\mathrm{SL}_2(\mathbb{Z})$ est engendré par les matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

On termine le chapitre en appliquant les considérations précédentes au calcul des centres et groupes dérivés des groupes linéaires.

Proposition G.6.
1. On a $Z(\mathrm{GL}_n(A)) = \{aI_n,\ a \in U(A)\}$, d'où un isomorphisme de groupes $Z(\mathrm{GL}_n(A)) \cong U(A)$.
2. On a $Z(\mathrm{SL}_n(A)) = \{aI_n,\ a \in A \text{ tq } a^n = 1\}$, d'où un isomorphisme de groupes $Z(\mathrm{GL}_n(A)) \cong \mu_n(A)$.

Le résultat est une application directe de la proposition B.2. Le lemme suivant est obtenu par des calculs directs.

Lemme G.7.
1. Supposons $n \geq 3$. On a pour i, j, k deux à deux distincts et $\lambda, \mu \in A$,
$$F_{ij}(\lambda) = F_{ik}(\lambda)F_{kj}(1)F_{ik}(\lambda)^{-1}F_{kj}(1)^{-1}$$
2. Supposons $n \geq 2$ et que $A = K$ est un corps ayant au moins 3 éléments. On a pour $i \neq j$, et $\lambda, \mu \in K$, $\mu \in K \setminus \{0, 1\}$,
$$F_{ij}(\lambda) = E_i(1-\mu)F_{ij}(-\lambda\mu^{-1})E_i(1-\mu)^{-1}F_{ij}(-\lambda\mu^{-1})^{-1}$$
3. Supposons $n \geq 2$ et que $A = K$ est un corps ayant au moins 4 éléments. Soit $\lambda \in K$ et $\mu \in K \setminus \{0, 1, -1\}$. On a
$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix} \begin{pmatrix} 1 & \lambda(\mu^2-1)^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 1 & \lambda(\mu^2-1)^{-1} \\ 0 & 1 \end{pmatrix}^{-1}$$

Rappelons que si G est un groupe, le groupe dérivé de G, noté $D(G)$, est le sous-groupe de G engendré par les commutateurs de G, c'est-à-dire les éléments de la forme $xyx^{-1}y^{-1}$, $x, y \in G$.

Corollaire G.8.
1. Si A est un anneau euclidien et $n \geq 3$, on a $D(\mathrm{SL}_n(A)) = D(\mathrm{GL}_n(A)) = \mathrm{SL}_n(A)$.
2. Si $A = K$ est un corps ayant au moins 3 éléments, on a $D(\mathrm{GL}_2(K)) = \mathrm{SL}_2(K)$.
3. Si $A = K$ est un corps ayant au moins 4 éléments, on a $D(\mathrm{SL}_2(K)) = D(\mathrm{GL}_2(K)) = \mathrm{SL}_2(K)$.

Preuve. Le déterminant est un morphisme de groupes à valeurs dans un groupe abélien, il est donc facile de voir que $D(\mathrm{SL}_n(A)) \subset D(\mathrm{GL}_n(A)) \subset \mathrm{SL}_n(A)$. le résultat est ensuite conséquence du théorème G.4 et des calculs du lemme. □

VI Modules de type fini sur un anneau principal

L'existence d'une base pour un espace vectoriel s'interprète comme un théorème de structure : Si M est un K-espace vectoriel (K un corps), il existe un ensemble I tel que $M \cong K^{(I)}$. On généralise ce résultat aux modules de type fini sur un anneau principal. On appliquera ensuite le théorème de structure à la réduction des endomorphismes, pour retrouver en particulier le fait que toute matrice à coefficients dans un corps algébriquement clos est similaire à une matrice en forme canonique de Jordan.

A Les théorèmes de structures : énoncé

Théorème A.1 (de structure, version facteurs invariants)**.** Soient A un anneau principal et M un A-module de type fini.

1. On a un isomorphisme de A-modules
$$M \cong A^n \oplus A/(a_1) \oplus \cdots \oplus A/(a_r)$$
pour des entiers $r, n \geq 0$ et des éléments non inversibles $a_1, \ldots, a_r \in A^*$ tels que $a_1 | a_2 | \cdots | a_r$.
2. La donnée précédente $(n, a_1, \ldots, a_r)$ détermine uniquement le module M, à multiplication près des a_i par des inversibles. Les éléments $a_1, \ldots, a_r$ sont appelés **les facteurs invariants de** M.

Théorème A.2 (de structure, version diviseurs élémentaires)**.** Soient A un anneau principal et M un A-module de type fini.

1. On a un isomorphisme de A-modules
$$M \cong A^n \oplus A/(p_1^{m_1}) \oplus \cdots \oplus A/(p_s^{m_s})$$
pour $n, s \in \mathbb{N}$, et $p_1, \ldots, p_s$ des irréductibles de A (non nécessairement deux à deux distincts).
2. La donnée précédente $(n, p_1^{m_1}, \ldots, p_s^{m_s})$ détermine uniquement le module M, à multiplication par des inversibles près pour les irréductibles, et à l'ordre près. Les éléments $p_1^{m_1}, \ldots, p_s^{m_s}$ sont appelés **les diviseurs élémentaires de** M.

Corollaire A.3. Un groupe abélien fini est isomorphe à un produit de groupes cycliques

Preuve. Si M est groupe abélien fini, c'est en particulier un $\mathbb{Z}$-module de type fini. Le n du théorème est nul car M est fini, d'où le résultat. □

B Le théorème de la base adaptée

Les théorèmes de structures seront des conséquences du théorème suivant.

Théorème B.1 (de la base adaptée)**.** Soient A un anneau principal, M un A-module libre de rang fini, et $N \subset M$ un sous-module. Il existe une base $\{e_1, \dots, e_n\}$ de M, un entier $p \leq n$ et des élements $a_1, \dots, a_p \in A$ tels que $\{a_1.e_1, \dots, a_p.e_p\}$ soit une base de N et $a_1|a_2| \cdots |a_p$.

En particulier tout sous-module d'un module d'un module libre de rang fini est libre si A est principal (on avait vu que cela n'est pas vrai en général).

Le but du paragraphe est de démontrer ce résultat. On commence par énoncer un lemme élémentaire, qui sera utilisé librement dans la suite. La preuve est laissée en exercice.

Lemme B.2. Soient A un anneau intègre et M un A-module libre. Soit $x \in M \setminus \{0\}$. Alors $Ax \subset M$ est un A-module libre de rang 1.

Tout d'abord, on a un résultat moins précis que le théorème de la base adaptée.

Théorème B.3. Soient A un anneau principal et M un A-module libre de rang n. Alors tout sous-module de M est libre de rang $\leq n$.

Preuve. Soit E un sous-module de M. On peut supposer E et M non nuls. Soit $\{x_1, \dots, x_n\}$ une base de M. et soit $f : M \longrightarrow A$ l'unique application linéaire telle que $f(x_i) = \delta_{i1}$. Il existe $a \in A$ tel que $f(E) = Aa$, car A est principal. On démontre le résultat par récurrence sur n.

$\rightsquigarrow$ Supposons $n = 1$. Alors f est un isomorphisme et f induit un isomorphisme $E \cong Aa$ avec $a \neq 0$, qui est donc libre de rang 1.

$\rightsquigarrow$ Supposons $n \geq 2$ et le résultat montré pour les modules libres de rang $< n$. Si $a = 0$, on a $E \subset \mathrm{Ker}(f) = Ax_2 + \cdots + Ax_n$ qui est un module libre de rang $n-1$, et donc l'hypothèse de récurrence donne le résultat. Supposons donc $a \neq 0$, c'est-à-dire $E \not\subset \mathrm{Ker}(f)$. Soit $Q = E \cap \mathrm{Ker}(f)$, par hypothèse de récurrence c'est un module libre de rang $\leq n-1$, il admet donc une base $e_2, \dots, e_q$, avec $2 \leq q \leq n$. Soit $e_1 \in E \setminus \{0\}$ tel que $f(e_1) = a$ ($f(E) = Aa$). Pour $x \in E$, on a $f(x) = ba = f(a.e_1)$, donc $x - a_1 e.1 \in \mathrm{Ker}(f) \cap E = Q$, donc

$$E = Q + Ae_1 = Ae_1 + Ae_2 + \cdots + Ae_q$$

Il reste donc à voir que la famille $\{e_1, \dots, e_q\}$ est libre. Soient $c_1, \dots, c_q \in A$ tels que $c_1e_1 + \cdots + c_qe_q = 0$. Alors on a

$$-c_1a = f(-c_1.e_1) = f(c_2e_2 + \cdots + c_qe_q) = 0$$

d'où $c_1 = 0$, et l'indépendance linéaire de $e_2, \dots, e_q$ permet de conclure. □

Le résultat suivant ne sera pas utilisé dans la suite. La preuve est laissée en exercice.

Corollaire B.4. Si M est un A-module de type fini sur un anneau principal A, alors tout sous-module de M est de type fini.

Preuve du théorème de la base adaptée. La preuve que nous allons donner utilise les résultats sur les opérations élémentaires sur les matrices, où nous avons utilisé l'hypothèse que A est euclidien. On

consultera l'appendice pour une preuve indépendante des opérations élémentaires, et donc valable pour un anneau principal quelconque, mais un peu plus difficile.

Soit N un sous-module du A-module libre A^n. On sait par le théorème précédent que le sous-module N de A^n est libre de rang fini.

Nous voulons en fait montrer que l'on peut choisir une base de N particulière.

Soit $\mathcal{B} = \{e_1, \ldots, e_n\}$ une base de A^n et soit $\mathcal{G} = \{x_1, \ldots, x_s\}$ un système générateur de N. Pour tout $1 \leqslant i \leqslant s$ on peut écrire $x_i = \sum_{j=1}^{n} a_{ij} e_j$ avec $a_{ij} \in A$ de manière unique.

Alors N est entièrement déterminé par le couple $(\mathcal{B}, R)$ où $\mathcal{B}$ est une base de A^n et R est la matrice $R = (a_{ij})_{1 \leqslant i \leqslant s, 1 \leqslant j \leqslant n}$.

Les opérations élémentaires sur les lignes et colonnes de R fournissent des matrices $P \in \mathrm{GL}_s(A)$, $Q \in \mathrm{GL}_n(A)$ telles que

$$PRQ = \mathrm{diag}(d_1, \ldots, d_t)$$

avec $d_1 \mid \ldots \mid d_t$ dans A et $t = \min(s, n)$. Posons

$$e'_j = \sum_{k=1}^{n} (Q^{-1})_{jk} e_k, \ \forall j \in \{1, \ldots, n\}$$

$$x'_i = \sum_{l=1}^{s} P_{il} x_l, \ \forall i \in \{1, \ldots, s\}$$

Les matrices P et Q étant inversibles, il est clair que $\{e'_1, \ldots, e'_n\}$ est une nouvelle base de A^n et que $\{x'_1, \ldots, x'_s\}$ est une nouvelle partie génératrice de N. On a, pour $1 \leq i \leq s$,

$$x'_i = \sum_{l=1}^{s} P_{il} x_l = \sum_{l=1}^{s} \sum_{k=1}^{n} P_{il} a_{lk} e_k = \sum_{l=1}^{s} \sum_{k=1}^{n} \sum_{j=1}^{n} P_{il} a_{lk} Q_{kj} e'_j = d_i e'_i$$

(avec la convention $d_i = 0$ si $i > n$). Soit r le nombre de d_i non nuls : $r \leqslant t \leqslant n$. Dans cette nouvelle base de A^n, les générateurs de N sont donnés par $g_i = d_i e_i$. Donc $N = \langle d_1 e_1, \ldots, d_r e_r \rangle$ (puisque les autres générateurs sont nuls). Enfin, on voit facilement que $\{d_1 e_1, \ldots, d_r e_r\}$ est une famille libre (A est intègre et les d_i sont non nuls pour $1 \leqslant i \leqslant r$) et donc une base de N, qui est donc libre de rang $r \leqslant n$. □

Remarque B.5. La démonstration précédente fournit non seulement l'existence de la base adaptée, mais aussi un moyen de la construire (quand A est euclidien donc). On reprend les données précédentes :

N est un sous-module du A-module libre A^n, $\mathcal{B} = \{e_1, \ldots, e_n\}$ est une base de A^n, $\mathcal{G} = \{x_1, \ldots, x_s\}$ est un système générateur de N avec $x_i = \sum_{j=1}^{n} a_{ij} e_j$, $R = (a_{ij}) \in \mathcal{M}_{s,n}(A)$.

Les opérations sur les colonnes de R fournissent la base adaptée. Plus précisément, si $P \in \mathrm{GL}_s(A)$, $Q \in \mathrm{GL}_n(A)$ sont les matrices telles que

$$PRQ = \mathrm{diag}(d_1, \ldots, d_t)$$

avec $d_1 \mid \ldots \mid d_t$, la matrice Q est obtenue en appliquant les mêmes opérations sur les colonnes à la matrice identité I_n. La base adaptée $\{e'_1, \ldots, e'_n\}$ est donnée par

$$e'_j = \sum_{k=1}^{n} (Q^{-1})_{jk} e_k, \ \forall j \in \{1, \ldots, n\}$$

et pour trouver Q^{-1}, il suffit d'appliquer en sens inverse les opérations inverses sur les colonnes à la matrice I_n. Les coordonnées de la nouvelle base dans l'ancienne sont données par les lignes de la matrice obtenue.

Exemple B.6. Soit M le groupe abélien libre $\mathbb{Z}^3$ de base $\{f_1, f_2, f_3\}$ et soit N le sous-module engendré par g_1, g_2 et g_3 avec $g_1 = -4f_1 - 6f_2 + 7f_3$, $g_2 = 2f_1 + 2f_2 + 4f_3$, $g_3 = 6f_1 + 6f_2 + 15f_3$. Pour trouver une base adaptée, on étudie la matrice

$$R = \begin{pmatrix} -4 & -6 & 7 \\ 2 & 2 & 4 \\ 6 & 6 & 15 \end{pmatrix}$$

Grâce aux opérations élémentaires sur les lignes et les colonnes suivantes : $L_1 \leftrightarrow L_2$; $L_2 \to L_2 + 2L_1$; $L_3 \to L_3 - 3L_1$; $C_2 \to C_2 - C_1$; $C_3 \to C_3 - 2C_1$; $L_1 \to L_1 + L_3$; $C_3 \to C_3 - C_1$; $C_3 \leftrightarrow C_1$; $C_3 \to C_3 - 2C_1$; $L_2 \to L_2 - 15L_1$; $L_3 \to L_3 - 3L_1$; $L_2 \to -L_2$; $C_3 \to C_3 - 15C_2$; $L_3 \to -L_3$ (par exemple), on obtient $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$. Il existe donc une base $\tilde{\mathcal{B}} = \{\tilde{e}_1, \tilde{e}_2, \tilde{e}_3\}$ de M telle que $\{\tilde{e}_1, 2\tilde{e}_2, 6\tilde{e}_3\}$ soit une base de N (et donc N est libre de rang 3).

Pour trouver la base $\tilde{\mathcal{B}}$, on applique en sens inverse les opérations inverses sur les colonnes à la matrice I_3, pour obtenir la matrice $Q^{-1} = \begin{pmatrix} 2 & 2 & 7 \\ 15 & 16 & 45 \\ 1 & 1 & 3 \end{pmatrix}$, et donc $\tilde{e}_1 = 2f_1 + 2f_2 + 7f_3, \tilde{e}_2 = 15f_1 + 16f_2 + 45f_3, \tilde{e}_3 = f_1 + f_2 + 3f_3$.

C Structure des modules de type fini

Soit M un A-module. Alors M est de type fini si et seulement s'il existe $n \in \mathbb{N}$ tel que M soit un quotient de A^n. Notons $\varphi : A^n \twoheadrightarrow M$. On peut appliquer ce qui précède au sous-module $\operatorname{Ker}\varphi$ de A^n. Le quotient $M \cong A^n / \operatorname{Ker}\varphi$ est entièrement déterminé par le choix d'un couple $(\mathcal{B}, R)$ où $\mathcal{B}$ est une base de A^n et R est la matrice donnant les générateurs de $\operatorname{Ker}\varphi$ dans la base $\mathcal{B}$.

Définition C.1. *La matrice R est appelée **matrice des relations** de M relative à $\mathcal{B}$.*

Corollaire C.2. Soient A un anneau principal et M un A-module de type fini. Alors M est isomorphe comme A-module à $\bigoplus_{i=1}^{n} (A/(a_i))$ où les (a_i) sont des idéaux de A tels que $(a_i) \supset (a_{i+1})$.

Démonstration. Puisque M est de type fini, on sait que c'est un quotient d'un module libre de type fini A^n. On a donc un morphisme surjectif $\varphi : A^n \twoheadrightarrow M$.

$\operatorname{Ker}\varphi$ est un sous-module de A^n, donc d'après les théorèmes qui précèdent, il existe une base $\{e_1, \ldots, e_n\}$ de A^n et une base $\{a_1 e_1, \ldots, a_q e_q\}$ de $\operatorname{Ker}\varphi$ avec $a_1 \mid \ldots \mid a_q$. On pose $a_i = 0$ pour $q \leqslant i \leqslant n$. L'application A-linéaire surjective

$$\begin{aligned} A^n &\longrightarrow A/(a_1) \oplus \cdots \oplus A/(a_n) \\ \sum_{i=1} b_i \cdot e_i &\longmapsto (\overline{b_1}, \ldots, \overline{b_n}) \end{aligned}$$

a alors $\operatorname{Ker}(\varphi)$ pour noyau, et donc $M \cong A^n/\operatorname{Ker}(\varphi) \cong \bigoplus_{i=1}^{n} (A/(a_i))$. □

Exemple C.3. Soit G est le quotient du groupe abélien libre $\mathbb{Z}^3$ de base $\{f_1, f_2, f_3\}$ par le sous-module N engendré par g_1, g_2 et g_3 avec $g_1 = -4f_1 - 6f_2 + 7f_3$, $g_2 = 2f_1 + 2f_2 + 4f_3$, $g_3 = 6f_1 + 6f_2 + 15f_3$.

On veut écrire G comme une somme directe de groupes monogènes.

On a vu qu'il existe une base $\tilde{\mathcal{B}} = \{\tilde{e}_1, \tilde{e}_2, \tilde{e}_3\}$ de M telle que $\{\tilde{e}_1, 2\tilde{e}_2, 6\tilde{e}_3\}$ soit une base de N. Donc

$$G = \mathbb{Z}^3/N \cong \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Corollaire C.4. Soit M un A-module de type fini. Alors il existe $r \in \mathbb{N}$, $q \in \mathbb{N}$ et $a_1, \ldots, a_q$ dans A non nuls et non inversibles vérifiant $a_1 \mid \ldots \mid a_q$ tels que $M \cong A^r \oplus A/(a_1) \oplus \cdots \oplus A/(a_q)$.

Démonstration. On applique le Corollaire **C.2**. Soit r le nombre de a_i qui sont nuls, donc $(a_n) = \ldots = (a_{n-r+1}) = \{0\}$ et donc pour $n - r < i \leqslant n$ on a $A/(a_i) = A$. De plus, si a_i est inversible, $(a_i) = A$ donc $A/(a_i) = \{0\}$ et on peut donc l'ignorer dans la décomposition. Quitte à renuméroter les a_i on suppose donc que a_1 (et donc tous les a_i non nuls, soit jusqu'à a_q) n'est pas inversible. Donc $M \cong \bigoplus_{i=1}^{q} A/(a_i) \oplus A^r$. □

Corollaire C.5. Avec les notations du théorème précédent, le sous module de torsion de M est $T(M) \cong A/(a_1) \oplus \cdots A/(a_q)$.

Démonstration. D'après le corollaire ci-dessus, on a

$$T(M) \cong T(A^r) \oplus T(A/(a_1)) \oplus \cdots \oplus T(A/(a_q)) = A/(a_1) \oplus \cdots \oplus A/(a_q)$$

car A intègre. □

Corollaire C.6. Soit M un A-module de type fini. Si M est sans torsion, alors M est libre.

On va maintenant montrer le théorème de structure en version diviseurs élémentaires.

Lemme C.7. Soit $M = Ax$ un A-module monogène et soit $\mathrm{Ann}_A(x) = (d)$ (on rappelle que $\mathrm{Ann}_A(x) = \{a \in A \mid a.x = 0\}$).

- **(i)** M est isomorphe comme A-module à $A/(d)$.
- **(ii)** Si $d = pq$ et p, q premiers entre eux dans A, alors $M = Ay \oplus Az$ avec $y = qx$, $z = px$, $\mathrm{Ann}_A(y) = (p)$, $\mathrm{Ann}_A(z) = (q)$.

Démonstration. **(i)** On applique le théorème d'isomorphisme au morphisme de A-modules $\varphi : A \to M$, $a \mapsto a.x$.

(ii) Il est clair que $p \in \mathrm{Ann}_A(y)$ puisque $py = pqx = dx = 0$ donc $(p) \subset \mathrm{Ann}_A(y)$. Soit maintenant $c \in \mathrm{Ann}_A(y)$. On a donc $0 = cy = cqx$ donc $cq \in \mathrm{Ann}_A(x) = (pq)$ donc $cq = pqr$ avec $r \in A$. Donc $c = pr \in (p)$ et donc $\mathrm{Ann}_A(y) = (p)$.

Puisque A est principal on sait qu'il existe $u, v \in A$ tels que $1 = up + vq$. Donc $x = upx + vqx = uz + vy \in Ax + Ay$. Donc $Ax = Ay + Az$.

Soit maintenant $t \in Ay \cap Az$. Alors $pt = 0$ puisque $t \in Ay$ et $p \in \mathrm{Ann}_A(y)$, et $qt = 0$ de même. Donc $t = upt + vqt = 0$. Donc $Ay \cap Az = \{0\}$ et donc $M = Ay \oplus Az$. □

Corollaire C.8. Soit M un A-module de type fini. Alors $M \cong \bigoplus A/(p^{n_r})$ où p parcourt les éléments irréductibles de A et où les n_r sont des entiers positifs presque tous nuls.
Les p^{n_r} sont appelés les **diviseurs élémentaires** de M.

Démonstration. On sait que $M \cong \bigoplus_{i=1}^{n} A/(a_i)$. On factorise chaque $a_i = u \prod p^{n_{p,i}}$ avec u inversible et p irréductible. On décompose ensuite à l'aide du lemme **C.7**. □

On étudie maintenant l'unicité dans les théorèmes de structure. Le lemme suivant est l'outil technique clé pour la preuve.

Lemme C.9. - Soit M un A-module et soit p un élément irréductible de A. Pour $n \in \mathbb{N}$, on considère le A-module $p^n M/p^{n+1}M$.

1. La structure de A-module sur M induit une structure de $A/(p)$-module sur $p^n M/p^{n+1}M$, et donc de $A/(p)$-espace vectoriel sur $p^n M/p^{n+1}M$.
2. Si M et N sont des A-modules isomorphes, alors les $A/(p)$-espaces vectoriels $p^n M/p^{n+1}M$ et $p^n N/p^{n+1}N$ sont isomorphes.
3. Si $M = M_1 \oplus \cdots \oplus M_r$, alors $p^n M/p^{n+1}M \cong p^n M_1/p^{n+1}M_1 \oplus \cdots \oplus p^n M_r/p^{n+1}M_r$.
4. Si $M = A/(d)$ pour $d \in A$, alors $\dim_{A/(p)}(p^n M/p^{n+1}M) = 1$ si p^{n+1} divise d et $\dim_{A/(p)}(p^n M/p^{n+1}M) = 0$ sinon.

Démonstration. Soient $a, b \in A$, $x, y \in M$. Le calcul

$$(ap^n).x - (bp^n).y = a.(p^n.x - p^n.y) + (a-b).(p^n.y)$$

montre que l'on a une application bien définie

$$\begin{aligned} A/(p) \times p^n M/p^{n+1}M &\longrightarrow p^n M/p^{n+1}M \\ (\overline{a}, \widetilde{p^n.x}) &\longmapsto \widetilde{(ap^n).x} \end{aligned}$$

qui munit $p^n M/p^{n+1}M$ d'une structure de $A/(p)$-module, et $A/(p)$ est un corps car A est principal. Les points 2 et 3 sont laissés en exercice. Pour le point 4, soit $n \in \mathbb{N}$. Pour tout $x \in M$ la structure de $A/(p)$-module sur $p^n M/p^{n+1}M$ donne une application $A/(p)$-linéaire

$$\begin{aligned} \varphi_x : A/(p) &\longrightarrow p^n M/p^{n+1}M \\ \overline{a} &\longmapsto \widetilde{(p^n a).x} \end{aligned}$$

Comme $M = A/(d)$, si on prend x la classe de 1 dans A, on a $M = Ax$ et alors φ_x est surjective. Pour $a \in A$, on a $\overline{a} \in \mathrm{Ker}(\varphi_x)$ si et seulement si il existe $b \in A$ tel que $p^n a - p^{n+1}b \in \mathrm{Ann}_A(x) = (d)$, ce qui est encore équivalent à $p^n a \in (p^{n+1}, d)$. Si p^{n+1} divise d, alors $(p^{n+1}) = (p^{n+1}, d)$ et on obtient facilement que $a \in \mathrm{Ker}(\varphi_x) \iff a \in (p)$, donc φ_x est injectif et est un isomorphisme. Sinon, p étant irréductible, le p.g.c.d. de p^{n+1} et d est de la forme p^r avec $r \in \mathbb{N}$, $r \leqslant n$, de sorte que $ap^n \in (p^r) = (p^{n+1}, d)$ pour tout $a \in A$. Ainsi φ_x est nul, et étant surjectif, on a $p^n M/p^{n+1}M = (0)$. □

Théorème C.10 (Unicité des facteurs invariants)**.** Soient $r, s \in \mathbb{N}^*$. On considère deux suites $(a_1) \supset \cdots \supset (a_r)$ et $(b_1) \supset \cdots \supset (b_s)$ d'idéaux de A distincts de A. Si les A-modules $\bigoplus_{i=1}^{r} A/(a_i)$ et $\bigoplus_{j=1}^{s} A/(b_j)$ sont isomorphes, alors $r = s$ et, pour $1 \leqslant i \leqslant r$, $(a_i) = (b_i)$.

Démonstration du théorème. On peut toujours supposer que $r \leqslant s$. Mais alors, quitte à rajouter à la fin de la liste $(a_1) \supset \cdots \supset (a_r)$ des idéaux égaux à $\{0\}$, on peut supposer que $r = s$.

Pour $1 \leqslant i \leqslant r$, on pose $M_i = A/(a_i)$. En outre, posons $M = \oplus_{i=1}^{r} M_i$. Soit $p \in A$ irréductible. Le lemme précédent assure que l'on a un isomorphisme de A-modules :

$$p^n M/p^{n+1}M \cong \bigoplus_{i=1}^{r} p^n M_i/p^{n+1}M_i.$$

D'après le lemme **C.9**, le A-module $p^n M/p^{n+1}M$ est isomorphe au A-module $(A/(p))^t$ où t est le cardinal de l'ensemble $\{i \in \{1,\dots,r\}; p^{n+1}|a_i\}$. De plus, comme A est principal, l'anneau $A/(p)$ est un corps et les A-modules $p^n M/p^{n+1}M$ et $(A/(p))^t$ (isomorphes en tant que A-modules) sont des $A/(p)$-espaces vectoriels, isomorphes en tant que $A/(p)$-espaces vectoriels.

Soit à présent i entier tel que $1 \leqslant i \leqslant r$. Puisque $a_1 \mid \dots \mid a_i \mid \dots \mid a_r$, ce qui précède montre donc que, pour tout irréductible p dans A et tout $n \in \mathbb{N}$,

$$p^{n+1}|a_i \iff \dim_{A/(p)} p^n M/p^{n+1}M \geqslant r+1-i.$$

Bien sûr, on a de même que, pour tout irréductible p dans A et tout $n \in \mathbb{N}$,

$$p^{n+1}|b_i \iff \dim_{A/(p)} p^n M/p^{n+1}M \geqslant r+1-i.$$

Finalement, on a montré que, pour tout irréductible p dans A et tout $n \in \mathbb{N}$,

$$p^{n+1}|a_i \iff p^{n+1}|b_i.$$

En écrivant les décompositions de a_i et b_i en produit de facteurs irréductibles, on en déduit que $(a_i) = (b_i)$. □

Théorème C.11 (Unicité des diviseurs élémentaires)**.** Si M est un A-module de type fini avec

$$M \cong A^s \oplus (\oplus_{i\in I} A/(p_i^{r_i})) \cong A^{s'} \oplus (\oplus_{i\in I'} A/((p'_i)^{r'_i}))$$

où $s, s' \in \mathbb{N}$, I, I' sont des ensembles finis, les p_i et les p'_i sont des irréductibles de A et les $r_i, r'_i \in \mathbb{N}^*$, alors $s = s'$ et il existe une bijection $\tau : I \longrightarrow I'$ telle que $\forall i \in I$, on a $p_i \sim p'_{\tau(i)}$ et $r_i = r'_{\tau(i)}$.

Preuve. Un isomorphisme de A-modules $M \cong N$ induit des isomorphismes $M/T(M) \cong N/T(N)$ et $T(M) \cong T(N)$. Donc l'isomorphisme du théorème induit des isomorphismes

$$A^s \cong A^{s'} \text{ et } \oplus_{i\in I} A/(p_i^{r_i}) \cong \oplus_{i\in I'} A/((p'_i)^{r'_i})$$

Donc $s = s'$ par l'unicité du cardinal d'une base d'un module libre (A est commutatif). Pour $p \in A$ irréductible et $n \in \mathbb{N}^*$, soit $f(p,n)$ le nombre d'indices $i \in I$ tels que $p_i \sim p$ et $r_i = n$ et soit $f'(p,n)$ est le nombre d'indices $i \in I'$ tels que $p'_i \sim p$ et $r'_i = n$. Il s'agit de montrer que $f(p,n) = f'(p,n)$ pour tout p et tout n.

Si on pose $E = \oplus_{i\in I} A/(p_i^{r_i})$, le lemme C.9 assure pour tout irréductible p de A et tout $n \in \mathbb{N}^*$, on a $\dim_{A/(p)}(p^{n-1}E/p^nE) = d(p,n)$, où $d(p,n)$ est le nombre d'indices $i \in I$ tels que $p_i \sim p$ et $r_i \geq n$. En définissant de même $d'(p,n)$ comme le nombre d'indices $i' \in I'$ tels que $p'_i \sim p$ et $r'_i \geq n$, on obtient $d(p,n) = d'(p,n)$. Finalement on a $f(p,n) = d(p,n) - d(p,n+1) = d'(p,n) - d'(p,n+1) = f'(p,n)$, ce qui donne le résultat. □

D Application à la réduction des endomorphismes d'un espace vectoriel

On va appliquer les résultats précédents à la réduction des endomorphismes d'un espace vectoriel. Dans la suite K est un corps. On s'intéresse aux problèmes (reliés) suivants. Soit E un K-espace vectoriel de dimension finie.

1. Soit $u \in \mathrm{End}_K(E)$. Trouver une base de E dans laquelle la matrice de u est la plus simple possible.
2. Soient $u, v \in \mathrm{End}_K(E)$. Trouver une condition nécessaire et suffisante pour que u et v soient conjugués (similaires), c'est-à-dire qu'il existe $w \in \mathrm{GL}(E)$ tel que $u = w \circ u \circ w^{-1}$.

Voici le résultat de base.

Proposition D.1. Soient E un K-espace vectoriel de dimension finie, et $u \in \mathrm{End}_K(E)$. Soit $\varphi : K[X] \longrightarrow \mathrm{End}_K(E)$ l'unique morphisme de K-algèbres tel que $\varphi(X) = u$. Pour $P \in K[X]$, on écrit $P(u) = \varphi(P)$.

1. Le morphisme d'algèbres $\varphi : K[X] \longrightarrow \mathrm{End}_K(E)$ est non injectif. Il existe donc un unique polynôme unitaire $P_u \in K[X]$ tel que $\mathrm{Ker}(\varphi) = (P_u)$. Le polynôme P_u est le polynôme minimal de u.
2. Le morphisme d'algèbres $\varphi : K[X] \longrightarrow \mathrm{End}_K(E)$ munit E d'une structure de $K[X]$-module, définie par $\forall x \in E, \forall P \in K[X], P.x = P(u)(x)$. Un sous-espace de E est stable par u si et seulemement si c'est un sous-$K[X]$-module.
3. Soient $u, v \in \mathrm{End}_K(E)$. Notons E_u et E_v les structures respectives de $K[X]$-modules sur E que l'on vient de définir. Alors u et v sont conjugués si et seulement si les $K[X]$-modules E_u et E_v sont isomorphes.

Preuve. 1. Le morphisme d'algèbres φ est non injectif car $\mathrm{End}_K(E)$ est un K-espace vectoriel de dimension finie. $\mathrm{Ker}(\varphi)$ est un idéal de $K[X]$, donc l'existence du polynme minimal P_u de u provient du fait que $K[X]$ est principal.
2. La deuxième assertion est immédiate car $X.x = u(x)$ pour tout $x \in E$ (on note également que $\mathrm{Ker}(\varphi) = \mathrm{Ann}_{K[X]}(E_u)$).
3. Soit $f : E \longrightarrow E$ une application K-linéaire. Si f est un morphisme de $K[X]$-modules $E_u \longrightarrow E_v$, on a $\forall x \in E, f(X.x) = X.f(x)$, c'est-à-dire $f \circ u = v \circ f$. Donc si f est un isomorphisme de $K[X]$-modules $E_u \longrightarrow E_v$, alors u et v sont conjugués. Réciproquement, s'il existe $f \in \mathrm{GL}(E)$ tel que $v = f \circ u \circ f^{-1}$, on a pour tout $P \in K[X]$, $f \circ P(u) = P(v) \circ f$, ce qui montre que f est un isomorphisme $E_u \cong E_v$. □

Les théorèmes de structures des $K[X]$-modules se traduisent ainsi.

Théorème D.2. Soient E un K-espace vectoriel de dimension finie, et $u \in \mathrm{End}_K(E)$.

1. Il existe des polynômes unitaires irréductibles $P_1, \ldots, P_s \in K[X]$, et des entiers $m_1, \ldots, m_s \geq 1$ tels que l'on a un isomorphisme de $K[X]$-modules

$$E_u \cong K[X]/(P_1^{m_1}) \oplus \cdots \oplus K[X]/(P_s^{m_s})$$

avec $P_u = \mathrm{PPCM}(P_1^{m_1}, \ldots, P_s^{m_s})$. Les polynômes $P_1^{m_1}, \ldots, P_s^{m_s}$ sont appelés les diviseurs élémentaires associés à u. Deux endomorphismes de E sont conjugués si et seulement si ils ont les mêmes diviseurs élémentaires associés (à l'ordre près).

2. Il existe une unique famille de polynômes unitaires $(Q_1, \ldots Q_r)$ non constants tels que

$$E_u \cong K[X]/(Q_1) \oplus \cdots \oplus K[X]/(Q_r)$$

et $Q_1 | Q_2 | \cdots | Q_r$, et on a $P_u = Q_r$. Les polynômes $Q_1, \ldots, Q_r$ sont appelés les facteurs invariants de u. Deux endomorphismes de E sont conjugués si et seulement si ils ont les mêmes facteurs invariants.

Preuve. 1. On applique le théorème de structure des $K[X]$-modules de type fini en version diviseurs élémentaires. Comme E_u est de dimension finie, il n'y a pas de partie libre et on obtient donc l'isomorphisme annoncé. On a $\mathrm{Ann}_{K[X]}(E_u) = (P_u)$, et puisqu'en général si A est un anneau principal on a $\mathrm{Ann}(A/(a_1) \oplus \cdots \oplus A/(a_m)) = (\mathrm{PPCM}(a_1, \ldots a_m))$, on obtient la deuxème assertion. Soient $u, v \in \mathrm{End}_K(E)$. Alors u et v sont conjugués si et seulement si les $K[X]$-modules E_u et E_v sont isomorphes, et le résultat d'unicité des diviseurs élémentaires pour les $K[X]$-modules de type fini donne le résultat.
2. La preuve est similaire en utilisant le théorème de structure des $K[X]$-modules de type fini en version facteurs invariants. □

Comme première application, on a le résultat suivant.

Corollaire D.3. Soit E un K-espace vectoriel de dimension finie et soit $u \in \mathrm{End}_K(E)$. Alors u est diagonalisable si et seulement si P_u est scindé sur K à racines simples.

Preuve. S'il existe une base de E dans laquelle la matrice de u est diagonale, on voit facilement que P_u divise un polynôme scindé à racines simples sur K, et est donc scindé à racines simples. Réciproquement supposons P_u est scindé à racines simples. On a

$$E_u \cong K[X]/(P_1^{m_1}) \oplus \cdots \oplus K[X]/(P_s^{m_s})$$

avec $P_1, \ldots, P_s$ unitaires irréductibles et $P_u = \mathrm{PPCM}(P_1^{m_1}, \ldots, P_s^{m_s})$. L'hypothèse sur P_u assure que $m_1 = \cdots = m_s = 1$ et que chaque P_i est de degré 1. Donc chaque sous $K[X]$-module $K[X]/(P_i)$ est un K-espace vectoriel de dimension 1 et on a le résultat. □

On s'intéresse maintenant au premier problème : trouver une base de E dans laquelle la matrice de $u \in \mathrm{End}_K(E)$ est la plus simple possible. La première version, la forme canonique de Jordan, ne fonctionne bien en général que si le corps de base algébriquement clos. La deuxième version, la forme canonique rationnelle, qui utilise les facteurs invariants du $K[X]$-module E_u, fonctionne sur n'importe quel corps.

D.1 Forme canonique de Jordan

Définition D.4. *Une **matrice de Jordan élémentaire** est une matrice de la forme*

$$J_\lambda = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & \ddots & & \vdots \\ \vdots & & \ddots & 1 & 0 \\ & & & \lambda & 1 \\ 0 & \cdots & & 0 & \lambda \end{pmatrix}, \quad \lambda \in K$$

*où les coefficients non indiqués sont nuls. On dit qu'une matrice est en **forme canonique de Jordan** si elle est diagonale par blocs, les blocs étant des matrices de Jordan élémentaires.*

Théorème D.5. Soit E un K-espace vectoriel de dimension finie, et soit $u \in \mathrm{End}_K(E)$. Les assertions suivantes sont équivalentes.

1. Il existe une base de E dans laquelle la matrice de u est en forme canonique de Jordan.
2. Le polynômes minimal P_u de u est scindé sur K.

Preuve. S'il existe une base de E dans laquelle la matrice de u est en forme canonique de Jordan, on voit facilement que P_u divise un polynôme scindé sur K, et est donc scindé.

Réciproquement, en gardant les notations précédentes, soit

$$\Psi : E_u \longrightarrow K[X]/(P_1^{m_1}) \oplus \cdots \oplus K[X]/(P_s^{m_s})$$

un isomorphisme de $K[X]$-modules, avec $P_1, \ldots, P_s$ unitaires irréductibles et $P_u = \mathrm{PPCM}(P_1^{m_1}, \ldots, P_s^{m_s})$. Si P_u est scindé sur K, il suit que les P_i sont de degré 1 et donc on a un isomorphisme de $K[X]$-modules

$$\Psi : E_u \longrightarrow K[X]/((X-\lambda_1)^{m_1}) \oplus \cdots \oplus K[X]/((X-\lambda_s)^{m_s})$$

Pour $i \in \{1, \ldots, n\}$, notons $E_i = \Psi^{-1}(K[X]/((X-\lambda_i)^{m_i}))$. Chaque E_i est un sous-$K[X]$-module de E, donc est stable par u, et on a $E = E_1 \oplus \cdots \oplus E_s$ comme $K[X]$-module. Il suffit donc de montrer que pour tout i, il existe une base de E_i dans laquelle la matrice de $u_{|E_i}$ soit une matrice de Jordan élémentaire. On utilise le lemme suivant.

Lemme D.6. Soit $\lambda \in K$ et $r \geq 1$. Considérons le $K[X]$-module $K[X]/((X-\lambda)^r)$ (qui est aussi un anneau et un K-espace vectoriel) et notons x la classe de X dans $K[X]/((X-\lambda)^r)$. Pour $k \in \{1, \ldots, r\}$, notons $e_k = (x-\lambda)^{r-k}$. Alors $\{e_1, \ldots, e_r\}$ est une base du K-espace vectoriel $K[X]((X-\lambda)^r)$, avec $X.e_1 = \lambda e_1$ et pour $k \geq 2$, $X.e_k = e_{k-1} + \lambda e_k$

Preuve du lemme. On vérifie facilement, par division euclidienne, que $\dim_K(K[X]/((X-\lambda)^r)) \leq r$, et un argument de degré montre que $e_1, \ldots, e_r$ est une famille libre. Ainsi on a $\dim_K(K[X]/((X-\lambda)^r)) = r$, et $\{e_1, \ldots, e_r\}$ est une base. On a

$$X.e_1 = X.(x-\lambda)^{r-1} = x(x-\lambda)^{r-1} = (x-\lambda+\lambda)(x-\lambda)^{r-1} = (x-\lambda)^r + \lambda(x-\lambda)^{r-1} = \lambda e_1$$

et pour $k \geq 2$

$$X.e_k = x(x-\lambda)^{r-k} = (x-\lambda+\lambda)(x-\lambda)^{r-k} = (x-\lambda)^{r-k+1} + \lambda(x-\lambda)^{r-k} = e_{k-1} + \lambda e_k \ \square$$

On termine maintenant aisément la preuve du théorème : pour chaque i on transporte la base précedente du lemme via Ψ pour obtenir une base $f_1, \ldots, f_{m_i}$ de E_i telle $u(f_1) = \lambda_i f_1$ et pour $k \geq 2$, $u(f_k) = f_{k-1} + \lambda_i f_k$, et la matrice de $u_{|E_i}$ dans cette base est une matrice de Jordan élémentaire. $\square$

Théorème D.7. Soit E un K-espace vectoriel de dimension finie, avec K algébriquement clos, et soit $u \in \mathrm{End}_K(E)$. Alors il existe une base de E dans laquelle la matrice de u est en forme canonique de Jordan. Deux endomorphismes de E sont conjugués si et seulement si il ont la même forme canonique de Jordan (à permutation des blocs de Jordan près).

Preuve. Le polynôme minimal de u est scindé sur K, on applique donc le théorème précédent. On a vu dans la preuve du théorème précédent que la forme canonique de Jordan de u est complètement déterminée par l'isomorphisme de $K[X]$-modules

$$\Psi : E_u \longrightarrow K[X]/((X-\lambda_1)^{m_1}) \oplus \cdots \oplus K[X]/((X-\lambda_s)^{m_s})$$

L'unicité de la forme canonique de Jordan est donc une conséquence de l'unicité des diviseurs élémentaires dans le théorème de structure des $K[X]$-modules de type fini. □

L'existence d'une base dans laquelle la matrice de $u \in \mathrm{End}_K(E)$ est en forme canonique de Jordan est un résultat théorique. En pratique on utilise le **polynôme caractérique de** u, défini par $\chi_u(X) = \det(M - XI_n)$ (où M est la matrice de u dans n'importe quelle base et $n = \dim(E)$). Les valeurs propres de u sont exactement les racines de χ_u dans K (ce sont également exactement les racines du polynôme minimal P_u dans K).

Théorème D.8 (Cayley-Hamilton)**.** Pour $u \in \mathrm{End}_K(E)$, on a $\chi_u(u) = 0$, et donc le polynôme minimal de u divise χ_u.

Preuve. Le résultat est facile à vérifier si la matrice de u dans une base est en forme canonique de Jordan, donc on a le résultat si K est algébriquement clos. Sinon, soit $\overline{K}$ une clôture algébrique de K. On fixe une base $\mathcal{B}$ de E, et soit $\overline{u} : \overline{K}^n \longrightarrow \overline{K}^n$ ($n = \dim_K(E)$) l'endomorphisme dont la matrice M dans la base canonique est la matrice de u dans la base $\mathcal{B}$. Alors $\chi_{\overline{u}}(X) = \det(M - XI_n) = \chi_u(X)$. Par le cas K algébriquement clos on a $0 = \chi_{\overline{u}}(\overline{u}) = \chi_u(M) = \chi_u(u)$. □

Enfin, pour mettre un endomorphisme en forme canonique de Jordan, on utilise le résultat suivant.

Proposition D.9 (lemme des noyaux)**.** Soit $P \in K[X]$ avec $P = P_1 \cdots P_r$ où les P_i sont premiers entre eux deux à deux. Pour $u \in \mathrm{End}_K(E)$, on a

$$\mathrm{Ker}(P(u)) = \mathrm{Ker}(P_1(u)) \oplus \cdots \oplus \mathrm{Ker}(P_(u))$$

Preuve. Le résultat est une application du théorème de Bezout aux polynômes $Q_1, \ldots, Q_r$ définis par $Q_i = \prod_{j \neq i} P_j$, qui sont premiers entre eux. Les détails sont laissés en exercice. □

On obtient finalement :

Méthode pour mettre un endomorphisme en forme canonique de Jordan.

1. On calcule χ_u, que l'on décompose

$$\chi_u(X) = (X-\lambda_1)^{m_1} \cdots (X-\lambda_r)^{m_r}, \lambda_1, \ldots \lambda_r \in K, \lambda_i \neq \lambda_j \text{si } i \neq j, \;\; m_1, \ldots, m_r \in \mathbb{N}^*$$

2. On peut alors déterminer P_u, qui se décompose

$$P_u(X) = (X-\lambda_1)^{p_1} \cdots (X-\lambda_r)^{p_r}, \; 0 < p_i \leq m_i, \; \forall i$$

3. Le lemme des noyaux assure alors que l'on a une décomposition en sous-espaces caractéristiques
$$E_u \cong \mathrm{Ker}((u-\lambda_1)^{p_1}) \oplus \cdots \oplus \mathrm{Ker}((u-\lambda_r)^{p_r})$$
On détermine les espaces caractéristiques, et on travaille enfin sur chaque espace caractéristique pour trouver une base dans laquelle la matrice de u est en forme canonique de Jordan (le nombre de blocs de Jordan pour $u_{|\mathrm{Ker}((u-\lambda_1)^{p_1})}$ est égal à $\dim(\mathrm{Ker}(u-\lambda_1))$). En petite dimension cela peut se faire "à la main", en étudiant la suite de sous-espaces $\mathrm{Ker}(u-\lambda_1)) \subset \mathrm{Ker}(u-\lambda_1)^2) \subset \ldots \subset \mathrm{Ker}(u-\lambda_1)^{p_1})$, et sinon la méthode des facteurs invariants fonctionne aussi, voir le paragraphe suivant.

D.2 Facteurs invariants et forme canonique rationnelle

Définition D.10. *Soit $Q(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0 \in K[X]$ un polynôme unitaire. La matrice*
$$\mathcal{C}(Q) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ & & & & -a_1 \\ & I_{m-1} & & & \vdots \\ & & & & -a_{m-1} \end{pmatrix} \in \mathcal{M}_m(K)$$
*est appelée la **matrice compagnon** de Q.*

Proposition D.11. Pour $Q(X) \in K[X]$ un polynôme unitaire, le polynôme caractéristique de la matrice $\mathcal{C}(Q)$ est égal à $(-1)^{\deg Q}Q : \chi_{\mathcal{C}(Q)} = (-1)^{\deg Q}Q$.

Preuve. Exercice. □

Définition D.12. *On dit qu'une matrice est en **forme canonique rationnelle** si elle est de la forme*
$$\mathcal{C}(Q_1, \ldots, Q_r) := \begin{pmatrix} \mathcal{C}(Q_1) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \mathcal{C}(Q_r) \end{pmatrix}.$$
pour des polynômes unitaires $Q_1, \ldots, Q_r$ tels que $Q_1|Q_2|\cdots|Q_r$

Théorème D.13 (Forme canonique rationnelle d'un endomorphisme)**.** Soit $u \in \mathrm{End}_K(E)$. Alors il existe une base de E dans laquelle la matrice de u est en forme canonique rationnelle. Plus précisément si $Q_1, \ldots, Q_r$ sont les facteurs invariants de u, il existe une base de E dans laquelle la matrice de u est
$$\mathcal{C}(Q_1, \ldots, Q_r) := \begin{pmatrix} \mathcal{C}(Q_1) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \mathcal{C}(Q_r) \end{pmatrix}.$$
Réciproquement les facteurs invariants d'une telle matrice sont $Q_1, \ldots, Q_r$.

Preuve. Supposons d'abord que $r = 1$. Dans ce cas $E_u \cong K[X]/(Q_1)$, et il existe $e \in E$ tel que $E_u = K[X]e$. Soit $m = \deg(Q_1)$. Le polynôme minimal de u est Q_1.

Vérifions $\{e, u(e), \dots, u^{m-1}(e)\}$ est une base de E. Tout élément $x \in E$ est de la forme $x = P.e = P(u)(e)$ pour un polynôme $P \in K[X]$ car $E_u = K[X]u$. Soient $R, S \in K[X]$ tels que $P = Q_1R + S$ avec $\deg(S) < m$. Alors $x = P.e = (RQ_1).e + S.e = R(u)Q_1(u)(e) + S(u)(e) = S(u)(e)$, ce qui montre que x est combinaison linéaire de $e, u(e), \dots, u^{m-1}(e)$. Si maintenant $\lambda_0, \dots, \lambda_{m-1} \in K$ vérifient $\sum_{i=0}^{m-1} \lambda_i u^i(e) = 0$, posons $R(X) = \sum_{i=0}^{m-1} \lambda_i X^i$. On a alors $R.e = 0$, d'où puisque $E_u = K[X]e$, $R \in \mathrm{Ann}_{K[X]}(E_u) = (Q_1)$ et donc Q_1 divise R et ainsi si $R \neq 0$ on a $\deg(Q_1) \leq \deg(R)$. Or ona $\deg(R) \leq m - 1 < \deg(Q_1)$, donc $R = 0$ et $\lambda_0 = \cdots = \lambda_{m-1} = 0$.

On vérifie alors sans difficulté que la matrice de u dans la base $\{e, u(e), \dots, u^{m-1}(e)\}$ est $\mathcal{C}(Q_1)$. Le cas général se déduit du cas $r = 1$: si $E_u \cong K[X]/(Q_1) \oplus \ldots \oplus K[X]/(Q_r)$, on obtient la base voulue en faisant la réunion des bases des sous-espaces $K[X]/(Q_i)$.

Réciproquement, si la matrice dans une base de u est $\mathcal{C}(Q)$, alors cette base est de la forme $\{e, u(e), \dots, u^{m-1}(e)\}$ ($m = \deg(Q)$) pour un certain $e \in E$ et alors l'application $K[X]$-linéaire $K[X] \longrightarrow E_u$, $P \longmapsto P(u)(e)$ induit un isomorphisme $K[X]/(Q) \cong E_u$, ce qui montre que Q est l'unique facteur invariant de u. Dans le cas général, si $\mathcal{C}(Q_1, \dots, Q_r)$ est la matrice de u dans une base, alors l'argument précédent va assurer que $E_u \cong K[X]/(Q_1) \oplus \ldots \oplus K[X]/(Q_r)$ et donc $Q_1, \dots, Q_r$ sont bien les facteurs invariants de u. □

Corollaire D.14. Deux endomorphismes de E sont conjugués si et seulement si ils ont la même forme canonique rationnelle.

Proposition D.15 (Recherche pratique des facteurs invariants)**.** Soit $u \in \mathrm{End}_K(E)$. Soit $\mathcal{B} = \{e_1, \dots, e_n\}$ une base de E comme K-espace vectoriel et soit M la matrice de u dans la base $\mathcal{B}$. Pour trouver les facteurs invariants de u (ou de M), on applique les operations élémentaires sur les lignes et les colonnes pour touver les facteurs invariants de la matrice ${}^tM - XI_n \in \mathcal{M}_n(K[X])$.
Plus précisément, soit $\{\varepsilon_1, \dots, \varepsilon_n\}$ une base du $K[X]$-module libre $K[X]^n$ et soit $\theta : K[X]^n \longrightarrow E_u$ l'unique application $K[X]$-linéaire qui envoie ε_i sur e_i, pour tout i. Alors la matrice des relations du $K[X]$-module E_u relative à $\{\varepsilon_1, \dots, \varepsilon_n\}$ est ${}^tM - XI_n$.

Preuve. Ecrivons $A = K[X]$. Le A-module E_u est de type fini. On l'écrit comme le quotient d'un A-module libre : $\mathcal{B}$ engendre E_u comme A-module, donc E_u est un quotient de A^n. Notons $\{\varepsilon_1, \dots, \varepsilon_n\}$ une base du A-module libre A^n. Soit $\theta : A^n \twoheadrightarrow E$ le morphisme de A-modules défini par $\theta(\varepsilon_i) = e_i$ pour tout i. Alors $E \cong A^n / \operatorname{Ker}\theta$.

Posons $M = (a_{ij})_{1 \leqslant i,j \leqslant n}$. Alors $u(e_i) = \sum_j a_{ji} e_j$ pour tout i, c'est-à-dire que $\sum_j a_{ji} e_j - X e_i = 0$, donc pour tout i l'élément $x_i = \sum_j a_{ji}\varepsilon_j - X\varepsilon_i$ est dans le noyau de θ. Les coordonnées de x_i dans la base $\{\varepsilon_1, \dots, \varepsilon_n\}$ forment la ligne i de ${}^tM - XI_n$. Donc pour conclure, il nous faut montrer que les x_i engendrent $\operatorname{Ker}\theta$. On a déjà l'inclusion $\sum_{i=1}^n Ax_i \subset \operatorname{Ker}\theta$.

On vient de voir que pour tout i, $X\varepsilon_i$ est dans $(\oplus_{j=1}^n K\varepsilon_j) + \sum_{i=1}^n Ax_i$, donc par récurrence, on peut dire de même pour tout $X^m\varepsilon_i$ et donc pour tout $P(X)\varepsilon_i$ avec $P(X) \in A$. Soit maintenant $z \in \operatorname{Ker}\theta$. Puisque $\{\varepsilon_1, \dots, \varepsilon_n\}$ est une base du A-module A^n, on peut écrire $z = \sum_i P_i(X)\varepsilon_i$ avec $P_i \in A$. D'après ce qui précède, on peut donc écrire $z = \sum_{i=1}^n \lambda_i \varepsilon_i + y$ avec $y \in Ax_1 + \cdots + Ax_n$ et $\lambda_i \in k$. On sait déjà que $y \in \operatorname{Ker}\theta$ par l'inclusion que l'on a déjà montrée, donc on a aussi $\sum_{i=1}^n \lambda_i \varepsilon_i = z - y \in \operatorname{Ker}\theta$. Donc en appliquant θ on a $\sum_{i=1}^n \lambda_i e_i = 0$. Or $\{e_1, \dots, e_n\}$ est une K-base de E, donc tous les λ_i sont nuls et donc $z = y \in Ax_1 + \cdots + Ax_n$.

Finalement on a bien $\operatorname{Ker}\theta = Ax_1 + \cdots + Ax_n$. □

Exemple D.16. Soit $u \in \mathrm{End}(K^3)$ dont la matrice dans la base canonique $\{e_1, e_2, e_3\}$ est $T = \begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 0 \\ 1 & -1 & 0 \end{pmatrix}$. On veut trouver les facteurs invariants de u.

On considère donc la matrice ${}^tT - XI_3 = \begin{pmatrix} 1-X & 1 & 1 \\ -1 & -1-X & -1 \\ 1 & 0 & -X \end{pmatrix}$. Les opérations suivantes : $C_2 \leftrightarrow C_1$; $L_2 \to L_2 + (X+1)L_1$; $C_2 \to C_2 - (1-X)C_1$; $C_3 \to C_3 - C_1$; $L_2 \leftrightarrow L_3$; $C_3 \to C_3 + XC_2$; $L_3 \to L_3 + X^2L_2$; $C_3 \to -C_3$ donnent la matrice $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & X^3 - X \end{pmatrix}$.

On en déduit que les facteurs invariants de u sont $X^3 - X$ et que $K^3_u \cong K[X]/(X^3 - X)$.

La matrice compagnon de $X^3 - X$ est $\mathcal{C}_{X^3-X} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

Soit $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ la base canonique de $K[X]^3$, et considérons l''application $K[X]$-linéaire $\theta : K[X]^3 \longrightarrow K^3_u$, $\varepsilon_i \mapsto e_i$. La base $\{\tilde{\varepsilon_1}, \tilde{\varepsilon_2}, \tilde{\varepsilon_3}\}$ de $K[X]^3$ adaptée à $\mathrm{Ker}(\theta)$ est obtenue grâce à la matrice Q^{-1} (voir le paragraphe sur le théorème de la base adaptée). Ici $Q^{-1} = \begin{pmatrix} 1-X & 1 & 1 \\ 1 & 0 & -X \\ 0 & 0 & -1 \end{pmatrix}$, donc la nouvelle base est donnée par $\tilde{\varepsilon_1} = (1-X)\varepsilon_1 + \varepsilon_2 + \varepsilon_3$, $\tilde{\varepsilon_2} = \varepsilon_1 - X\varepsilon_3$ et $\tilde{\varepsilon_3} = -\varepsilon_3$. Alors on a $\theta(\tilde{\varepsilon_1}) = \theta(\tilde{\varepsilon_2}) = 0$ et $\theta(\tilde{\varepsilon_3}) = -e_3$ et θ induit un isomorphisme de $K[X]$-modules $K[X]/(X^3 - X) \cong E_u$, et $\{e_3, u(e_3) = e_1, u^2(e_3) = e_1 + e_2 + e_3\}$ est une base de K^3 dans laquelle la matrice de u est $\mathcal{C}_{X^3-X}$

Remarque. Dans l'exemple précédent, le calcul des facteurs invariant assure que $X^3 - X$ est le polynôme minimal de u, donc u est en fait diagonalisable.

Remarque D.17. A partir de la forme de Jordan, on peut retrouver les facteurs invariants.

On construit un tableau de la façon suivante :

1. A chaque valeur propre λ_{ij} on associe une ligne : on remplit les lignes avec les $(X - \lambda_{ij})^{n_{ij}}$ avec les n_{ij} en ordre décroissant (n_{ij} est la taille du bloc de Jordan), et on complète avec des 1 pour avoir des lignes de même longueur.
2. Pour obtenir les facteurs invariants, on fait le produit colonne par colonne.

Exemple D.18. Les diviseurs élémentaires (polynômes unitaires égaux au signe près aux

polynômes caractéristiques des blocs de Jordan) de

$$\begin{pmatrix} \boxed{2} & 0 & 0 & 0 & 0 \\ & \boxed{\begin{matrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{matrix}} & & & \\ 0 & & 0 & 0 & 0 \\ & & \boxed{2} & & \\ 0 & 0 & & \boxed{\begin{matrix} 3 & 1 \\ 0 & 3 \end{matrix}} & 0 \\ & & & & \boxed{\begin{matrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{matrix}} \\ 0 & 0 & 0 & 0 & \end{pmatrix}$$

sont $X-2$, $(X-3)^3$, $X-2$, $(X-3)^2$ et $(X-3)^3$.

$\lambda = 2$	$X-2$	$X-2$	1
$\lambda = 3$	$(X-3)^3$	$(X-3)^3$	$(X-3)^2$
Résultat	$(X-2)(X-3)^3$ (Q_3)	$(X-2)(X-3)^3$ (Q_2)	$(X-3)^2$ (Q_1)

Les facteurs invariants sont Q_1, Q_2, Q_3.

VII Représentations linéaires des groupes finis

A Introduction

Dans ce chapitre on étudie les représentations linéaires des groupes finis, qui sont les modules sur l'algèbre du groupe $\mathbb{C}[G]$. On n'utilisera pas (ou peu) la langage des modules, ce qui rend ce chapitre essentiellement indépendant des précédents (à la construction de l'algèbre du groupe près).

On a en vue deux applications. La première concerne la srtucture de l'algèbre d'un groupe fini. Rappelons que si G est un groupe, l'algèbre du groupe G, notée $\mathbb{C}[G]$, est l'espace vectoriel des fonctions à support fini $G \longrightarrow \mathbb{C}$ (de base $\{e_g,\ g \in G\}$), muni du produit défini par $e_g * e_h = e_{gh}$, $\forall g, h \in G$.

Théorème A.1. Soit G un groupe fini. On a un isomorphisme d'algèbres

$$\mathbb{C}[G] \cong \prod_{i=1}^{r} \mathcal{M}_{n_i}(\mathbb{C})$$

où r est le nombre de classes de conjugaison de G et $n_1, \ldots, n_r \in \mathbb{N}^*$.

Ce résultat, assez surprenant au premier abord, est une conséquence de la théorie des représentations linéaires de G. La deuxième application est une application interne à la théorie des groupes.

Théorème A.2 (Théorème "pq" de Burnside)**.** Soient p et q des nombres premiers. Soit G un groupe d'ordre $p^\alpha q^\beta$ où $\alpha, \beta \in \mathbb{N}$ vérifient $\alpha + \beta \geq 2$. Alors le groupe G n'est pas simple.

B Définitions

Le corps de base est $K = \mathbb{C}$. On considère un groupe G.

Définition B.1. *Une **représentation linéaire** de G est un couple (V, π_V) où V est un espace vectoriel de dimension finie et où $\pi_V : G \longrightarrow \mathrm{GL}(V)$ est un morphisme de groupes.*

Remarques. 1. On peut aussi définir des représentations linéaires avec un corps de base K quelconque, ainsi que sur des espaces vectoriels de dimension infinie. Nous limiterons au cadre de la définition.
2. Si G est un sous-groupe de $\mathrm{GL}(V)$, alors (V, i), où i est l'injection $G \hookrightarrow \mathrm{GL}(V)$ est une représentation linéaire de G.

3. Soit $\pi : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$ un morphisme de groupes. En identifiant $\mathrm{GL}_n(\mathbb{C})$ et $\mathrm{GL}(\mathbb{C}^n)$, on a une représentation linéaire $(\pi, \mathbb{C}^n)$ de G.
4. Si (V, π_V) est une représentation de G, alors le morphisme de groupes $\pi_V : G \longrightarrow \mathrm{GL}(V)$ induit un morphisme d'algèbres $\widetilde{\pi_V} : \mathbb{C}[G] \longrightarrow \mathrm{End}_{\mathbb{C}}(V)$ et donc une structure de $\mathbb{C}[G]$-module sur V. Réciproquement un tel morphisme d'algèbres induit, par restriction à G, une représentation linéaire de G. La théorie des représentations linéaires d'un groupe G est donc la même que celle des $\mathbb{C}[G]$-modules. Dans la suite on n'utilisera pas le langage des modules.

Définition B.2. *Un G-**espace** est un espace vectoriel de dimension finie V muni d'une opération de G sur V*

$$\begin{aligned} G \times V &\longrightarrow V \\ (g, v) &\longmapsto g.v \end{aligned}$$

telle que $\forall g \in G, \forall v_1, v_2 \in V, \forall \lambda \in \mathbb{C}$,

$$g.(v_1 + v_2) = g.v_1 + g.v_2, \quad g.(\lambda v) = \lambda(g.v).$$

Proposition B.3. Les notions de G-espace et de représentation linéaire de G sont équivalentes.
Si V est un G-espace, on obtient un morphisme de groupe

$$\begin{aligned} \pi_V : G &\longrightarrow \mathrm{GL}(V) \\ g &\longmapsto \pi_V(g),\ \pi_V(g)(v) = g.v, \forall v \in V \end{aligned}$$

Réciproquement si (V, π_V) est une représentation linéaire de G, alors on définit sur V une structure de G-espace en posant

$$\begin{aligned} G \times V &\longrightarrow V \\ (g, v) &\longmapsto g.v := \pi_V(g)(v) \end{aligned}$$

Preuve. Si V est un G-espace, on a en particulier une opération de G sur V, et donc le morphisme de groupes annoncé $\pi_V : G \longrightarrow S_V$ dans le groupe symétrique de G. Alors pour tout $g \in G$, l'application π_V est linéaire par les axiomes de G-espace, donc est un élément de $\mathrm{GL}(V)$.

Réciproquement si (V, π_V) est une représentation linéaire de G, on vérifie sans difficulté que la formule donnée muni V d'une structure de G-espace. □

On a donc deux notions équivalentes, que l'on utilisera de façon interchangeable suivant les situations. Plus simplement on dira que V est **une représentation de** G, ce qui signifie que V est un G-espace avec l'opération associée, et que l'on a le morphisme de groupes correspondant $\pi_V : G \longrightarrow \mathrm{GL}(V)$.

Définition B.4. *Soient V et W des représentations de G. Un **morphisme de représentations de V dans W**, ou un **G-morphisme**, est une application linéaire $f : V \longrightarrow W$ telle que*

$$\forall g \in G, \forall v \in V,\ f(g.v) = g.f(v).$$

L'ensemble des morphismes de morphismes de représentations de V dans W est noté $\mathrm{Hom}_G(V, W)$. *C'est un sous-espace vectoriel de* $\mathrm{Hom}(V, W)$ *(exercice).*

Remarque. Au niveau des morphismes de groupes $\pi_V : G \longrightarrow \mathrm{GL}(V)$ et $\pi_W : G \longrightarrow \mathrm{GL}(W)$, dire que f est un morphisme entre V et W signifie que $\forall g \in G$, on $f \circ \pi_V(g) = \pi_W(g) \circ f$, c'est-à-dire que les diagrammes suivants sont commutatifs :

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle \pi_V(g)}\downarrow & & \downarrow{\scriptstyle \pi_W(g)} \\ V & \xrightarrow{f} & W \end{array}$$

On vérifie sans difficulté que la composée de deux G-morphismes est encore un G-morphisme. Un **isomorphisme de représentations**, ou G**-isomorphisme** est un morphisme de représentations qui est bijectif. L'inverse est alors aussi un morphisme de représentations (vérifier).

Définition B.5. *La **dimension** d'une représentation est la dimension de l'espace vectoriel sous-jacent.*

Il est clair que deux représentations isomorphes ont même dimension.

Définition B.6. *Soit (V, π_V) une représentation de G. Le **caractère de** V est la fonction $\chi_V : G \longrightarrow \mathbb{C}$ définie par*

$$\chi_V(g) = \mathrm{Tr}(\pi_V(g)), \quad \forall g \in G.$$

*On dit qu'une fonction $\chi : G \longrightarrow \mathbb{C}$ est un **caractère** si χ est le caractère d'une représentation de G.*

On verra que, de manière un peu surprenante, une représentation linéaire est entièrement déterminée par son caractère.

Définition B.7. *Soit V une représentation de G et soit $W \subset V$ un sous-espace. On dit que W est une **sous-représentation de** V si $\forall g \in G$, $\forall w \in W$, on a $g.w \in W$.*

Il est clair qu'une sous-représentation est elle-même une représentation de G.

Définition B.8. *Soit V une représentation de G. On dit que V est **irréductible** si $V \neq \{0\}$ et si les seules sous-représentations de V sont $\{0\}$ et V.*

On définit une relation d'équivalence sur l'ensemble des représentations de G en posant $V \sim W$ si V et W sont isomorphes. On notera $\mathrm{Irr}(G)$ l'ensemble des classes d'isomorphismes de représentations irréductibles. Pour une représentation V de G, on notera $[V]$ sa classe d'isomorphisme.

L'objectif des paragraphes qui suivent est de décrire la structure des représentations d'un groupe fini.

C Constructions et exemples de représentations

On considère toujours un groupe G.

C.1 Représentations de dimension un

Les représentations de dimension 1 de G correspondent exactement aux morphismes de groupes $\pi : G \longrightarrow \mathbb{C}^*$. En effet, si V est un espace vectoriel de dimension un, le groupe $\mathrm{GL}(V)$ s'identifie à $\mathbb{C}^*$, ainsi un morphisme de groupes $G \longrightarrow \mathrm{GL}(V)$ est exactement un morphisme de groupes $G \longrightarrow \mathbb{C}^*$.

Une représentation de dimension 1 est nécessairement irréductible, puisque les seuls sous-espaces d'un espace de dimension 1 sont $\{0\}$ et lui-même.

Deux représentations de dimension 1 $\pi, \chi : G \longrightarrow \mathbb{C}^*$ sont isomorphes si et seulement si $\pi = \chi$.

On notera $\widehat{G}$ l'ensemble des morphismes de groupes $G \longrightarrow \mathbb{C}^*$, qui s'identifie donc à l'ensemble des représentations de dimension 1 de G. On verra qu'en fait si G est un groupe abélien fini, alors $\widehat{G} = \mathrm{Irr}(G)$.

On notera $\mathbb{I}$ la représentation donné par le morphisme trivial $G \longrightarrow \mathbb{C}^*$, $g \longmapsto 1$. On dit que $\mathbb{I}$ est la **représentation triviale de** G.

On vérifie sans difficulté que la loi

$$\begin{aligned} &\widehat{G} \times \widehat{G} \longrightarrow \widehat{G} \\ &(\phi, \psi) \longmapsto \phi.\psi,\ \phi.\psi(x) = \phi(x)\psi(x),\ \forall x \in G, \end{aligned}$$

munit $\widehat{G}$ d'une structure de groupe abélien.

Théorème C.1. Si G est un groupe fini abélien, alors les groupes G et $\widehat{G}$ sont isomorphes.

Preuve. Etape 1. Supposons d'abord que $G = C_n = \langle x \rangle$ est cyclique d'ordre n. Pour toute racine n-ième de l'unité $\omega \in \mu_n$, on a un unique morphisme de groupes $\phi_\omega : G \longrightarrow \mu_n$ tel que $\phi_\omega(x) = \omega$. Cela donne une application $\mu_n \longrightarrow \widehat{G}$, $\omega \longmapsto \phi_\omega$ qui est un morphisme de groupes, injectif car x engendre G. Réciproquement, si $\phi \in \widehat{G}$, on a $\phi(x)^n = \phi(x^n) = \phi(1) = 1$, donc $\phi(x) \in \mu_n$. Puisque x engendre G, on en déduit que $\phi = \phi_\omega$ pour $\omega = \phi(x)$. Ainsi on a un isomorphisme $\mu_n \cong \widehat{G}$, et μ_n étant lui même un groupe cyclique (engendré par exemple par $e^{\frac{2i\pi}{n}}$), on a bien l'isomorphisme annoncé.

Etape 2. Soient G et H des groupes. Alors on a $\widehat{G \times H} \cong \widehat{G} \times \widehat{H}$. En effet on vérifie que l'application

$$\begin{aligned} \theta : \widehat{G \times H} &\longrightarrow \widehat{G} \times \widehat{H} \\ \phi &\longmapsto (\phi \circ i_1, \phi \circ i_2), \end{aligned}$$

où $i_1 : G \to G \times H$, $g \mapsto (g, 1)$ et $i_2 : H \to G \times H$, $h \mapsto (1, h)$, désignent les injections respectives, est un isomorphisme de groupes.

Etape 3. On peut conclure en utilisant le théorème de structure des groupes finis abéliens : tout groupe abélien fini est isomorphe à un produit de groupes cycliques, donc les étapes 1 et 2 donnent le résultat. □.

Corollaire C.2. Si G est un groupe fini, alors $|\widehat{G}|$ divise $|G|$.

Preuve. On vérifie que les groupes $\widehat{G}$ et $\widehat{G/D(G)}$ sont isomorphes, où $D(G)$ est le groupe dérivé de G. Le groupe $G/D(G)$ est abélien, donc le théorème assure que $|\widehat{G/D(G)}| = |G/D(G)|$, d'où le résultat en utilisant le théorème de Lagrange. □

C.2 Représentations de permutation

Soit X un ensemble fini. On note $\mathbb{C}^X$ le $\mathbb{C}$-espace vectoriel de applications $X \longrightarrow \mathbb{C}$. Pour $x \in X$, on note e_x la fonction indicatrice de l'ensemble $\{x\} : e_x(x) = 1$ et $e_x(y) = 0$ si $y \neq x$. L'ensemble $(e_x)_{x\in X}$ est une base de $\mathbb{C}^X$ (si $\varphi \in \mathbb{C}^X$, on a $\varphi = \sum_{x\in X} \varphi(x)e_x$).

Proposition C.3. Supposons que G opère sur un ensemble fini X. Alors l'application suivante munit $\mathbb{C}^X$ d'une structure de G-espace

$$\begin{aligned} G \times \mathbb{C}^X &\longrightarrow \mathbb{C}^X \\ (g, \varphi) &\longmapsto g.\varphi,\ g.\varphi(x) = \varphi(g^{-1}.x),\ \forall x \in X. \end{aligned}$$

Pour $g \in G$ et $x \in X$, on a $g.e_x = e_{g.x}$.

Preuve. On doit tout d'abord vérifier que l'on a bien une opération. Soit $\varphi \in \mathbb{C}^X$ et $x \in X$. On a $1.\varphi(x) = \varphi(1.x) = \varphi(x)$, d'où $1.\varphi = \varphi$. Soient $g, h \in G$. Alors

$$(gh).\varphi(x) = \varphi((gh)^{-1}.x) = \varphi((h^{-1}g^{-1}).x) = \varphi(h^{-1}.(g^{-1}.x)) = h.\varphi(g^{-1}.x) = g.(h.\varphi)(x)$$

donc $(gh).\varphi = g.(h.\varphi)$ et on a bien une opération. Il reste à voir que cette opération est linéaire. Soient $\varphi, \psi \in \mathbb{C}^X$ et $\lambda \in \mathbb{C}$. On a

$$g.(\varphi + \lambda\psi)(x) = (\varphi + \lambda\psi)(g^{-1}.x) = \varphi(g^{-1}.x) + \lambda\psi(g^{-1}.x) = g.\varphi(x) + \lambda(g.\psi)(x),$$

donc $g.(\varphi + \lambda\psi) = g.\varphi + \lambda g.\psi$ est $\mathbb{C}^X$ est bien un G-espace.

Pour $x, y \in X$ et $g \in G$, on a $g.e_x(y) = e_x(g^{-1}.y) = 1$ si $x = g^{-1}.y$, c'est-à-dire si $y = g.x$, et 0 sinon. Donc $g.e_x = e_{g.x}$. □

On obtient ainsi un procédé général pour construire des représentations linéaires. Par exemple pour l'opération de G sur lui-même par translations, on obtient une représentation linéaire de G sur $\mathbb{C}^G$, appelée **représentation régulière de** G.

C.3 Somme directe de représentations

Les constructions de ce paragraphe sont des cas particuliers de constructions pour les modules (chapitre 1)

Commençons par quelques rappels sur les sommes directes. Soit V un espace vectoriel et soient $V_1, \ldots, V_n$ des sous-espaces de V. On dit que V est somme directe des V_i, et on écrit $V = \bigoplus_{i=1}^n V_i$, si tout élément $v \in V$ s'écrit de manière *unique* sous la forme $v = \sum_{i=1}^n v_i$ où $\forall i,\ v_i \in V_i$.

Si on part maintenant d'une famille $V_1, \ldots, V_n$ d'espaces vectoriels, on peut former le produit $\prod_{i=1}^n V_i$, qui est un espace vectoriel pour les lois produit. On peut alors identifier chaque V_i à un sous-espace de $\prod_{i=1}^n V_i$ via l'application linéaire injective

$$\begin{aligned} V_i &\longrightarrow V_1 \times \ldots \times V_i \times \ldots \times V_n \\ v_i &\longmapsto (0, \ldots, 0, v_i, 0, \ldots, 0) \end{aligned}$$

et sous cette identification, on a $\prod_{i=1}^n V_i = \bigoplus_{i=1}^n V_i$.

Soient $V_1, \dots, V_n$ des représentations de G. On munit alors $\bigoplus_{i=1}^n V_i$ d'une structure de G-espace grâce à l'application

$$\begin{aligned} G \times \bigoplus_{i=1}^n V_i &\longrightarrow \bigoplus_{i=1}^n V_i \\ (g, (v_i)_{1\leq i\leq n}) &\longmapsto (g.v_i)_{1\leq i\leq n} \end{aligned}$$

ce qui au niveau des morphisme de groupes, donne le morphisme

$$\begin{aligned} \pi = \bigoplus_{i=1}^n \pi_{V_i} : G &\longrightarrow \mathrm{GL}(\bigoplus_{i=1}^n V_i) \\ g &\longmapsto \bigoplus_{i=1}^n \pi_{V_i}(g),\ (v_i)_{1\leq i\leq n} \longmapsto (\pi_{V_i}(g)(v_i))_{1\leq i\leq n} \end{aligned}$$

La représentation de G obtenue est **la somme directe des représentations** $V_1, \dots, V_n$.

Si maintenant V est une représentation de G et si $V_1, \dots, V_n$ sont des sous-représentations de G telles $V = \bigoplus_{i=1}^n V_i$ en tant qu'espace vectoriel, alors V s'identifie, en tant que repésentation de G, à la somme directe des représentations que l'on vient de construire.

Le résultat d'algèbre linéaire élémentaire suivant sera utile.

Lemme C.4. Soient $V_1, \dots, V_n, W_1, \dots, W_p$ des représentations de G. Alors on un isomorphisme d'espaces vectoriels

$$\mathrm{Hom}_G(\bigoplus_{i=1}^n V_i, \bigoplus_{j=1}^p W_j) \cong \bigoplus_{i=1}^n \bigoplus_{j=1}^p \mathrm{Hom}_G(V_i, W_j).$$

Preuve. Posons $V = \bigoplus_{i=1}^n V_i$ et $W = \bigoplus_{j=1}^p W_j$. Pour $1 \leq i \leq n$, notons ν_i l'injection $V_i \longrightarrow V$ et $p_i : V \longrightarrow V_i$ la projection sur la i-ème composante. Pour $1 \leq j \leq p$, notons η_j l'injection $W_j \longrightarrow W$ et $q_j : W \longrightarrow W_j$ la projection sur la j-ième composante. Ce sont des morphismes de représentations. On obtient donc des application linéaires

$$\begin{aligned} \mathrm{Hom}_G(\bigoplus_{i=1}^n V_i, \bigoplus_{j=1}^p W_j) &\longrightarrow \bigoplus_{i=1}^n \bigoplus_{j=1}^p \mathrm{Hom}_G(V_i, W_j) \\ f &\longmapsto (q_j \circ f \circ \nu_i)_{1\leq i\leq n, 1\leq j\leq p} \end{aligned}$$

$$\begin{aligned} \bigoplus_{i=1}^n \bigoplus_{j=1}^p \mathrm{Hom}_G(V_i, W_j) &\longrightarrow \mathrm{Hom}_G(\bigoplus_{i=1}^n V_i, \bigoplus_{j=1}^p W_j) \\ (f_{ij})_{1\leq i\leq n, 1\leq j\leq p} &\longmapsto \sum_{i,j} \eta_j \circ f_{ij} \circ p_i \end{aligned}$$

On vérifie que ce sont des isomorphismes réciproques, ce qui provient des identités

$$\sum_{i=1}^n \nu_i \circ p_i = \mathrm{Id}_V,\ \sum_{j=1}^p \eta_j \circ q_j = \mathrm{Id}_W,\ p_i \circ \nu_{i'} = \delta_{ii'}\mathrm{Id}_{V_i},\ q_j \circ \eta_{j'} = \delta_{jj'}\mathrm{Id}_{W_j}. \quad \square$$

C.4 Représentation duale

On commence par une construction un peu plus générale.

Proposition C.5. Soient V et W des représentations de G. Alors l'application

$$\begin{aligned} G \times \mathrm{Hom}(V,W) &\longrightarrow \mathrm{Hom}(V,W) \\ (g,f) &\longmapsto g.f := \pi_W(g) \circ f \circ \pi_V(g^{-1}) \end{aligned}$$

munit $\mathrm{Hom}(V,W)$ d'une structure de G-espace.

Preuve. Vérifions d'abord que l'on a bien une opération. Il est clair que $1.f = f$. Soient $g, h \in G$ et $f \in \mathrm{Hom}(V,W)$. Alors

$$(gh).f = \pi_W(gh) \circ f \circ \pi_V((gh)^{-1}) = \pi_W(g) \circ \pi_W(h) \circ f \circ \pi_V(h^{-1}) \circ \pi_V(g^{-1}) = g.(h.f)$$

Enfin il est immédiat, puisque la composition des applications est bilinéaire, que l'opération est bien linéaire. □

En prenant $W = \mathbb{I}$ la repésentation triviale dans la proposition précédente, on obtient donc une structure de G-espace sur $V^* = \mathrm{Hom}(V, \mathbb{C})$. La représentation obtenue, notée V^* est appelée **représentation duale de** V. Le morphisme de groupe correspondant est

$$\begin{aligned} \pi_{V^*} : G &\longrightarrow \mathrm{GL}(V^*) \\ g &\longmapsto {}^t\pi_V(g^{-1}) \end{aligned}$$

(Rappelons que la transposée d'une application linéaire $f : V \longrightarrow W$ est l'application linéaire ${}^tf : W^* \longrightarrow V^*$ définie par ${}^tf(\phi) = \phi \circ f$)

D Enoncé des théorèmes principaux

On peut déjà énoncer le théorème principal sur les représentations d'un groupe fini.

Théorème D.1 (Le théorème de structure des représentations d'un groupe fini)**.** Soit G un groupe fini.
1. L'ensemble $\mathrm{Irr}(G)$ des classes d'isomorphismes de représentations irréductibles de G est fini et son cardinal s est égal au nombre de classes de conjugaison de G.
Soit $W_1, \ldots, W_s$ un ensemble complet de représentations irréductibles de G (c'est-à-dire que $\mathrm{Irr}(G) = \{[W_1], \ldots, [W_s]\}$). Notons $d_i = \dim(W_i)$ pour $1 \leq i \leq s$.
2. Soit V une représentation de G. Alors on a un isomorphisme de représentations

$$V \cong \bigoplus_{i=1}^{s} W_i^{n_i}$$

où les entiers $n_1, \ldots n_s$ sont donnés par $n_i = \dim(\mathrm{Hom}_G(W_i, V))$.
3. On a $|G| = \sum_{i=1}^{s} d_i^2$.
4. Pour tout $i \in \{1, \ldots, s\}$, on a $d_i || G|$, donc la dimension d'une représentation irréductible de G divise l'ordre de G.
5. Le nombre de représentations irréductibles de dimension 1, égal à $|\widehat{G}| = |\mathrm{Hom}(G, \mathbb{C}^*)|$, divise $|G|$.

Rappelons que les classes de conjugaison de G sont les classes d'équivalence pour la relation d'équivalence sur G définie par $x \backsim y \iff \exists g \in G$ tel que $y = gxg^{-1}$. La classe de conjugaison d'un élément $g \in G$ est donc l'ensemble $C = \{gxg^{-1},\ g \in G\}$, c'est aussi l'orbite de g pour l'opération de G sur lui-même par conjugaison.

Voici quelques illustrations simples de l'utilisation du théorème de structure.

• Si G est un groupe abélien fini, il y a exactement $|G|$-classes de conjugaison, donc $|G|$ classes d'isomorphisme de représentations irréductibles de G. La formule $|G| = \sum_i d_i^2$ assure que ces représentations sont toutes de dimension 1 (ce qui peut se démontrer aussi plus directement en utilisant le lemme de Schur à venir).

Réciproquement si G est un groupe fini dont toutes les représentations irréductibles sont de dimension 1, alors la formule $\sum_{i=1}^{s} d_i^2 = s = |G|$ assure que G à $|G|$ classes de conjugaison, donc que G est abélien.

On a donc le résultat suivant.

Théorème D.2. Soit G un groupe fini. Alors G est abélien si et seulement si toutes ses représentations irréductibles sont de dimension 1.

• Le groupe symétrique S_3. Si d est la dimension d'une représentation irréductible de S_3, on a $d^2 \leq |S_3| = 6$, d'où $d \leq 2$. Comme S_3 est non abélien, il existe donc nécessairement une représentation irréductible de dimension 2. En fait on peut construire cette représentation en remarquant que S_3 est le groupe des isométries d'un triangle. Un coup d'oeil à la formule $\sum_i d_i^2 = 6$ assure alors qu'il y exactement deux autres représentations irréductibles de S_3 non isomorphes, qui sont de dimension 1. Il y a bien sûr la représentation triviale, ainsi que la signature.

En résumé, il y a 3 classes de représentations irréductibles pour S_3 : deux de dimension 1, et une de dimension 2.

On a aussi un critère utile pour montrer qu'une représentation est irréductible.

Théorème D.3. Soit V une représentation d'un goupe fini G. Alors

$$V \text{ est irreductible } \iff \mathrm{End}_G(V) = \mathbb{C}\mathrm{Id}_V$$

Le théorème qui suit fournit un critère commode pour savoir si des représentations sont isomorphes.

Théorème D.4. Soient V et W des représentations d'un groupe fini G. Alors

$$V \text{ et } W \text{ sont isomorphes } \iff \chi_V = \chi_W$$

où χ_V et χ_W sont les caractères respectifs de V et W.

la preuve du sens $\Rightarrow$ est facile : soit $f : V \longrightarrow W$ un isomorphisme de représentations. On a $\pi_W(g) \circ f = f \circ \pi_V(g)$ pour tout $g \in G$, donc $\pi_W(g) = f \circ \pi_V(g) \circ f^{-1}$, et $\chi_W(g) = \mathrm{Tr}(f \circ \pi_V(g) \circ f^{-1}) = \mathrm{Tr}(\pi_V(g)) = \chi_V(g)$, ce qui donne le résultat. Le sens $\Leftarrow$ sera démontré dans le paragraphe sur les caractères.

Le but des paragraphes qui suivent est de démontrer les trois théorèmes enoncés ici, avec aussi des résultats intermédiaires intéressants. Le point 5 du théorème de structure a déjà été démontré.

On travaille désormais avec un groupe fini fixé G.

E Représentations unitaires, complète réductibilité des représentations

Théorème E.1. Soit V une représentation de G. Alors il existe un produit scalaire $\langle , \rangle$ sur V qui est G-invariant :

$$\langle g.v, g.w \rangle = \langle v, w \rangle, \ \forall g \in G, \ \forall v, w \in V.$$

Si on note $H = (V, \langle , \rangle)$ l'espace de Hilbert correspondant, le morphisme de groupes $\pi_V : G \longrightarrow \mathrm{GL}(V)$ est alors à valeurs dans $\mathrm{U}(H)$.

Preuve. Soit $(,)$ un produit scalaire quelconque sur V. On pose alors, pour $v, w \in V$,

$$\langle v, w \rangle = \frac{1}{|G|} \sum_{g \in G} (g.v, g.w).$$

On vérifie sans problème que $\langle , \rangle$ est un produit scalaire sur G. Pour $h \in G$, on a

$$\langle hv, h.w \rangle = \frac{1}{|G|} \sum_{g \in G} (g.(h.v), g.(h.w)) =$$

$$\frac{1}{|G|} \sum_{g \in G} ((gh).v, (gh).w) = \frac{1}{|G|} \sum_{g' \in G} (g'.v, g'.w) = \langle v, w \rangle$$

où on a effectué le changement de variables (bijectif) $g' = gh$. La dernière assertion est alors immédiate. □

On appelle alors **représentation unitaire de** G la donnée d'un morphisme de groupes $\pi : G \longrightarrow \mathrm{U}(H)$ pour un espace de Hilbert H. La proposition précédente affirme donc que toute représentation peut être considérée comme unitaire. C'est un résultat important, dont voici les premières applications.

Théorème E.2. Soit V une représentation de G et soit $W \subset V$ une sous-représentation de G. Alors il existe une sous-représentation $Z \subset V$ de G telle que $V = W \oplus Z$.

Preuve. On considère un produit scalaire invariant $\langle , \rangle$ sur V, et soit $Z = W^{\perp}$. On a $V = W \oplus W^{\perp}$. Montrons que $W^{\perp}$ est une sous-représentation de G. Soit $g \in G$, on a $\pi_V(g)(W) \subset W$, et puisque $\pi_V(g)$ est unitaire, on a $\pi_V(g)(W^{\perp}) \subset W^{\perp}$ (pour $v \in W^{\perp}$, $w \in W$, on a $\langle \pi_V(g)(v), w \rangle = \langle v, \pi_V(g^{-1})(w) \rangle = 0$). □

Théorème E.3. Soit V une représentation de G. Alors il existe $t \in \mathbb{N}$ et des représentations irréductibles $V_1, \ldots, V_t$ de G telles que $V \cong V_1 \oplus \ldots \oplus V_t$.

Preuve. On procède par récurrence sur la dimension de V. Si $\dim V = 0$ on prend $t = 0$ et si $\dim V = 1$ la représentation est irréductible. Supposons donc le résultat montré pour les représentations de dimension $\leq n$ (avec $n \geq 1$) et soit V une représentation de dimesnion $n + 1$. Si V est irréductible, on a le résultat. Sinon, soit $W \subset V$ une sous-représentation telle que $\{0\} \subsetneq W \subsetneq V$, avec donc $1 \leq \dim W \leq n$. On considère alors une sous-représentation Z de V telle que $V = W \oplus Z$, avec $1 \leq \dim Z \leq n$. On applique l'hypothèse de récurrence à W et Z et on a le résultat. □

F Le lemme de Schur

Proposition F.1. Soient V et W des représentations de G et soit $f \in \mathrm{Hom}_G(V,W)$. Alors $\mathrm{Ker} f$ est une sous-représentation de V et $\mathrm{Im}\, f$ est une sous-représentation de W.

La preuve est laissée en exercice.

Théorème F.2 (Lemme de Schur)**.** Soient V_1 et V_2 des représentations irréductibles de G.
(i) Si V_1 et V_2 ne sont pas isomorphes, alors $\mathrm{Hom}_G(V_1,V_2) = \{0\}$.
(ii) Si $V_1 = V_2$, alors $\mathrm{Hom}_G(V_1,V_1) = \mathbb{C}\mathrm{Id}_{V_1}$.

Preuve. Soit $f \in \mathrm{Hom}_G(V_1,V_2)$. D'après la proposition précédente $\mathrm{Ker}\, f$ est une sous-repésentation de V_1 et $\mathrm{Im}\, f$ est une sous-représentation de V_2. Comme V_1 et V_2 sont irréductibles, on a $\mathrm{Ker}\, f = \{0\}$ ou $\mathrm{Ker}\, f = V_1$, et $\mathrm{Im}\, f = \{0\}$ ou $\mathrm{Im}\, f = V_2$. Si $f \neq 0$, alors donc $\mathrm{Ker}\, f = \{0\}$ et $\mathrm{Im}\, f = V_2$, donc f est un isomorphisme. Ainsi si V_1 et V_2 ne sont pas isomorphes, on a bien $f = 0$ et $\mathrm{Hom}_G(V_1,V_2) = \{0\}$.

Supposons maintenant que $V_1 = V_2 = V$ et soit $f \in \mathrm{Hom}_G(V,V)$. Soit $\lambda \in \mathbb{C}$ une valeur propre de f. Alors $f - \lambda\mathrm{Id}_V \in \mathrm{Hom}_G(V,V)$ avec $\mathrm{Ker}(f - \lambda \mathrm{id}_V) \neq \{0\}$. Comme V est irréductible, on a $\mathrm{Ker}(f - \lambda\mathrm{Id}_V) = V$, d'où $f = \lambda\mathrm{Id}_V$, et on a le résultat. □

On démontre maintenant sans difficulté le critère d'irréductibilité déjà annoncé.

Théorème F.3. Soit V une représentation de G. Alors

$$V \text{ est irreductible } \iff \mathrm{End}_G(V) = \mathbb{C}\mathrm{Id}_V$$

Preuve. Le sens $\Rightarrow$ est donné par la partie ii du lemme de Schur. Réciproquement, si V n'est pas irréductible, on a $V = U \oplus W$ pour des sous-représentations non nulles U et W. On a alors

$$\begin{aligned}\mathrm{End}_G(V,V) &= \mathrm{Hom}_G(U \oplus W, U \oplus W)\\ &\cong \mathrm{Hom}_G(U,U) \oplus \mathrm{Hom}_G(U,W) \oplus \mathrm{Hom}_G(W,U) \oplus \mathrm{Hom}_G(W,W)\end{aligned}$$

et donc $\dim(\mathrm{End}_G(V)) \geq 2$, ce qui donne le résultat. □

G Invariants et moyenne

Définition-Proposition G.1. Soit V une représentation de G. On considère

$$V^G = \{v \in V \mid g.v = v, \forall g \in G\}.$$

Alors V^G est un sous-espace de V, appellé espace des G-invariants de V.

On vérifie sans difficulté que V^G est bien un sous-espace de V (c'est même une sous-représentation). La proposition qui suit permet de construire tous les G-invariants.

Définition-Proposition G.2. Soit V une repésentation de G. On considère l'application

$$\begin{aligned} M : V &\longrightarrow V \\ v &\longmapsto \frac{1}{|G|}\sum_{g\in G} g.v \end{aligned}$$

Alors M est application linéaire, appelée **l'opérateur de moyenne de** V. L'opérateur M est un projecteur ($M \circ M = M$) d'image égale à V^G.

Preuve. On a $M = \frac{1}{|G|}\sum_{g\in G} \pi_V(g)$, donc M est linéaire. On a

$$\begin{aligned} M \circ M &= \frac{1}{|G|^2}\sum_{g,h\in G} \pi_V(g)\circ\pi_V(h) = \frac{1}{|G|^2}\sum_{g,h\in G}\pi_V(gh) \\ &= \frac{1}{|G|^2}\sum_{g,g'\in G}\pi_V(g') = \frac{1}{|G|}\sum_{g\in G}\frac{1}{|G|}\sum_{g'\in G}\pi_V(g') = M, \end{aligned}$$

donc M est bien un projecteur. Pour $v \in V$ et $h \in G$, on a

$$h.M(v) = \frac{1}{|G|}\sum_{g\in G} h.(g.v) = \frac{1}{|G|}\sum_{g\in G}(hg).v = \frac{1}{|G|}\sum_{g\in G} g.v = M(v)$$

donc $M(v) \in V^G$, et $\operatorname{Im} M \subset V^G$. Réciproquement si $v \in V^G$, on a $M(v) = \frac{1}{|G|}\sum_{g\in G} g.v = \frac{1}{|G|}\sum_{g\in G} v = v$, donc $v \in \operatorname{Im} M$ et $V^G \subset \operatorname{Im} M$. □

On applique alors cela aux applications linéaires entre représentations.

Corollaire G.3. Soient V et W des représentations de G et soit $f : V \longrightarrow W$ une application linéaire. Alors l'application linéaire $M(f) : V \longrightarrow W$ définie par

$$M(f) = \frac{1}{|G|}\sum_{g\in G}\pi_W(g)\circ f\circ\pi_V(g^{-1})$$

appartient à $\operatorname{Hom}_G(V, W)$. De plus si $V = W$, on a $\operatorname{Tr}(M(f)) = \operatorname{Tr}(f)$.

Preuve. On considère la représentation de G sur $\operatorname{Hom}(V, W)$, donnée par $g.f = \pi_W(g)\circ f\circ\pi_V(g^{-1})$ pour $g \in G$. Alors il est immédiat que $f \in \operatorname{Hom}(V, W)^G \iff f \in \operatorname{Hom}_G(V, W)$, donc puisque le $M(f)$ décrit plus haut est l'opérateur de moyenne de la représentation $\operatorname{Hom}(V, W)$ appliqué à f, on a bien $M(f) \in \operatorname{Hom}_G(V, W) = \operatorname{Hom}(V, W)^G$.

Si $V = W$, alors

$$\operatorname{Tr}(M(f)) = \frac{1}{|G|}(\sum_{g\in G}\operatorname{Tr}(\pi_W(g)\circ f\circ\pi_V(g^{-1})) = \frac{1}{|G|}\sum_{g\in G}\operatorname{Tr}(f) = \operatorname{Tr}(f). \qquad \square$$

H Relations d'orthogonalité et applications

On note $L^2(G)$ l'espace vectoriel $\mathbb{C}^G$ des fonctions de G dans $\mathbb{C}$ muni du produit scalaire

$$\langle \phi, \psi\rangle_G = \frac{1}{|G|}\sum_{g\in G}\phi(g)\overline{\psi(g)}.$$

Les relations d'orthogonalité expriment l'orthogonalité, dans $L^2(G)$, de certaines fonctions associées à des représentations irréductibles. Elles auront en particulier comme conséquence le fait que l'ensemble $\mathrm{Irr}(G)$ des classes d'isomorphismes de représentations irréductibles de G est fini.

Introduisons quelques notations.
1. Soient V et W des espaces vectoriels et $f \in V^*$, $x \in W$. On note $x \otimes f$ l'application linéaire $V \to W$ définie par $(x \otimes f)(v) = f(v)x$.
2. Soit V une représentation de G et notons $\pi : G \longrightarrow \mathrm{GL}(V)$ le morphisme de groupes correspondant. Soit $v_1, \ldots, v_n$ une base de V, et notons π_{ij}, $1 \leq i, j \leq n = \dim V$, les fonctions coordonnées sur G associées à l'identification $\mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbb{C})$ donnée par la base, de telle sorte que

$$\forall g \in G, \quad \pi(g) = \sum_{i,j=1}^{n} \pi_{ij}(g) v_i \otimes v_j^*.$$

Théorème H.1 (Relations d'orthogonalité, première version)**.** Soient V et W des représentations irréductibles de G avec $n = \dim V$ et $m = \dim W$. Notons $\pi : G \longrightarrow \mathrm{GL}(V)$ et $\rho : G \longrightarrow \mathrm{GL}(W)$ les morphismes de groupes correspondant, et $(\pi_{ij})_{1 \leq i,j \leq n}$ et $(\rho_{kl})_{1 \leq k,l \leq m}$, les fonctions coordonnées sur G associées au choix de bases de V et W.
(i) Si V et W ne sont pas isomorphes, alors on a

$$\frac{1}{|G|} \sum_{g \in G} \rho_{kl}(g) \pi_{ij}(g^{-1}) = 0, \quad 1 \leq i, j \leq n,\ 1 \leq k, l \leq n$$

(ii) Si $V = W$ ($\pi = \rho$), alors on a

$$\frac{1}{|G|} \sum_{g \in G} \pi_{kl}(g) \pi_{ij}(g^{-1}) = \frac{\delta_{kj}\delta_{il}}{n}, \quad 1 \leq i, j, k, l \leq n.$$

Preuve. On va obtenir le résultat en faisant la moyenne de certains opérateurs de rang 1 et en appliquant le lemme de Schur. Soient donc $v_1, \ldots, v_n$ et $w_1, \ldots w_m$ des bases respectives de V et W, et soient (π_{ij}) et (ρ_{ij}) les fonctions coordonnées sur G associées. Soient $i_0 \in \{1, \ldots, n\}$ et $k_0 \in \{1, \ldots, m\}$. Alors

$$\begin{aligned}
M(w_{k_0} \otimes v_{i_0}^*) &= \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ (w_{k_0} \otimes v_{i_0}^*) \circ \pi(g^{-1}) \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{i,j=1}^{n} \sum_{k,l=1}^{m} \rho_{kl}(g) \pi_{ij}(g^{-1}) (w_k \otimes w_l^*) \circ (w_{k_0} \otimes v_{i_0}^*) \circ (v_i \otimes v_j^*) \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{j=1}^{n} \sum_{k=1}^{m} \rho_{kk_0}(g) \pi_{i_0 j}(g^{-1}) (w_k \otimes v_j^*) \\
&= \sum_{j=1}^{n} \sum_{k=1}^{m} \left(\frac{1}{|G|} \sum_{g \in G} \rho_{kk_0}(g) \pi_{i_0 j}(g^{-1}) \right) (w_k \otimes v_j^*) \in \mathrm{Hom}_G(V, W).
\end{aligned}$$

(i) Supposons V et W non isomorphes. Alors d'après le lemme de Schur $\mathrm{Hom}_G(V, W) = \{0\}$, donc l'opérateur précédent est nul, et puisque $(w_k \otimes v_j^*)$ est une base de $\mathrm{Hom}(V, W)$, chaque coefficient est nul, et on a les relations recherchées.

(ii) Supposons maintenant que $V = W$. Toujours par le lemme de Schur, on obtient $M(v_{k_0} \otimes v_{i_0}^*) = \lambda \mathrm{id}_V$, pour

$$\lambda = \frac{\mathrm{Tr}(M(v_{k_0} \otimes v_{i_0}^*))}{n} = \frac{\mathrm{Tr}(v_{k_0} \otimes v_{i_0}^*)}{n} = \frac{\delta_{i_0 k_0}}{n}.$$

On a $\mathrm{Id}_V = \sum_i v_j \otimes v_j^*$, donc en identifiant on trouve bien

$$\frac{1}{|G|}\sum_{g\in G}\pi_{kk_0}(g)\pi_{i_0j}(g^{-1}) = \delta_{kj}\lambda = \frac{\delta_{kj}\delta_{i_0k_0}}{n}. \qquad \square$$

On obtient maintenant les relations d'orthogonalité dans $L^2(G)$.

Théorème H.2 (Relations d'orthogonalité dans $L^2(G)$)**.** Pour chaque $\alpha \in \mathrm{Irr}(G)$, fixons V_α une représentation de G telle que $\alpha = [V_\alpha]$, avec $\pi^\alpha : G \longrightarrow \mathrm{GL}(V_\alpha)$ le morphisme de groupe correspondant. Notons $d_\alpha = \dim V_\alpha$. Fixons sur V_α un produit scalaire G-invariant et une base orthonormée pour ce produit scalaire, et notons (π^α_{ij}) les fonctions coordonnées sur G associées. Alors on a

$$\langle \pi^\alpha_{ij}, \pi^\beta_{kl}\rangle_G = \frac{\delta_{\alpha\beta}\delta_{ik}\delta_{jl}}{d_\alpha}, \quad \forall \alpha,\beta \in \mathrm{Irr}(G),\ 1\le i,j\le d_\alpha,\ 1\le k,l\le d_\beta.$$

Preuve. Pour $\alpha \in \mathrm{Irr}(G)$, on a choisi un produit scalaire invariant sur V_α, donc si on note H_α l'espace de Hilbert associé, on a $\pi^\alpha(G) \subset U(H_\alpha)$, et donc $\pi^\alpha(g^{-1}) = \pi^\alpha(g)^{-1} = \pi^\alpha(g)^*$, $\forall g \in G$. Au niveau des fonctions coordonnées, cela donne $\pi^\alpha_{ij}(g^{-1}) = \overline{\pi^\alpha_{ji}(g)}$, pour $1 \le i,j \le d_\alpha$. On a alors

$$\langle \pi^\alpha_{ij}, \pi^\beta_{kl}\rangle_G = \frac{1}{|G|}\sum_{g\in G}\pi^\alpha_{ij}(g)\overline{\pi^\beta_{kl}(g)} = \frac{1}{|G|}\sum_{g\in G}\pi^\alpha_{ij}(g)\pi^\beta_{lk}(g^{-1}) = \frac{\delta_{\alpha\beta}\delta_{ik}\delta_{jl}}{d_\alpha}$$

où l'on a utilisé la première version des relations d'orthogonalité. $\square$

Corollaire H.3. L'ensemble $\mathrm{Irr}(G)$ des classes de représentations irréductibles de G est fini. On notera $s = |\mathrm{Irr}(G)|$. Si $W_1,\dots,W_s$ sont des représentations de G telles que $\mathrm{Irr}(G) = \{[W_1],\dots,[W_s]\}$, alors on a $\sum_{i=1}^s d_i^2 \le |G|$, où $d_i = \dim W_i$, $\forall i$.

Preuve. En reprenant les notations des relations d'orthogonalité, on voit que $\{\pi^\alpha_{ij},\ \alpha \in \mathrm{Irr}(G), 1 \le i,j \le d_\alpha\}$ est une famille d'éléments non nuls de $L^2(G)$ qui sont deux à deux orthogonaux. C'est donc une famille libre de $L^2(G)$, qui est de dimension finie égale à $|G|$. On obtient donc à la fois que $\mathrm{Irr}(G)$ est fini et l'inégalité du corollaire. $\square$

On veut en fait démontrer que l'inégalité précédente est une égalité. Pour cela il faut démontrer que $\{\pi^\alpha_{ij},\ \alpha \in \mathrm{Irr}(G), 1 \le i,j \le d_\alpha\}$ est une base de $L^2(G)$ (on utilise toujours les notations des relations d'orthogonalité). Pour cela on introduit une transformation $\mathcal{F}$ sur les fonctions de $L^2(G)$, qui est un peu un analogue de la transformée de Fourier sur $L^2(\mathbb{S}^1)$.

Lemme H.4. Soit $\phi \in \mathbb{C}^G$. Soit V une représentation de G. On considère l'application linéaire définie par

$$\mathcal{F}_V(\phi) = \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_V(g) \in \mathrm{End}(V).$$

1. Si $v_1, \ldots, v_n$ est une base de V et si (π_{ij}) sont les fonctions coordonnées sur G correspondantes, on a

$$\mathcal{F}_V(\phi) = \sum_{i,j=1}^{n} \langle \pi_{ij}, \phi \rangle_G v_i \otimes v_j^*.$$

2. Si V et W sont des représentations de G, on a $\mathcal{F}_{V \oplus W}(\phi) = \mathcal{F}_V(\phi) \oplus \mathcal{F}_W(\phi)$
3. Soient V et W des représentations de G et soit $f : V \to W$ un G-isomorphisme. Alors on a $\mathcal{F}_W(\phi) = f \circ \mathcal{F}_V(\phi) \circ f^{-1}$.

Preuve. 1. On a

$$\begin{aligned}\mathcal{F}_V(\phi) &= \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_V(g) = \frac{1}{|G|} \sum_{g \in G} \sum_{i,j=1}^{n} \overline{\phi(g)} \pi_{ij}(g) v_i \otimes v_j^* \\ &= \sum_{i,j=1}^{n} \left(\frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_{ij}(g) \right) v_i \otimes v_j^* = \sum_{i,j=1}^{n} \langle \pi_{ij}, \phi \rangle_G v_i \otimes v_j^*\end{aligned}$$

2. On a

$$\begin{aligned}\mathcal{F}_{V \oplus W}(\phi) &= \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_{V \oplus W}(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} (\pi_V(g), \pi_W(g)) \\ &= \left(\frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_V(g), \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_W(g) \right) = \mathcal{F}_V(\phi) \oplus \mathcal{F}_W(\phi).\end{aligned}$$

3. Pour tout $g \in G$, on a $\pi_W(g) \circ f = f \circ \pi_V(g)$, c'est-à-dire $\pi_W(g) = f \circ \pi_W(g) \circ f^{-1}$, d'où le résultat. □

Théorème H.5 (Théorème de Peter-Weyl pour les groupes finis)**.** On reprend les notations utilisées pour l'énoncé des relations d'orthogonalité. Alors

$$\left\{ \sqrt{d_\alpha} \pi_{ij}^\alpha,\ \alpha \in \mathrm{Irr}(G),\ 1 \leq i, j \leq d_\alpha \right\}$$

est une base orthonormée de $L^2(G)$. En particulier

$$\sum_{\alpha \in \mathrm{Irr}(G)} d_\alpha^2 = |G|.$$

Preuve. On sait déjà des relations d'orthogonalité que le système donné est orthonormé, et il faut donc voir que l'on a une base de $L^2(G)$. Soit W le sous-espace de $L^2(G)$ engendré par notre système. Pour voir que $W = L^2(G)$, il suffit de voir que $W^\perp = \{0\}$. Soit donc $\phi \in W^\perp$. En utilisant le 1 du lemme précédent on voit que $\forall \alpha \in \mathrm{Irr}(G)$, on a

$$\mathcal{F}_{V_\alpha}(\phi) = \sum_{i,j=1}^{d_\alpha} \langle \pi_{ij}, \phi \rangle_G v_i \otimes v_j^* = 0.$$

Donc si V est une représentation irréductible quelconque de G, on a $\mathcal{F}_V(\phi) = 0$ d'après la partie 3 du lemme. Si maintenant V est une représentation quelconque de G, elle est somme directe de représentations irréductibles, et on a $\mathcal{F}_V(\phi) = 0$ d'après la partie 2 du lemme.

On applique maintenant ceci à la représentation régulière $R = \mathbb{C}^G$ obtenue en utilisant l'opération de G sur lui-même par translations. Pour $g, x \in G$, on a $\pi_R(g)(e_x) = e_{gx}$. Donc

$$\mathcal{F}_R(\phi)(e_1) = \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} \pi_R(g)(e_1) = \frac{1}{|G|} \sum_{g \in G} \overline{\phi(g)} e_g = 0$$

et puisque $(e_g)_{g \in G}$ est une base de $\mathbb{C}^G$, on conclut que $\phi = 0$. Donc $W^\perp = \{0\}$ et $L^2(G) = W$. La dimension de $L^2(G)$ est $|G|$, et doit être égale au cardinal d'une base quelconque. □

Corollaire H.6. Soient $W_1, \ldots, W_s$ sont des représentations irréductibles de G telles que $\mathrm{Irr}(G) = \{[W_1], \ldots, [W_s]\}$, où $s = |\mathrm{Irr}(G)|$. Alors on a

$$\sum_{i=1}^{s} d_i^2 = |G|, \text{ avec } d_i = \dim W_i, \ \forall i.$$

Preuve. Chaque W_i est isomorphe à exactement un V_α, donc on applique simplement le résultat précédent. □

I Structure de l'algèbre du groupe

L'objectif est maintenant de montrer que $s = |\mathrm{Irr}(G)|$ est égal au nombre de classes de conjugaison de G. On démontrera au passage le premier théorème de l'introduction.

Soit (V, π_V) une représentation de G. On sait qu'il existe un unique morphisme d'algèbres

$$\widetilde{\pi_V} : \mathbb{C}[G] \longrightarrow \mathrm{End}(V)$$

tel que $\widetilde{\pi_V}(e_g) = \pi_V(g), \forall g \in G$.

En fait pour $\phi \in \mathbb{C}[G]$, on a $\widetilde{\pi_V}(\phi) = |G| \mathcal{F}_V(\overline{\phi})$, où $\mathcal{F}_V$ a été introduit dans le paragraphe précédent. Cela nous permet de montrer facilement le résultat suivant.

Théorème I.1. Soient $W_1, \ldots, W_s$ sont des représentations irréductibles de G telles que $\mathrm{Irr}(G) = \{[W_1], \ldots, [W_s]\}$, où $s = |\mathrm{Irr}(G)|$. Alors on a un isomorphisme d'algèbres

$$\begin{aligned} \Omega : \mathbb{C}[G] &\longrightarrow \prod_{i=1}^{s} \mathrm{End}(W_i) \\ \phi &\longmapsto (\widetilde{\pi_{W_i}}(\phi))_{1 \leq i \leq r} \end{aligned}$$

Preuve. Chaque $\widetilde{\pi_{W_i}}$ est un morphisme d'algèbres, donc il est facile de voir que Ω est bien un morphisme d'algèbres. On a $\dim(\mathbb{C}[G]) = |G| = \sum_{i=1}^{s} (\dim W_i)^2 = \dim(\prod_{i=1}^{s} \mathrm{End}(W_i))$, donc il suffit donc de voir que Ω est injectif. Soit alors $\phi \in \mathrm{Ker}\,\Omega$: on a $\widetilde{\pi_{W_i}}(\phi) = 0 = \mathcal{F}_{W_i}(\overline{\phi}), \forall i$. On peut raisonner de la même façon que dans la preuve du théorème de Peter-Weyl : on a $\mathcal{F}_V(\overline{\phi}) = 0$ pour toute représentation V et on applique cela à la représentation régulière pour trouver que $\overline{\phi} = 0 = \phi$. □

On va maintenant utiliser ce théorème pour déterminer s. Si A est une algèbre, on considère son centre $Z(A) = \{a \in A \mid ab = ba, \forall b \in A\}$. C'est une sous-algèbre de A, et

donc aussi une algèbre. Si A et B sont des algèbres, alors une vérification immédiate donne $Z(A \times B) = Z(A) \times Z(B)$. Donc en reprenant les notations précédentes, on a

$$Z(\prod_{i=1}^{s} \mathrm{End}(W_i)) = \prod_{i=1}^{s} Z(\mathrm{End}(W_i)) \cong \mathbb{C}^s$$

puisque le centre d'une algèbre de matrices est réduit à $\mathbb{C}$, et donc

$$\dim(Z(\prod_{i=1}^{s} \mathrm{End}(W_i)) = s.$$

Théorème I.2. Le nombre $s = |\mathrm{Irr}(G)|$ de classes d'isomorphisme de représentations irréductibles de G est égal au nombre de classes de conjugaison de G.

Preuve. L'isomorphisme d'algèbres $\mathbb{C}[G] \cong \prod_{i=1}^{s} \mathrm{End}(W_i)$ induit un isomorphisme entre les centres, qui ont donc même dimension, égale à s. On a vu au chapitre 3 que $\dim(Z(\mathbb{C}[G]))$ est égal au nombre de classe de conjugaison de G, d'où le résultat. □

Fin de la démonstration des points 1, 2 et 3 du théorème de structure des représentations d'un groupe fini.

On vient de finir la preuve de la partie 1, et la partie 3 a été démontrée au paragraphe précédent. Passons au point 2. Soit V une représentation de G et soient $W_1, \ldots, W_s$ des représentations irréductibles telles que $\mathrm{Irr}(G) = \{[W_1], \ldots, [W_s]\}$. Alors V est somme directe de représentations irréductibles, chacune isomorphe à l'un des W_i, donc on a un isomorphisme de représentations

$$V \cong \bigoplus_{i=1}^{s} W_i^{n_i}$$

pour des entiers $n_1, \ldots, n_s \in \mathrm{N}$. Pour $j \in \{1, \ldots, s\}$, on a, en utilisant le lemme de Schur,

$$\begin{aligned} \mathrm{Hom}_G(W_j, V) &\cong \mathrm{Hom}_G(W_j, \bigoplus_{i=1}^{s} W_i^{n_i}) \cong \bigoplus_{i=1}^{s} \mathrm{Hom}_G(W_j, W_i)^{n_i} \\ &= \mathrm{Hom}_G(W_j, W_j)^{n_j} \cong \mathbb{C}^{n_j} \end{aligned}$$

donc $n_j = \dim(\mathrm{Hom}_G(W_j, V))$. Cela termine la démonstration du point 2.

J Caractères

Rappelons la définition du caractère d'une représentation.

Définition J.1. *Soit (V, π_V) une représentation de G. Le **caractère de** V est la fonction $\chi_V : G \longrightarrow \mathcal{C}$ définie par*

$$\chi_V(g) = \mathrm{Tr}(\pi_V(g)), \quad \forall g \in G.$$

*On dit qu'une fonction $\chi : G \longrightarrow \mathbb{C}$ est un **caractère** si χ est le caractère d'une représentation de G.*

Voici les premières propriétés des caractères.

Proposition J.2. Soient V et W des représentations de G.
1. $\chi_V(1) = \dim V$.
2. Si les représentations V et W sont isomorphes, alors $\chi_V = \chi_W$.
3. On a $\forall g, h \in G$, $\chi_V(gh) = \chi_V(hg)$, et ainsi χ_V est une fonction centrale sur G.
4. On a $\chi_{V\oplus W} = \chi_V + \chi_W$.

Preuve. On a $\chi_V(1) = \mathrm{Tr}(\pi_V(1)) = \mathrm{Tr}(\mathrm{id}_V) = \dim V$. La deuxième assertion a déjà été montrée. Pour $g, h \in G$ on a $\chi_V(gh) = \mathrm{Tr}(\pi_V(gh)) = \mathrm{Tr}(\pi_V(g) \circ \pi_V(h)) = \mathrm{Tr}(\pi_V(h) \circ \pi_V(g)) = \mathrm{Tr}(\pi_V(hg)) = \chi_V(hg)$. La dernière assertion se montre sans difficulté à partir de l'écriture matricielle de $\pi_{V\oplus W}$. □

Théorème J.3 (Relations d'orthogonalité des caractères)**.** Soient V et W des représentations irréductibles de G. Alors dans $L^2(G)$ on a

$$\langle \chi_V, \chi_W \rangle_G = \begin{cases} 0 & \text{si } V \text{ et } W \text{ ne sont pas isomorphes,} \\ 1 & \text{si } V \text{ et } W \text{ sont isomorphes.} \end{cases}$$

Preuve. Notons $\pi : G \longrightarrow \mathrm{GL}(V)$ et $\rho : G \longrightarrow \mathrm{GL}(W)$ les morphismes de groupes correspondant. On fixe sur V et W des produit scalaires G-invariants et soient $v_1, \ldots, v_n$ et $w_1, \ldots, w_m$ des bases orthonormées respectives de V et W pour ces produits scalaires. On note (π_{ij}) et (ρ_{kl}) les fonctions coordonnées associées sur G. On a

$$\chi_V = \sum_{i=1}^{n} \pi_{ii} \quad \text{et} \quad \chi_W = \sum_{k=1}^{m} \rho_{kk}$$

et donc

$$\langle \chi_V, \chi_W \rangle_G = \sum_{i,k} \langle \pi_{ii}, \rho_{kk} \rangle_G.$$

Les relations d'orthogonalité dans $L^2(G)$ assurent alors que $\langle \chi_V, \chi_W \rangle_G = 0$ si $V \ncong W$. Si $V \cong W$ on a $\chi_V = \chi_W$ par le 2 de la proposition précédente, on peut donc supposer que $V = W$, et alors, toujours grâce aux relations d'orthogonalité dans $L^2(G)$, on a

$$\langle \chi_V, \chi_V \rangle_G = \sum_{i=1}^{n} \langle \pi_{ii}, \pi_{ii} \rangle_G = \frac{\dim V}{\dim V} = 1. \quad \square$$

Corollaire J.4. Soient V et W des représentations de G avec V irréductible. Alors

$$\langle \chi_V, \chi_W \rangle_G = \dim(\mathrm{Hom}_G(V, W)).$$

Preuve. Soient $W_1, \ldots, W_s$ des représentations irréductibles de G telles que $\mathrm{Irr}(G) = \{[W_1], \ldots, [W_s]\}$, où $s = |\mathrm{Irr}(G)|$. Alors

$$W \cong \bigoplus_{i=1}^{s} W_i^{n_i}$$

pour $n_i = \dim(\mathrm{Hom}_G(W_i, W))$. On a alors, en utilisant la première proposition, $\chi_W = \sum_{i=1}^{s} n_i \chi_{W_i}$. Soit i_0 tel que $V \cong W_{i_0} : \chi_V = \chi_{W_{i_0}}$. On a donc, en utilisant les relations d'orthogonalité des caractères,

$$\langle \chi_V, \chi_W \rangle_G = \sum_{i=1}^{n} n_i \langle \chi_{W_{i_0}}, \chi_{W_i} \rangle = n_{i_0} = \dim(\mathrm{Hom}_G(W_{i_0}, W)) = \dim(\mathrm{Hom}_G(V, W)). \quad \square$$

On arrive alors au résultat important suivant.

Théorème J.5. Soient V et W des représentations d'un groupe fini G. Alors

$$V \text{ et } W \text{ sont isomorphes } \iff \chi_V = \chi_W.$$

Preuve. Soit $W_1, \dots, W_s$ un système complet de représentations irréductibles de G. Alors

$$V \cong \bigoplus_{i=1}^{s} W_i^{n_i} \quad \text{et} \quad V \cong \bigoplus_{i=1}^{s} W_i^{m_i}$$

pour $n_i = \dim(\mathrm{Hom}_G(W_i, V))$ et $m_i = \dim(\mathrm{Hom}_G(W_i, W))$. Donc si $\chi_V = \chi_W$, on a pour tout i

$$n_i = \dim(\mathrm{Hom}_G(W_i, V)) = \langle \chi_{W_i}, \chi_V \rangle = \langle \chi_{W_i}, \chi_W \rangle = \dim(\mathrm{Hom}_G(W_i, W)) = m_i.$$

Il est clair alors que V et W sont isomorphes. □

Proposition J.6. Soit χ un caractère sur G. Alors $\forall g \in G$, $\chi(g) \in \mathbb{C}$ est un entier algébrique.

Preuve. Soit V une représentation de G telle que $\chi = \chi_V$. Pour $g \in G$, on a $g^{|G|} = 1$ donc $\pi_V(g)^{|G|} = \mathrm{id}_V$, donc les valeurs propres de $\pi_V(g)$ sont des racines de l'unités, donc des entiers algébriques. Alors $\chi(g)$ qui est la trace de $\pi_V(g)$, est la somme des valeurs propres de $\pi_V(g)$, est un entier algébrique (voitr chapitre IV). □

Proposition J.7. Soit χ le caractère d'une représentation irréductible de dimension d de G. Soit C une classe de conjugaison de G. Alors pour tout $g \in C$, $\frac{|C|\chi(g)}{d}$ est un entier algébrique.

Preuve. $\mathbb{Z}[G]$ est un sous-anneau de $\mathbb{C}[G]$. Considérons $Z(\mathbb{Z}[G])$, le centre de $\mathbb{Z}[G]$. De la même façon que pour $\mathbb{C}[G]$, on montre que les éléments de $Z(\mathbb{Z}[G])$ sont exactement les combinaison linéaires à coefficients entiers des (x_C), où C parcourt l'ensemble des classes de conjugaison de G. On en déduit que $Z(\mathbb{Z}[G])$ est un groupe abélien de type fini, donc ses éléments, et en particulier x_C pour chaque classe de conjugaison C, sont des entiers algébriques.

Soit (V, π_V) une représentation irréductible telle que $\chi = \chi_V$ et soit $\widetilde{\pi_V} : \mathbb{C}[G] \longrightarrow \mathrm{End}(V)$ le morphisme d'algèbre qui prolonge π_V. Soit C une classe de conjugaison de G. L'élément x_C appartient au centre de $\mathbb{C}[G]$, donc $\widetilde{\pi_V}(x_C)$ commute avec tous les $\pi_V(g)$, ce qui signifie que $\widetilde{\pi_V}(x_C) \in \mathrm{End}_G(V)$. Par le lemme de Schur $\widetilde{\pi_V}(x_C) = \lambda \mathrm{id}_V$ pour un $\lambda \in \mathbb{C}$. Puisqu'il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(x_C) = 0$, on a $\widetilde{\pi_V}(P(x_C)) = 0 = P(\widetilde{\pi_V}(x_C)) = P(\lambda)\mathrm{Id}_V$, donc λ est entier algébrique. On obtient

$$\mathrm{Tr}(\widetilde{\pi_V}(x_C)) = \mathrm{Tr}(\sum_{g \in C} \pi_V(g)) = \sum_{g \in C} \chi_V(g) = |C|\chi(g) = d\lambda$$

et donc $\frac{|C|\chi(g)}{d} = \lambda$ est entier algébrique. □

On arrive au résultat suivant, qui termine la démonstration du théorème de structure des représentations.

Théorème J.8. La dimension d'une représentation irréductible de G divise $|G|$.

Preuve. Soit V une représentation irréductible de dimension d de G, de caractère χ. Notons $C_1, \ldots, C_s$ les classes de conjugaison distinctes de G. Pour $g \in C_i$, on notera $\chi(C_i)$ la valeur de $\chi(g)$. On sait que $\langle \chi, \chi \rangle_G = 1$, ce qui, explicité, donne

$$1 = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi(g)} = \frac{1}{|G|} \sum_{i=1}^{r} \sum_{g \in C_i} \chi(g)\overline{\chi(g)} = \frac{1}{|G|} \sum_{i=1}^{r} |C_i| \chi(C_i)\overline{\chi(C_i)}$$

ou encore

$$\frac{|G|}{\dim V} = \sum_{i=1}^{r} \frac{|C_i|\chi(C_i)}{\dim V} \overline{\chi(C_i)}$$

avec par pour tout i, les deux propositions précédentes, $\frac{|C_i|\chi(C_i)}{\dim V}$ et $\overline{\chi(C_i)}$ des entiers algébriques. Une somme d'entiers algébrique est encore un entier algébrique, donc $\frac{|G|}{\dim V}$ est entier algébrique et puisque $\frac{|G|}{\dim V} \in \mathbb{Q}$, on a bien $\frac{|G|}{\dim V} \in \mathbb{Z}$. □

On termine ce paragraphe par en introduisant la table des caractères du groupe G. Soient $C_1, \ldots, C_s$ les classes de conjugaison de G avec la convention $C_1 = \{1\}$. Soient $W_1, \ldots, W_s$ des représentations irréductibles de G telles que $\mathrm{Irr}(G) = \{[W_1], \ldots, [W_s]\}$, avec la convention que W_1 est la représentation triviale. Notons pour tout i, $\chi_i = \chi_{W_i}$. **La table des caractère de** G est alors le tableau suivant :

	$C_1 = \{1\}$	C_2	$\cdots$	C_i	$\cdots$	C_s
χ_1	1	1	$\cdots$	1	$\cdots$	1
χ_2	$d_2 = \chi_2(1)$	$\chi_2(C_2)$	$\cdots$	$\chi_2(C_i)$	$\cdots$	$\chi_2(C_s)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
χ_j	$d_j = \chi_j(1)$	$\chi_j(C_2)$	$\cdots$	$\chi_j(C_i)$	$\cdots$	$\chi_j(C_s)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
χ_s	$d_s = \chi_s(1)$	$\chi_s(C_2)$	$\cdots$	$\chi_s(C_i)$	$\cdots$	$\chi_s(C_s)$

L'usage quand on écrit la table des caractères est de remplacer les classes C_i par un représentant.

On considère que l'on a décrit de façon satisfaisante les représentations de G lorsque l'on a calculé sa table des caractères (qui bien sûr dépend de l'ordre choisi sur l'ensembles des classes de conjugaison et sur l'ensemble des classes d'isomorphismes de représentaions irréductibles).

Exemple. La table des caractères du groupe symétrique S_3 est

	1	$(1,2)$	$(1,2,3)$
χ_1	1	1	1
ε	1	-1	1
χ_2	2	0	-1

où χ_1 est la représentation triviale, ε est la signature, et χ_2 est le caractère de la représentation irréductible de degré 2.

Pour trouver les valeurs de χ_2 dans l'exemple précédent, on peut utiliser la description suivante de la représentation régulière (qui sera aussi utilisée dans le prochain paragraphe).

Proposition J.9. Notons χ_{reg} le caractère de la représentation régulière de G. On a

$$\chi_{\text{reg}}(g) = 0 \text{ si } g \neq 1 \quad \text{et} \quad \chi_{\text{reg}}(1) = |G|.$$

Soient $W_1, \ldots, W_s$ un système complet de représentations irréductibles de G. Notons $d_i = \dim W_i$ et $\chi_i = \chi_{W_i}$ pour tout i. Alors

$$\chi_{\text{reg}} = \sum_{i=1}^{s} d_i \chi_i.$$

Preuve. Notons $R = \mathbb{C}^G$ la représentation régulière de G. On utilise la base $(e_g)_{g\in G}$ de R. On a $\forall g, h \in G$, $\pi_R(g)(e_h) = e_{gh}$. Si $g \neq 1$, les termes diagonaux de la matrice de $\pi_R(g)$ dans cette base sont nuls ($gh \neq h$), donc $\chi_{\text{reg}}(g) = \text{Tr}(\pi_R(g)) = 0$. Le cas $g = 1$ est clair.

Pour $i \in \{1, \ldots, s\}$, on a

$$\dim(\text{Hom}_G(W_i, R)) = \langle \chi_{W_i}, \chi_{\text{reg}} \rangle = \frac{1}{|G|} \sum_{g\in G} \chi_{W_i}(g)\overline{\chi_{\text{reg}}(g)} = \chi_{W_i}(1) = d_i.$$

Le théorème de structure des représentations assure alors que

$$R \cong \bigoplus_{i=1}^{s} W_i^{d_i}$$

et on a le résultat recherché en passant aux caractères. □

Le résultat suivant est souvent utile pour construire une table de caractère, il exprime des relations d'"orthogonalité pondérée" pour les lignes et colonnes de la table des caractères.

Proposition J.10. Soient $C_1, \ldots, C_s$ les classes de conjugaison de G et soient $\chi_1, \ldots, \chi_r$ les caractères irréductibles de G. Alors la matrice

$$M = \left(\sqrt{\frac{|C_j|}{|G|}} \chi_i(C_j) \right) \in \mathcal{M}_s(\mathbb{C})$$

est unitaire, c'est-à-dire que

$$\sum_{k=1}^{s} \overline{\chi_k(C_i)}\chi_k(C_j) = \delta_{ij}\frac{|G|}{|C_i|} \quad \text{et} \quad \sum_{k=1}^{s} \chi_i(C_k)\overline{\chi_j(C_k)}|C_k| = \delta_{ij}|G|$$

En particulier les colonnes de la table des caractères sont deux à deux orthogonales.

Preuve. On applique les relations d'orthogonalité des caractères : $\langle \chi_i, \chi_j \rangle_G = \delta_{ij}$. □

K Application : le théorème "pq" de Burnside

On démontre dans ce paragraphe le théorème de Burnside annoncé au début.

On aura besoin du lemme suivant, qui concerne les entiers algébriques, et que l'on ne montre pas.

Lemme K.1. Soient $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ des racines de l'unité. Supposons que $\frac{\lambda_1+\ldots+\lambda_n}{n}$ est un entier algébrique. Alors on a l'alternative suivante :
- soit $\lambda_1 + \ldots + \lambda_n = 0$,
- soit $\lambda_1 = \ldots = \lambda_n$.

Proposition K.2. Soit V une représentation irréductible de G. Soit C une classe de conjugaison de G et soit $g \in C$. Supposons que $\dim V$ et $|C|$ sont premiers entre eux. Alors $\frac{\chi_V(g)}{\dim V}$ est un entier algébrique. Si de plus $\chi_V(g) \neq 0$, alors $\pi_V(g)$ est une homothétie.

Preuve. Puisque $|C|$ et $\dim V$ sont premiers entre eux, le théorème de Bezout fournit $a, b \in \mathbb{Z}$ tels que $a|C| + b \dim V = 1$, ce qui donne

$$\frac{\chi_V(g)}{\dim V} = \frac{a|C|\chi_V(g)}{\dim V} + b\chi_V(g).$$

Or on sait que $\frac{|C|\chi_V(g)}{\dim V}$ et $\chi_V(g)$ sont des entiers algébriques, donc puisque les entiers algébriques sont un sous-anneau de $\mathbb{C}$, on a démontré la première assertion.

Soient $\lambda_1, \ldots, \lambda_n$ ($n = \dim V$) les valeurs propres de $\pi_V(g)$, qui sont des racines de l'unité. On a $\frac{\chi_V(g)}{n} = \frac{\lambda_1+\ldots+\lambda_n}{n}$ qui est un entier algébrique, donc par le lemme si $\chi_V(g) \neq 0$ on a $\lambda_1 = \ldots = \lambda_n$, et donc $\pi_V(g)$ est une homothétie ($\pi_V(g)$ est diagonalisable). □

Proposition K.3. Soit G un groupe tel qu'il existe une classe de conjugaison C de G satisfaisant à $|C| = p^m$ pour p premier et $m \geq 1$. Alors G n'est pas simple.

Preuve. On va utiliser la description du caractère de la représentation régulière. Rappelons que si $W_1, \ldots, W_s$ sont des représentations irréductibles telles que $\mathrm{Irr}(G) = \{[W_1], \ldots, [W_s]\}$, alors en notant $d_i = \dim W_i$ et $\chi_i = \chi_{W_i}$ pour tout i, on a

$$\chi_{\mathrm{reg}} = \sum_{i=1}^{s} d_i \chi_i$$

où χ_1 est le caractère de la représentation triviale. Soit $g \in C$ ($g \neq 1$ car $|C| > 1$). On a

$$\chi_{\mathrm{reg}}(g) = 0 = \sum_{i=1}^{s} d_i \chi(g) \Rightarrow \frac{-1}{p} = \sum_{i=2}^{s} \frac{d_i \chi_i(g)}{p}$$

On $\frac{-1}{p} \in \mathbb{Q} \setminus \mathbb{Z}$, donc $\frac{-1}{p}$ n'est pas entier algébrique, et il existe donc $i \in \{2, \ldots, s\}$ tel que $\frac{d_i\chi_i(g)}{p}$ n'est pas entier algébrique. En particulier $\chi_i(g) \neq 0$ et p ne divise pas $d_i = \dim(W_i)$, ce qui assure que $|C|$ et $\dim W_i$ sont premiers entre eux. L'avant dernière proposition assure que $\pi_{W_i}(g)$ est une homothétie.

Supposons maintenant G simple. Comme π_{W_i} est irréductible non triviale, on a $\mathrm{Ker}(\pi_{W_i}) \neq \{1\}$ et donc $\mathrm{Ker}(\pi_{W_i}) = \{1\}$ et π_{W_i} injectif. Comme $\pi_{W_i}(g)$ est une homothétie, il commute avec tous les éléments $\pi_{W_i}(h)$, $h \in G$. Alors puisque π_{W_i} est injectif, on a $g \in Z(G)$ et donc puisque G est simple $Z(G) = G$ ($Z(G) \triangleleft G$). Alors G est abélien, donc toutes les classes de conjugaison sont réduites à un élément, ce qui contredit notre hypothèse. On conclut donc que G n'est pas simple. □

Théorème K.4 (Théorème "pq" de Burnside)**.** Soient p et q des nombres premiers. Soit G un groupe d'ordre $p^\alpha q^\beta$ où $\alpha, \beta \in \mathbb{N}$ vérifient $\alpha + \beta \geq 2$. Alors le groupe G n'est pas simple.

Preuve. On peut supposer que α et β sont non nuls sinon on connait le résultat. Montrons qu'il existe une classe de conjugaison $C \neq \{1\}$ telle que q ne divise pas $|C|$. Soient $C_1, \ldots, C_s$ les classes de conjugaison distinctes de G avec $C_1 = \{1\}$. Alors comme $G = C_1 \amalg \ldots \amalg C_s$, on a

$$|G| = 1 + \sum_{i=2}^{s} |C_i|.$$

Comme q divise $|G|$, il existe $i \geq 2$ tel que q ne divise pas C_i. Puisque $|C_i|$ divise $|G|$ (c'est une orbite pour l'opération de G sur lui-même par conjugaison), on a donc $|C_i| = p^m$ pour $m \geq 1$ ou $|C_i| = 1$. Dans le premier cas la proposition précédente assure que G n'est pas simple. Dans le deuxième soit $g \neq 1 \in C_i$. Puisque $|C_i| = 1$, on a $g \in Z(G)$, d'où $\{1\} \subsetneq Z(G)$. Si G était simple on aurait $Z(G) = G$ et G serait abélien. Mais un groupe abélien simple est nécesairement cyclique d'ordre premier, ce qui est contraire à notre hypothèse. □

L Exercices : exemples de représentations.

Exercice 1. Soit $n \in \mathrm{N}^*$. Pour $\sigma \in S_n$, on considère la matrice $M(\sigma) = \sum_{i,j=1}^{n} \delta_{i\sigma(j)} E_{ij} \in \mathcal{M}_n(\mathbb{C})$.
a) Montrer que $M(\sigma) \in \mathrm{GL}_n(\mathbb{C})$.
b) Montrer que l'application $S_n \to \mathrm{GL}_n(\mathbb{C})$, $\sigma \mapsto M(\sigma)$, est un morphisme de groupe.
c) Montrer que la représentation de S_n construite à la question b) est isomorphe à la représentation associée à l'opération naturelle de S_n sur $[n]$.

Exercice 2. Soit G un groupe fini.
a) Soient V et W des représentations de G et soit $f \in \mathrm{Hom}_G(V, W)$. Montrer que ${}^t f \in \mathrm{Hom}_G(W^*, V^*)$.
b) Montrer que l'isomorphisme canonique $V \longrightarrow V^{**}$ est un isomophisme de représentations. En déduire que l'on a un isomorphisme linéaire $\mathrm{Hom}_G(V, W) \cong \mathrm{Hom}_G(W^*, V^*)$, puis que V est irréductible si et seulement si V^* est irréductible.

Exercice 3. Retrouver, en utilisant seulement le lemme de Schur, que les représentations irréductibles d'un groupe fini abélien sont toutes de dimension 1.

Exercice 4. Soit $G \subset \mathrm{GL}_n(\mathbb{C})$ un sous-groupe fini. Alors il existe $p \in \mathrm{GL}_n(\mathbb{C})$ telle que $pGp^{-1} \subset \mathrm{U}_n(\mathbb{C})$.

Exercice 5. Dans le cas où $G = \mathbb{Z}/n\mathbb{Z}$, donner une construction explicite de l'isomorphisme d'algèbres $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}] \simeq \mathbb{C}^n$ du théorème A.1.

Exercice 6. Soit $n \geq 4$ un entier pair. On considère le groupe diédral $\mathcal{D}_n$. On rappelle que

$|D_n| = 2n$ et que $\mathcal{D}_n$ est engendré par des éléments r, s tels que $r^n = 1 = s^2$ et $sr = r^{n-1}s$, et que si G est un groupe contenant des éléments x, y tels que $x^n = y^2 = 1$, $yx = x^{n-1}y$, alors il existe un unique morphisme de groupes $\pi : \mathcal{D}_n \longrightarrow G$ tel que $\pi(r) = x$ et $\pi(s) = y$.
a) Montrer que $|\widehat{\mathcal{D}_n}| = 4$.
b) Soit $\omega = e^{\frac{2i\pi}{n}}$. Montrer que pour tout $h \in \mathbb{Z}$, il existe un unique morphisme de groupes $\pi_h : \mathcal{D}_n \longrightarrow \mathrm{GL}_2(\mathbb{C})$ tel que $\pi(x) = \begin{pmatrix} \omega^h & 0 \\ 0 & \omega^{-h} \end{pmatrix}$ et $\pi(y) = \begin{pmatrix} 0 & \omega^{-h} \\ \omega^h & 0 \end{pmatrix}$.
c) Notons V_h la représentation de dimension 2 associée au morphisme π_h. Montrer que pour $1 \leq h \leq \frac{n}{2} - 1$, alors V_h est une représentation irréductible de $\mathcal{D}_n$.
d) Montrer que pour $1 \leq h, h' \leq \frac{n}{2} - 1$, les représentations V_h et $V_{h'}$ sont isomorphes si et seulement si $h = h'$.
e) Décrire $\mathrm{Irr}(\mathcal{D}_n)$, montrer que $|\mathrm{Irr}(\mathcal{D}_n)| = \frac{n}{2} + 3$ puis que $\mathbb{C}[\mathcal{D}_n] \cong \mathbb{C}^4 \times \mathcal{M}_2(\mathbb{C})^{\frac{n}{2}-1}$.

Exercice 7. Soit G un groupe non abélien d'ordre 8. Décrire $\mathrm{Irr}(G)$ (nombres d'éléments, dimension des représentations irréductibles), et donner la table des caractères de G (on constatera qu'elle ne dépend pas du groupe en question).

Exercice 8. Soit G un groupe non abélien d'ordre pq, où p et q sont des nombres premiers avec $p > q$.
a) Décrire $\mathrm{Irr}(G)$ (nombres d'éléments, dimension des représentations irréductibles). En déduire que $\mathbb{C}[G] \cong \mathbb{C}^q \times \mathcal{M}_q(\mathbb{C})^{\frac{p-1}{q}}$, et le nombre de classes de conjugaison de G.
b) Montrer que pour $n < q$, G n'est isomorphe à aucun sous-groupe de $\mathrm{GL}_n(\mathbb{C})$.

Exercice 9. Soit V une représentation d'un groupe fini G et soit $\phi \in \widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$.
a) Vérifier que l'application

$$\begin{aligned} G &\longrightarrow \mathrm{GL}(V) \\ g &\longmapsto \phi(g)\pi_V(g) \end{aligned}$$

est un morphisme de groupes. On note V_ϕ la représentation de G ainsi obtenue.
b) Montrer que si V est une représentation irréductible de G, alors V_ϕ est aussi une représentation irréductible de G.
c) Déterminer le caractère de la représentation V_ϕ. Montrer alors que les représentations V et V_ϕ ne sont pas isomorphes si et seulement si il existe $g \in G$ tel que $\phi(g) \neq 1$ et $\chi_V(g) \neq 0$.

Exercice 10. Soit V une représentation d'un groupe fini G. Montrer que $\forall g \in G$, on a $\chi_V(g^{-1}) = \overline{\chi_V(g)}$.

Montrer que si $\forall g \in G, \chi_V(g) \in \mathbb{R}$, alors les représentations V et V^* sont isomorphes.

Exercice 11. Soit G un groupe fini opérant sur un ensemble fini X. On cherche à construire des représentations irréductibles de G à partir de la représentation de G sur $\mathbb{C}^X$ associée à cette opération.
A. 1. Soit $t = \sum_{x \in X} e_x$. Montrer que $t \in (\mathbb{C}^X)^G$. En déduire que $\mathbb{C}^X$ est irréductible si et seulement si $|X| = 1$.

2. Montrer qu'il existe une sous-représentation V_X de $\mathbb{C}^X$ telle que l'on ait un isomorphisme de représentations

$$\mathbb{C}^X \cong \mathbb{I} \oplus V_X.$$

3. Pour $g \in G$, on note $\mathrm{Fix}(g) = \{x \in X \mid g.x = x\}$ l'ensemble des points fixes de g. On note χ_X le caractère de la représentation $\mathbb{C}^X$. Montrer que

$$\chi_X(g) = |\mathrm{Fix}(g)| \quad \text{et} \quad \chi_{V_X}(g) = |\mathrm{Fix}(g)| - 1.$$

4. Montrer que

$$\langle \chi_{\mathbb{I}}, \chi_X \rangle = \langle \chi_X, \chi_{\mathbb{I}} \rangle = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| \quad \text{et} \quad \langle \chi_X, \chi_X \rangle = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|^2.$$

B. On suppose désormais que $|X| \geq 2$.

On dit que G opère 2-transitivement sur X si $\forall (x,y), (x',y') \in X \times X$ avec $x \neq y$ et $x' \neq y'$, il existe $g \in G$ tel que $x' = g.x$ et $y' = g.x$.

1. Vérifier que si G opère 2-transitivement sur X alors il opère transitivement sur X.
2. On rappelle la formule de Burnside : si m est le nombre d'orbites pour l'opération de G sur X, on a

$$m = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Montrer que si G opère 2-transitivement sur X, on a

$$2 = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|^2$$

(on étudiera l'opération de G sur $X \times X$ donnée par $g.(x,y) = (g.x, g.y)$, dont on comptera le nombre d'orbites, et on appliquera la formule de Burnside)

3. Montrer que si G opère 2-transitivement sur X, alors la représentation V_X est irréductible.

C. 1. Montrer que pour $n \geq 3$, S_n admet une représentation irréductible de dimension $n-1$.
2. Montrer que pour $n \geq 4$, A_n admet une représentation irréductible de dimension $n-1$.
3. Montrer que pour $n \geq 4$, S_n admet deux représentations irréductibles non isomorphes de dimension $n-1$.

Exercice 12. Montrer que

$$\mathbb{C}[A_4] \cong \mathbb{C}^3 \times \mathcal{M}_3(\mathbb{C}), \quad \mathbb{C}[S_4] \cong \mathbb{C}^2 \times \mathcal{M}_2(\mathbb{C}) \times \mathcal{M}_3(\mathbb{C})^2$$

Dresser la table des caractères des groupes A_4 et S_4.

Exercice 13. Soit G un groupe fini simple non abélien et soit $\pi_V : G \to \mathrm{GL}(V)$ une représentation irréductible non triviale.
a) Montrer que $\pi_V(G) \subset \mathrm{SL}(V)$.
b) Montrer que $\dim(V) \geq 3$.
c) On suppose que $\dim(V) = 3$. Montrer que si $g \in G$ est d'ordre 3, alors $\chi_V(g) = 0$.

Exercice 14. Dresser la table des caractères du groupe A_5 (utiliser l'exercice précédent).

VIII Groupes projectifs linéaires

Ce chapitre est consacré au groupes projectifs linéaires. On va en particulier établir la simplicité des groupes projectifs spéciaux linéaires. Cela fournira de nouveaux exemples de groupes finis simples.

A Généralités

Soient K un corps et E un K-espace vectoriel de dimension finie.

Définition A.1. *Le quotient de* $\mathrm{GL}(E)$ *par son centre est appelé le* ***groupe projectif linéaire de*** *E et est noté* $\mathrm{PGL}(E)$. *De même le quotient de* $\mathrm{SL}(E)$ *par son centre est noté* $\mathrm{PSL}(E)$, *et est appelé* ***groupe projectif spécial linéaire de*** *E. Les groupes matriciels correspondants sont notés* $\mathrm{PGL}_n(K)$ *et* $\mathrm{PSL}_n(K)$.

Dans le cas où le corps K est fini, on obtient des groupes finis, dont le cardinal est donné par le résultat suivant.

Proposition A.2. Soit K un corps fini de cardinal égal à q. On a

1. $|\mathrm{GL}_n(K)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$.
2. $|\mathrm{SL}_n(K)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1}$.
3. $|\mathrm{PGL}_n(K)| = |\mathrm{SL}_n(K)|$.
4. $|\mathrm{PSL}_n(K)| = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1}}{|\mu_n(K)|}$.

Preuve. 1. On identifie $\mathrm{GL}_n(K)$ et $\mathrm{GL}(K^n)$. Soit $e_1,\dots,e_n$ la base canonique de K^n. Si A est dans $\mathrm{GL}_n(K)$, alors $A(e_1),\dots,A(e_n)$ est une base de K^n. Réciproquement toute base de K^n définit un unique élément de $\mathrm{GL}_n(K)$, donc on a une bijection entre $\mathrm{GL}_n(K)$ et l'ensemble des bases de K^n. Pour choisir une telle base $a_1,\dots,a_n$, on doit choisir a_1 non nul, on a donc q^n-1 choix pour a_1. On doit ensuite choisir a_2 non colinéaire à a_1, on a q^n-q choix (la droite engendrée par un élément non nul a q éléments). Plus généralement si $a_1,\dots,a_i$ linéairement indépendants sont choisis, on doit choisir a_{i+1} dans K^n privé de $\mathrm{Vect}(a_1,\dots,a_i)$, donc on a q^n-q^i choix. Donc

$$|\mathrm{GL}_n(K)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$$

Le déterminant induit un isomorphisme $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \cong K^* \Rightarrow |\mathrm{SL}_n(K)| = \frac{|\mathrm{GL}_n(K)|}{|K^*|}$, d'où le deuxième résultat. Les troisièmes et quatrièmes résultats proviennent directement de la description des centres. □

On se propose d'établir le résultat suivant.

Théorème A.3. Soit K un corps et $n \geq 2$. Alors le groupe $\mathrm{PSL}_n(K)$ est simple si et seulement si $(n,K) \notin \{(2,\mathbb{F}_2),(2,\mathbb{F}_3)\}$.

Bien sûr, si q est une puissance d'un nombre premier, $\mathbb{F}_q$ désigne le corps à q éléments.

• On va montrer le résultat pour $n = 2$ de manière assez directe, grâce à des techniques matricielles simples.

• Le cas $n \geq 3$ peut aussi être traité directement grâce à des calculs matriciels (moins naturels, voir [Tauvel]) ou des considérations plus abstraites équivalentes (plus naturelles, voir [Perrin]). On va plutôt utiliser le critère de simplicté d'Iwasawa, qui a le mérite de s'appliquer à des classes plus générales de groupes, et qui par ailleurs nous conduira à étudier l'opération de $\mathrm{PGL}(E)$ sur l'espace projectif associé.

Remarque A.4. On a $|\mathrm{PSL}_2(\mathbb{F}_2)| = 6$ et $|\mathrm{PSL}_2(\mathbb{F}_3)| = 12$, ces groupes ne sont donc pas simples, le sens $\Rightarrow$ du théorème est donc réglé.

B Simplicité de $\mathrm{PSL}_2(K)$

Théorème B.1. Le groupe $\mathrm{PSL}_2(K)$ est simple si et seulement si K a au moins 4 éléments.

On commence par deux résultats généraux sur les groupes.

Lemme B.2. Soit G un groupe et soient N, T des sous-groupes de G avec $N \triangleleft G$. On a $D(TN) \subset D(T)N$, et donc si T est abélien, on a $D(TN) \subset N$.

Preuve. Soient $x, y \in NT : x = n_1 t_1, y = n_2 t_2$ avec $n_1, n_2 \in N$, $t_1, t_2 \in T$. On a

$$\begin{aligned}[x, y] &= n_1 t_1 n_2 t_2 t_1^{-1} n_1^{-1} t_2^{-1} n_2^{-1} \\ &= n_1 n_2' t_1 t_2 t_1^{-1} t_2^{-1} x \ (x, n_2' \in N) \\ &\in [t_1, t_2] N \in D(T)N\end{aligned}$$

où l'on a utilisé plusieurs fois que N est normal, ce qui donne le résultat puisque $D(T)N$ est un sous-groupe. □

Proposition B.3. Soient G un groupe et B un sous-groupe de B. Supposons qu'il existe $w \in G$, $w \notin B$, tel que $G = B \cup BwB$.
Alors pout tout sous-groupe normal $N \triangleleft G$ tel que $N \not\subset B$, on a $G = NB$.

Preuve. Montrons d'abord que si K est un sous-groupe de G tel que $B \subset K$, alors on a $B = K$ ou $K = G$. Si $B \subsetneq K$, soit $x \in K$, $x \notin B$. Alors $x \in BwB$: il existe $b_1, b_2 \in B$ tels que $x = b_1 w b_2$, d'où $w \in BxB$, et $BwB \subset BxB$, et $G = B \cup BwB \subset B \cup BxB \subset K$.

Si maintenant $N \triangleleft G$, on applique ce qui précède à $K = NB$ (c'est un sous-groupe car N normal) : si $N \not\subset B$ on a $B \subsetneq NB$ et $G = NB$. □

Proposition B.4. Soit $B = \{\begin{pmatrix} \lambda & \mu \\ 0 & \lambda^{-1} \end{pmatrix},\ \lambda \in K^*, \mu \in K\}$. B est un sous-groupe de $\mathrm{SL}_2(K)$.
Soit $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. On a $\mathrm{SL}_2(K) = B \cup BwB$.

Preuve. Il est facile de voir que B est bien un sous-groupe de $\mathrm{SL}_2(K)$. Soit $g \in \mathrm{SL}_2(K)$, $g \notin B$. On doit montrer qu'il existe $b_1, b_2 \in B$ tels que $b_1 g b_2 = w$. Ecrivons $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ avec $\gamma \neq 0$. On a

$$\begin{pmatrix} -\gamma & 0 \\ 0 & -\gamma^{-1} \end{pmatrix} \begin{pmatrix} 1 & -\gamma^{-1}\alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} -\gamma & 0 \\ 0 & -\gamma^{-1} \end{pmatrix} \begin{pmatrix} 0 & -\gamma^{-1} \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -\gamma^{-1}\delta \end{pmatrix}$$

et

$$\begin{pmatrix} 0 & 1 \\ -1 & -\gamma^{-1}\delta \end{pmatrix} \begin{pmatrix} 1 & -\gamma^{-1}\delta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = w$$

d'où le résultat. □

Proposition B.5. Soit N un sous-groupe normal de $\mathrm{SL}_2(K)$. On garde les notations précédentes.

1. Si $N \subset B$, alors $N \subset Z(\mathrm{SL}_2(K))$.
2. Si $N \not\subset B$, alors $D(\mathrm{SL}_2(K)) \subset N$.

Preuve. 1. Soit $g \in N$, $g \neq 1$. On a $g = \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix}$ et $wgw^{-1} = \begin{pmatrix} \alpha^{-1} & 0 \\ -\beta & \alpha \end{pmatrix} \in N \subset B$, d'où $\beta = 0$. Par ailleurs

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & -\alpha + \alpha^{-1} \\ 0 & \alpha^{-1} \end{pmatrix} \in N$$

Donc $\alpha^2 = 1$ et $g \in Z(\mathrm{SL}_2(K))$.

2. Supposons $N \not\subset B$. La proposition précédente assure que $\mathrm{SL}_2(K) = B \cup BwB$, et donc la première proposition assure que $\mathrm{SL}_2(K) = NB$. Soit $T_1 = \{\begin{pmatrix} \varepsilon & \mu \\ 0 & \varepsilon \end{pmatrix},\ \varepsilon = \pm 1,\ \mu \in K\}$. On voit sans difficulté que T_1 est un sous-groupe normal de B, et que T_1 est abélien. Montrons que $\mathrm{SL}_2(K) = NT_1$.

On sait que $\mathrm{SL}_2(K)$ est engendrée par les éléments

$$F_{12}(\lambda) = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix},\ F_{21}(\lambda) = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix},\ \lambda \in K$$

et pour montrer que $\mathrm{SL}_2(K) = NT_1$, il suffit donc de voir que ces matrices sont dans NT_1. Evidemment $F_{12}(\lambda) \in T_1 \subset NT_1$. D'autre part

$$F_{21}(\lambda) = w^{-1} F_{12}(-\lambda) w$$

avec $w \in \mathrm{SL}_2(K) = NB = BN : w = bn$ pour $n \in N$ et $b \in B$. Donc $F_{21}(\lambda) \in n^{-1}b^{-1}T_1 bn$. Comme T_1 est normal dans B, on a donc $F_{21}(\lambda) \in NT_1N = NT_1$ (N normal), et finalement $\mathrm{SL}_2(K) = NT_1$. Comme T_1 est abélien, le premier lemme donne $D(\mathrm{SL}_2(K)) = D(NT_1) \subset N$. □

Corollaire B.6. Si K a au moins 4 éléments, les seuls sous-groupes normaux propres de $\mathrm{SL}_2(K)$ sont contenus dans son centre.

Preuve. Dans ce cas on sait que $D(\mathrm{SL}_2(K)) = \mathrm{SL}_2(K)$, le résultat est donc une conséquence de la proposition précédente. □

La démontration de notre théorème est maintenant immédiate : Si N est un sous-groupe normal de $\mathrm{PSL}_2(K)$, alors $\pi^{-1}(N)$ (où $\pi : SL_2(K) \to \mathrm{PSL}_2(K)$ est la surjection canonique) est un sous-groupe normal de $\mathrm{SL}_2(K)$ avec $\pi(\pi^{-1}(N)) = N$, le corollaire donne donc que $N = \{1\}$ ou $N = \mathrm{PSL}_2(K)$.

Si $q = p^n \geq 4$ (avec p premier), il suit donc que $\mathrm{PSL}_2(\mathbb{F}_q)$ est un groupe simple d'ordre $\frac{(q^2-1)q}{2}$ si q impair, et d'ordre $(q^2-1)q$ si q est pair. Ainsi :

• $\mathrm{PSL}_2(\mathbb{F}_4)$ est un groupe simple d'ordre 60 (il est donc isomorphe à A_5, l'unique groupe simple d'ordre 60, mais cela peut aussi se montrer grâce à l'opération sur le plan projectif, voir plus loin).

• $\mathrm{PSL}_2(\mathbb{F}_5)$ est un groupe simple d'ordre 60 (donc isomorphe à A_5).

• $\mathrm{PSL}_2(\mathbb{F}_7)$ est un groupe simple d'ordre 168, il n'est donc isomorphe à aucun A_n. On peut démontrer que c'est, à isomorphisme près, l'unique groupe simple d'ordre 168.

• $\mathrm{PSL}_2(\mathbb{F}_9)$ est un groupe simple d'ordre 360, on peut démontrer qu'il est isomorphe à A_6.

C Opération sur l'espace projectif

Dans la suite E est un K-espace vectoriel de dimension $n > 0$. On note $\mathbb{P}(E)$ l'espace projetif associé à E : c'est l'ensemble des droites vectorielles de E. Lorsque $E = K^n$, on note souvent $\mathbb{P}(K^n) = \mathbb{P}^{n-1}(K)$.

On a une opération évidente de $\mathrm{GL}(E)$ sur sur $\mathbb{P}(E)$, donnée par

$$\begin{aligned} \mathrm{GL}(E) \times \mathbb{P}(E) &\longrightarrow \mathbb{P}(E) \\ (g, D) &\longmapsto g(D) \end{aligned}$$

qui induit par restriction une opération de $\mathrm{SL}(E)$ sur E.

Rappels : soit G un groupe opérant sur un ensemble E
(1) On dit que l'opération est **fidèle** si $\forall x \in G \setminus \{1\}$, $\exists a \in E$ tel que $x.a \neq a$ (en d'autres termes le morphisme $G \longrightarrow S_E$ correspondant à l'opération est injectif).
(2) On dit que l'opération est **2-transitive** si

$$\forall (a,b),(c,d) \in G \times G \text{ avec } a \neq b \text{ et } c \neq d,\ \exists x \in G \text{ t.q } x.a = c \text{ et } x.b = d$$

Proposition C.1. L'opération de $\mathrm{GL}(E)$ (resp. $SL(E)$) sur $\mathbb{P}(E)$ induit une opération fidèle de $\mathrm{PGL}(E)$ (resp. $\mathrm{PSL}(E)$) sur $\mathbb{P}(E)$. Cette opération est 2-transitive si $\dim(E) \geq 2$.

Preuve. Considérons le morphisme de groupes $\alpha : \mathrm{GL}(E) \longrightarrow S_{\mathbb{P}(E)}$ induit par l'opération de $\mathrm{GL}(E)$ sur $\mathbb{P}(E)$. Un élément $u \in \mathrm{GL}(E)$ est dans le noyau si et seulement si il préserve toutes les droites de E.

Lemme C.2. Soit $u \in \mathrm{GL}(E)$. Si u laisse invariantes toutes les droites de E, alors u est une homothétie : il existe $\lambda \in K^*$ tel que $u = \lambda \mathrm{Id}_E$.

Preuve. On peut supposer $\dim(E) \geq 2$, sinon il n'y a rien à montrer. Pour tout $x \in E \setminus \{0\}$, u préserve la droite $D_x = \mathrm{Vect}(x)$, donc il existe $\lambda_x \in K$ tel que $u(x) = \lambda_x x$. Soient alors $x, y \in E$ non colinéaires. On a $u(x+y) = \lambda_{x+y}(x+y) = u(x) + u(y) = \lambda_x x + \lambda_y y$, donc $\lambda_x = \lambda_{x+y} = \lambda_y$. En prenant une base de E en notant λ le scalaire précédent, on voit que $u = \lambda \mathrm{Id}_E$. □

Le centre de $\mathrm{GL}(E)$ étant formé des homothéties, il suit que α induit une opération fidèle de $\mathrm{PGL}(E)$ sur $\mathbb{P}(E)$. Même chose pour $\mathrm{PSL}(E)$.

Pour montrer la 2-transitivité, il suffit de voir que $\mathrm{SL}(E)$ opère 2-transitivement sur $\mathbb{P}(E)$. Soient D_1, D_2, D_1', D_2' des droites de E avec $D_1 \neq D_2$ et $D_1' \neq D_2'$. Soient $e_1, \ldots, e_n$ et $e_1', \ldots, e_n'$ des bases de

E telles que $D_1 = Ke_1$, $D_2 = Ke_2$, $D_1' = Ke_1'$, $D_2' = Ke_2'$. Soit $f \in \mathrm{GL}(E)$ l'unique application linéaire telle que $\forall k$, $f(e_k) = e_k'$. On a $f(D_1) = D_1'$ et $f(D_2) = D_2'$. Si $f \in \mathrm{SL}(E)$, on a le résultat voulu. Sinon on considère $f' \in \mathrm{GL}(E)$ l'unique application linéaire telle que $f(e_1) = \frac{1}{\det(f)} e_1'$ et $\forall k \geq 2$, $f(e_k) = e_k'$. On a $\det(f') = 1$, $f(D_1) = D_1'$ et $f(D_2) = D_2'$, ce qui donne le résultat recherché. □

Remarque C.3. Dans le cas des corps finis, on a les conséquences suivantes.

1. On a un morphisme injectif de groupes $\mathrm{PSL}_n(\mathbb{F}_q) \subset \mathrm{PGL}_n(\mathbb{F}_q) \hookrightarrow S_t$, où $t = \frac{q^n-1}{q-1}$. En particulier $\mathrm{PSL}_2(\mathbb{F}_q) \subset \mathrm{PGL}_2(\mathbb{F}_q) \hookrightarrow S_{q+1}$.
2. $\mathrm{PSL}_n(\mathbb{F}_q)$ et $\mathrm{PGL}_n(\mathbb{F}_q)$ possèdent une représentation irréductible de dimension $\frac{q^n-q}{q-1}$. En particulier $\mathrm{PSL}_2(\mathbb{F}_q)$ et $\mathrm{PGL}_2(\mathbb{F}_q)$ possèdent une représentation irréductible de dimension q (voir les exercices du chapitre précédent).
3. $\mathrm{PGL}_2(\mathbb{F}_3)$ est isomorphe à S_4, et $\mathrm{PSL}_2(\mathbb{F}_3)$ est isomorphe à A_4.
4. $\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{SL}_2(\mathbb{F}_4)$ est isomorphe à A_5.
5. $\mathrm{PGL}_2(\mathbb{F}_5)$ est isomorphe à S_5, et $\mathrm{PSL}_2(\mathbb{F}_5)$ est isomorphe à A_5 (ces deux groupes possèdent donc une représentation irréductible de dimension 5).

La construction de l'opération 2-transitive de $\mathrm{PSL}(E)$ est le premier ingrédient pour lui appliquer le critère de simplicité d'Iwasawa. On aura besoin d'autres propriétés, auxquelles la fin du paragraphe est consacrée.

Si S est une partie d'un groupe G, on note $\langle\langle S \rangle\rangle$ le sous-groupe normal de G engendré par S. Si S est un sous-groupe, alors $\langle\langle T \rangle\rangle = \langle xSx^{-1}, x \in G \rangle$, le sous-groupe engendré par les conjugués de G.

Proposition C.4. Pour $n \geq 2$, on a $\mathrm{SL}_n(K) = \langle\langle F_{12}(\lambda), \lambda \in K \rangle\rangle$.

Preuve. On sait déjà que $\mathrm{SL}_n(K)$ est engendré par les $F_{ij}(\lambda)$, $i \neq j$, $\lambda \in K$. Il suffit donc de voir que $\forall i \neq j$, $\forall \lambda \in K$, on a $F_{ij}(\lambda) \in \langle\langle F_{12}(\lambda), \lambda \in K \rangle\rangle = H$.

Pour $\sigma \in S_n$, notons $M(\sigma)$ la matrice $M(\sigma) = \sum_{i=1}^n E_{\sigma(i),i}$. On a $\det(M(\sigma)) = \varepsilon(\sigma)$, et si $A = \sum_i a_{ij} E_{ij} \in M_n(K)$, on a $M(\sigma)^{-1} A M(\sigma) = \sum_{i,j} a_{\sigma(i)\sigma(j)} E_{ij}$. En particulier on a $M(\sigma)^{-1} F_{12}(\lambda) M(\sigma) = F_{\sigma(1)\sigma(2)}(\lambda)$. Si $n \geq 4$, pour tous $i \neq j$, il existe $\sigma \in A_n$ tel que $\sigma(1) = i$ et $\sigma(2) = j$. On a donc bien $\mathrm{SL}_n(K) = H$.

Si $n = 2$, on a

$$F_{21}(\lambda) = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}$$

et on en déduit bien que $\mathrm{SL}_2(K) = H$. Le cas $n = 3$ est laissé en exercice. □

Proposition C.5. Soit D une droite de E. Alors $\mathrm{Stab}_{\mathrm{PSL}(E)}(D)$ contient un sous-groupe normal et abélien T tel que $\mathrm{PSL}(E) = \langle xTx^{-1}, x \in \mathrm{PSL}(E) \rangle$.

Preuve. Montrons que $\mathrm{Stab}_{\mathrm{SL}(E)}(D)$ contient un sous-groupe normal et abélien T tel que $\mathrm{SL}(E) = \langle xTx^{-1}, x \in G \rangle$. Cela donnera le résultat en utilisant la surjection canonique. Soit $e_1, \ldots, e_n$ une base

de E telle que $D = Ke_1$, et on identifie $\mathrm{SL}(E)$ à $\mathrm{SL}_n(K)$ grâce au choix de cette base. Alors $\mathrm{Stab}_{\mathrm{SL}(E)}(D)$ s'identifie à l'ensemble des matrices de la forme

$$\begin{pmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ 0 & & & \\ \vdots & & M & \\ 0 & & & \end{pmatrix}, \ \lambda_1, \dots \lambda_n \in K, \ M \in \mathrm{GL}_{n-1}(K), \ \lambda_1 \det(M) = 1$$

Considérons l'application

$$\begin{aligned} f : \mathrm{Stab}_{\mathrm{SL}(E)}(D) &\longrightarrow \mathrm{GL}_{n-1}(K) \\ \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ 0 & & & \\ \vdots & & M & \\ 0 & & & \end{pmatrix} &\longmapsto M \end{aligned}$$

On vérifie sans difficulté que f est un morphisme de groupes, soit donc $T = \mathrm{Ker}(f)$, c'est un sous-groupe normal de $\mathrm{Stab}_{\mathrm{SL}(E)}(D)$, dont on voit facilement qu'il est isomorphe à $(K^{n-1}, +)$, et qui est donc abélien. Pour $\lambda \in K$, on a $F_{12}(\lambda) \in T$, donc $\langle\langle F_{12}(\lambda), \lambda \in K \rangle\rangle \subset \langle\langle T \rangle\rangle = \langle xTx^{-1}, x \in \mathrm{SL}(E) \rangle$ et la proposition précédente permet de conclure. □

D Critère de simplicité d'Iwasawa

D.1 Vocabulaire

Définition D.1. *Soit G un groupe opérant sur un ensemble E. Soit $B \subset E$. On dit que B est un G-**bloc** si $|B| \geq 2$, $B \neq E$ et si*

$$\forall x \in G, \text{ on a } xB = B \text{ ou } xB \cap B = \emptyset$$

*On dit que l'opération de G sur E est **primitive** si elle est transitive et s'il n'existe pas de G-bloc.*

Proposition D.2. Soit G un groupe opérant 2-transitivement sur un ensemble E. Alors l'opération est primitive.

Preuve. Soit B une partie de E ayant au moins deux éléments et telle que $B \neq E$. Montrons qu'il existe $x \in G$ tel que $xB \neq B$ et $xB \cap B \neq \emptyset$, cela montrera que B n'est pas un G-bloc. Soient $a \neq b \in B$ et $c \in E \setminus B$. Il existe $x \in G$ tel que $xa = a$ et $xb = c$ (2-transitivité). On a $a \in xB \cap B$ d'où $xB \cap B \neq \emptyset$, et $c \in xB$, $c \notin B$, d'où $xB \neq B$. □

Remarque D.3. (a) Soit G un groupe opérant transitivement sur un ensemble E. Alors l'opération est primitive si et seulement si $\forall a \in E$, le sous-groupe $\mathrm{Stab}_G(a) \subset G$ est maximal.

(b) Soit G un groupe opérant transitivement sur un ensemble E de cardinal p premier. Alors l'opération est primitive.

(c) Le groupe diédral D_4 opère transitivement sur l'ensemble des sommets du carré, mais que l'opération n'est pas primitive.

(d) Le groupe diédral D_5 opère primitivement sur l'ensemble des sommets du pentagone régulier, mais que l'opération n'est pas 2-transitive.

Rappelons que si G est un groupe, on définit une suite décroisante $(D^m(G))_{m\geq 0}$ de sous-groupes (normaux) de G par $D^0(G) = G$, $D^1(G) = D(G)$ (groupe dérivé de G), $\ldots, D^{m+1}(G) = D(D^m(G)$.... Le groupe G est résoluble si et seulement si il existe $m \geq 0$ tel que $D^m(G) = \{1\}$.

D.2 Enoncé

Théorème D.4. (**critère de simplicité d'Iwasawa**) Soit G un groupe opérant sur un ensemble E. Soit $a \in E$, et notons $H = \mathrm{Stab}_G(a)$. On suppose que les conditions suivantes sont vérifiées.

1. $G = D(G)$.
2. L'opération de G sur E est fidèle et primitive.
3. Il existe un sous-groupe résoluble $K \lhd H$ tel que $G = \langle xKx^{-1}, x \in G\rangle$.

Alors le groupe G est simple.

Le corollaire suivant sera suffisant pour nos besoins. Il se déduit de manière évidente du premier théorème (car une opération 2-transitive est primitive).

Théorème D.5. Soit G un groupe opérant sur un ensemble E. Soit $a \in E$, et notons $H = \mathrm{Stab}_G(a)$. On suppose que les conditions suivantes sont vérifiées.

1. $G = D(G)$
2. L'opération de G sur E est fidèle et 2-transitive.
3. Il existe un sous-groupe abélien $K \lhd H$ tel que $G = \langle xKx^{-1}, x \in G\rangle$.

Alors le groupe G est simple.

D.3 Démonstration

Lemme D.6. Soit G un groupe opérant sur un ensemble E et soit $N \subset G$ un sous-groupe opérant transitivement sur E. Pour tout $a \in E$, on a $G = N\mathrm{Stab}_G(a)$.

Preuve. Soit $g \in G$. Comme N opère transitivement sur E, il existe $x \in N$ tel que $x(ga) = a$, d'où $xg \in \mathrm{Stab}_G(a)$ et $g \in N\mathrm{Stab}_G(a)$. □

Lemme D.7. Soit G un groupe opérant primitivement sur un ensemble E et soit $\{1\} \subsetneqq N \lhd G$. On suppose que N opère fidèlement sur E. Alors N opère transitivement sur E.

Preuve. Soit $x \in N$, $x \neq 1$, il existe alors $a \in E$ tel que $xa \neq a$ (opération fidèle). Montrons que $B = Na = E$. Par construction $B = Na$ a au moins deux éléments. Pour $g \in G$, on a $gB = gNa = Nga$ (normalité de N), donc B et gB sont des N-orbites, elles sont donc égales ou disjointes. Si $B \subsetneqq E$, alors B est un G-bloc. Donc $B = E = Na$. □

Démonstration du critère de simplicité d'Iwasawa. Soit G un groupe opérant sur un ensemble E et satisfaisant les hypothèses du théorème D.4. Soit $\{1\} \subsetneqq N \lhd G$. Le lemme précédent assure que N opère transitivement sur E, et le premier lemme assure que pour

tout $a \in E$, on a $G = N\text{Stab}_G(a)$. Soit $a \in E$ tel qu'il existe un sous-groupe résoluble $K \triangleleft H = \text{Stab}_G(a)$ tel que $G = \langle xKx^{-1}, x \in G\rangle$. Comme $G = NH$ et $K \triangleleft H$, on a $NK \triangleleft NH = G$. Pour tout $x \in G$, on a alors

$$NK = xNKx^{-1} = xNx^{-1}xKx^{-1} = NxKx^{-1} \Rightarrow xKx^{-1} \subset NK$$

et on en déduit que $G = NK$. On a alors (voit premier lemme du paragraphe B) que $G = D(G) \subset D(K)N$, puis par récurrence que pour tout m, $G = D^m(G) \subset D^m(K)N$. Comme K est résoluble, on a $D^m(K) = \{1\}$ pour un certain m et donc $G = N$, et le théorème est donc montré. □

Démonstration de la simplicité de $\text{PSL}_n(K)$ lorsque $(n, K) \notin \{(2, \mathbb{F}_2), (2, \mathbb{F}_3)\}$.

$\text{PSL}_n(K)$ opère fidèlement et 2-transitivement sur $\mathbb{P}(K^n)$. De plus $D(\text{PSL}_n(K)) = \text{PSL}_n(K)$ si $(n, K) \notin \{(2, \mathbb{F}_2), (2, \mathbb{F}_3)\}$. Enfin si D est une droite de K^n, alors $\text{Stab}_{\text{PSL}_n(K)}(D)$ contient un sous-groupe normal et abélien T tel que $\text{PSL}_n(K) = \langle xTx^{-1}, x \in \text{PSL}_n(K)\rangle$. On peut donc appliquer le critère de simplicité d'Iwasawa. □

IX le théorème des zéros de Hilbert

Dans ce chapitre on énonce et démontre le théorème des zéros de Hilbert. Ce théorème est une généralisation du théorème de Bezout aux anneaux de polynômes à plusieurs variables. Il est par ailleurs le résultat de base de la géométrie algébrique.

A Rappel : le théorème de Bezout

Pour les polynômes à une variable sur un corps algébriquement clos, le théorème de Bezout a la forme suivante.

Proposition A.1. Soit K un corps algébriquement clos et soient $P, Q \in K[X]$. Les assertions suivantes sont équivalentes.

1. P et Q sont premiers entre eux.
2. Il existe $U, V \in K[X]$ tels que $UP + VQ = 1$.
3. P et Q n'ont pas de racine commune.

Bien sûr l'équivalence entre (1) et (2) est vrai sans l'hypothèse que K est algébriquement clos, car $K[X]$ est un anneau principal.

Que peut-on dire si l'on passe aux polynômes à plusieurs variables ? Bien sûr $(2) \Rightarrow (1)$ reste vrai, mais ce n'est pas le cas de l'implication réciproque (par exemple X et Y sont premiers entre eux dans $K[X, Y]$, mais ne vérifient pas (2)). On s'intéressera donc à l'équivalence possible entre (2) et (3) (il est clair qu'en général $(2) \Rightarrow (3)$).

B Ensembles algébriques affines

Soit K un corps. Pour une partie S de $K[X_1, \ldots, X_n]$, on pose

$$V(S) = \{(a_1, \ldots, a_n) \in K^n \mid \forall P \in S,\ P(a_1, \ldots, a_n) = 0\} \subset K^n$$

$V(S)$ est donc l'ensemble des zéros commun des polynômes $P \in S$. Une telle partie de K^n est appelée un **ensemble algébrique affine**.

Si $S = \{P\}$, on note simplement $V(\{P\}) = V(P)$.

Exemples B.1.

1. $\{(x, y) \in K^2 \mid y = x^2\} = V(Y - X^2) \subset K^2$ est un ensemble algébrique affine.
2. $\mathrm{SL_n}(K)$ est un ensemble algébrique affine ($\subset M_n(K) \simeq K^{n^2}$).
3. Les sous-ensembles algébriques affines de K sont $\emptyset = V(1)$, $K = V(0)$ et les sous-ensembles finis de K.

Proposition B.2. Soient K un corps et $S \subset K[X_1, \ldots, X_n]$.

1. On a $V(S) = V(\langle S \rangle)$, où $\langle S \rangle$ est l'idéal de $K[X_1, \ldots, X_n]$ engendré par S.
2. Il existe des polynômes $P_1, \ldots, P_m \in K[X_1, \ldots, X_n]$ tels que $V(S) = V(P_1, \ldots, P_m)$.

Preuve. Comme $S \subset \langle S \rangle$, on a $V(\langle S \rangle) \subset V(S)$. Un élément arbitraire de $\langle S \rangle$ s'écrit $\sum_{i=1}^{p} A_i B_i$ pour $A_1, \ldots, A_p \in K[X_1, \ldots, X_n]$, $B_1, \ldots, B_p \in S$: on en déduit facilement l'inclusion inverse.

L'anneau $K[X_1, \ldots, X_n]$ est noethérien par le théorème de la base finie de Hilbert (tout idéal est de type fini) : il existe donc $P_1, \ldots, P_m \in K[X_1, \ldots, X_n]$ tels que $\langle S \rangle = (P_1, \ldots, P_m)$. On a donc $V(S) = V(\langle S \rangle) = V((P_1 \ldots, P_m)) = V(P_1, \ldots, P_m)$. □

C Version faible du théorème des zéros de Hilbert

C.1 Enoncé

Théorème C.1. (Théorème des zéros de Hilbert, version faible) Soient K un corps algébriquement clos et I un idéal propre de $K[X_1, \ldots, X_n]$. Alors on a $V(I) \neq \emptyset$.

Une conséquence immédiate est la généralisation attendue du théorème de Bezout.

Théorème C.2. (Théorème de Bezout pour les polynômes à plusieurs variables) Soient K un corps algébriquement clos et $P_1, \ldots, P_r \in K[X_1, \ldots, X_n]$. Les assertions suivantes sont équivalentes.

1. $P_1, \ldots, P_r$ n'ont pas de zéro commun dans K^n.
2. Il existe $Q_1, \ldots, Q_r \in K[X_1, \ldots, X_r]$ tels que $Q_1 P_1 + \ldots + Q_r P_r = 1$.

Preuve. Le sens (2) $\Rightarrow$ (1) est immédiat. Supposons (1) vérifié. Alors $V(P_1, \ldots, P_r) = \emptyset = V(\langle P_1, \ldots, P_r \rangle)$, ce qui d'après le théorème des zéros de Hilbert donne $\langle P_1, \ldots, P_r \rangle = K[X_1, \ldots, X_n]$, et puisque

$$\langle P_1, \ldots, P_r \rangle = K[X_1, \ldots, X_n] P_1 + \cdots + K[X_1, \ldots, X_n] P_r,$$

on le résultat. □

C.2 Démonstration

La démonstration va s'appuyer sur le résultat suivant.

Théorème C.3. (Zariski) Soit $K \subset L$ une extension de corps. Si L est de type fini comme K-algèbre, alors L est de type fini comme K-module, et en particulier l'extension $K \subset L$ est algébrique.

Preuve. On démontre le résultat par récurrence sur les nombre de générateurs en tant que K-algèbre. Si $K = L$ il n'y a rien à montrer, supposons donc que $L = K[v_1, \ldots v_n]$ pour $n \geq 1$. Si $n = 1$, on a donc $K(v_1) \subset L = K[v_1]$, d'où $K(v_1) = K[v_1]$. Des résultats connus de théorie des corps assurent alors que l'extension $K \subset K(v_1) = L$ est finie.

Supposons donc maintenant $n > 1$ et le résultat montré au rang $n-1$. Posons $K_1 = K(v_1)$. Alors par hypothèse de récurrence $K_1 \subset K_1[v_2, \ldots, v_n]$ est une extension finie. Si v_1 est algébrique sur K, alors $K \subset K_1 = K(v_1)$ est finie, et ainsi $K \subset L$ est finie. Supposons donc que v_1 n'est pas algébrique sur K. Alors $K[v_1] \cong K[X]$ et $K(v_1) \simeq K(X)$.

On utilisera le lemme suivant.

Lemme C.4. Il n'existe pas de polynôme non nul $P \in K[X]$ vérifiant la propriété suivante : $\forall R \in K(X)$, il existe $N \geq 0$ tel que $P^N R \in K[X]$.

Preuve. Supposons qu'un tel $P \in K[X]$ existe. Soit $R \in K[X]$ non constant premier avec P. Il existe alors $N \geq 0$ tel que $\frac{P^N}{R} \in K[X]$, avec P^N et R premier entre eux : contradiction. □

Il existe donc pour tout v_i des éléments $a_{i,0}, \ldots a_{i,p_{i-1}} \in K_1$ tels que

$$v_i^{p_i} + a_{i,p_i-1} v_i^{p_i-1} + \cdots + a_{i,1} v_i + a_{i,0} = 0$$

Si maintenant $a \in K[v_1]$ est un multiple de tous les dénominateurs des $a_{i,j}$, on a pour tout i

$$(av_i)^{p_i} + a a_{i,p_i-1} (av_i)^{p_i-1} + \cdots + a^{p_i-1} a_{i,1} (av_i) + a^{p_i} a_{i,0} = 0$$

et donc pour tout i, av_i est entier sur $K[v_1]$. Les éléments de L entiers sur $K[v_1]$ forment un sous-anneau. Donc pour tout $z \in L = K[v_1, \ldots, v_n]$, il existe un entier $N \geq 0$ tel que $a^N z$ soit entier sur $K[v_1]$. Ceci est en particulier vrai pour tout $z \in K(v_1) \subset L$, et cela contredit le lemme donné plus haut. Donc v_1 est algébrique sur K et on a le résultat. □

Corollaire C.5. Soit $K \subset L$ une extension de corps avec K algébriquement clos et L de type fini comme K-algèbre. Alors $K = L$.

Preuve. Si K est algébriquement clos, les extensions finies de K sont triviales, il suffit donc d'appliquer le théorème de Zariski. □

Corollaire C.6. Soit K un corps algébriquement clos. Les idéaux maximaux de $K[X_1, \ldots, X_n]$ sont les idéaux de la forme $(X_1 - a_1, \ldots, X_n - a_n)$, $(a_1, \ldots, a_n) \in K^n$.

Preuve. On sait déjà (chapitre III) que l'idéal $(X_1 - a_1, \ldots, X_n - a_n) \subset K[X_1, \ldots, X_n]$ est maximal. Réciproquement, soit I un idéal maximal de $K[X_1, \ldots, X_n]$. Alors $K[X_1, \ldots, X_n]/I$ est un corps, et considérons l'extension de corps $K \subset K[X_1, \ldots, X_n]/I$, $a \mapsto \overline{a}$. Par le corollaire précédent c'est un isomorphisme. Soit $f : K[X_1, \ldots, X_n]/I \to K$ l'isomorphisme inverse, que l'on compose avec la surjection canonique $\pi : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]/I$, ce qui donne un morphisme de K-algèbres $\phi = f \circ \pi : K[X_1, \ldots, X_n] \to K$, surjectif et de noyau I. Pour $i \in \{1, \ldots, n\}$, posons $a_i = \phi(X_i)$. On a alors $(X_1 - a_1, \ldots, X_n - a_n) \subset I$. L'idéal $(X_1 - a_1, \ldots, X_n - a_n)$ est maximal, d'où l'égalité. □

On démontre maintenant sans problème la version faible du théorème des zéros de Hilbert. Soit donc $I \subsetneq K[X_1, \ldots, X_n]$ un idéal. Soit $\mathfrak{M}$ un idéal maximal de $K[X_1, \ldots, X_n]$ tel que $I \subset \mathfrak{M}$ (théorème de Krull). On a $V(\mathfrak{M}) \subset V(I)$, et il suffit donc de montrer que $V(\mathfrak{M}) \neq \emptyset$. Par le corollaire précédent il existe $(a_1, \ldots, a_n) \in K^n$ tel que $\mathfrak{M} = (X_1 - a_1, \ldots, X_n - a_n)$, d'où $(a_1, \ldots, a_n) \in V(\mathfrak{M}) \subset V(I)$.

C.3 Une autre démonstration (cas non dénombrable)

On peut donner une preuve simplifiée du théorème de Zariski dans le cas où K est non dénombrable. Elle repose sur le résultat élémentaire suivant.

Lemme C.7. Soit K un corps. La famille $\{\frac{1}{X-a},\ a \in K\}$ est K-linéairement indépendante dans $K(X)$.

La preuve est laissée en exercice.

Supposons maintenant K non dénombrable et soit $K \subset L$ est un extension de corps. Si L est une K-algèbre de type fini ($L \simeq K[X_1, \ldots, X_n]/I$ pour un idéal I), des arguments standards de théorie des ensembles assurent que L a une K-base dénombrable.

Supposons que $K \subset L$ n'est pas algébrique : alors le choix d'un élément transcendant de L sur K donne un plongement $K(X) \hookrightarrow L$, et par conséquent d'après le lemme aucune K-base de L n'est dénombrable, contradiction. Donc $K \subset L$ est algébrique.

D Le théorème des zéros de Hilbert : version générale et conséquence

Si U est une partie de K^n, on note

$$\mathcal{J}(U) = \{P \in K[X_1, \ldots, X_n] \mid \forall (a_1, \ldots a_n) \in U,\ P(a_1, \ldots, a_n) = 0\}$$

On voit sans difficulté que $\mathcal{J}(U)$ est un idéal de $K[X_1, \ldots, X_n]$.

On a donc deux applications

$$V : \{\text{ideaux de } K[X_1, \ldots, X_n]\} \to \{\text{ensembles algebriques affines} \subset K^n\}$$

$$\mathcal{J} : \{\text{ensembles algebriques affines} \subset K^n\} \to \{\text{ideaux de } K[X_1, \ldots, X_n]\}$$

Il n'est pas difficile de voir que ce ne sont pas des bijections réciproques (par exemple car $V(X_1^2) = V(X_1)$, et il s'agit donc de déterminer les sous-ensembles sur lesquels elles induisent des bijections réciproques.

Définition-Proposition D.1. Soient A est un anneau commutatif et I un idéal de A. On note

$$\mathrm{Rad}(I) = \{x \in I \mid \exists n \in \mathbb{N}^* \text{ tq } x^n \in I\}$$

$\mathrm{Rad}(I)$ est un idéal de A qui contient I, appelé le **radical de** I. On dit qu'un idéal est **radical** s'il est égal à son radical.

C'est une vérification directe en utilsant la formule du binôme. Si $I = (0)$, le radical de I est $\mathrm{Nil}(A)$, l'ensemble des éléments nilpotents de A.

Remarque D.2. Si A est un anneau et I un idéal de A, notons $\pi : A \to A/I$ la surjection canonique. Pour $a \in A$ on a $a \in \mathrm{Rad}(I) \iff \pi(a) \in \mathrm{Nil}(A/I)$.

Exemples D.3. 1. Un idéal premier est radical.

2. On voit sans difficulté que si U est une partie de K^n, alors $\mathcal{J}(U)$ est un idéal radical.
3. L'idéal (X^2-1) de $K[X]$ n'est pas premier, mais si K est de caractérique différente de 2, alors (X^2-1) est radical (car $K[X]/(X^2-1) \simeq K^2$, qui n'a pas de nilpotent non nul).

Théorème D.4. (Théorème des zéros de Hilbert) Soient K un corps algébriquement clos et I un idéal de $K[X_1,\dots,X_n]$. On a

$$\mathcal{J}(V(I)) = \mathrm{Rad}(I)$$

Preuve. Soit I un idéal de $K[X_1,\dots,X_n]$. Vérifions d'abord que $\mathcal{J}(V(I)) \supset \mathrm{Rad}(I)$ (c'est la partie facile). Soit $P \in \mathrm{Rad}(I)$: il existe $m \in \mathbb{N}^*$ tel que $P^m \in I$. Si $(a_1,\dots,a_n) \in V(I)$, on a donc $P^m(a_1,\dots,a_n) = 0 = P(a_1,\dots,a_n)^m$, d'où $P(a_1,\dots,a_n) = 0$ et $P \in \mathcal{J}(V(I))$.

Réciproquement soit $P \in \mathcal{J}(V(I))$. On note $B = K[X_1,\dots,X_n]/I$ et J l'idéal de $K[X_1,\dots,X_n,Z]$ engendré par I et $1-PZ$. Montrons que $V(J) \subset K^{n+1}$ est vide. Sinon, soit $(a_1,\dots,a_n,b) \in V(J)$. On a alors pour tout $Q \in I$, $Q(a_1,\dots a_n) = 0$, c'est-à-dire que $(a_1,\dots,a_n) \in V(I)$, d'où $P(a_1,\dots,a_n) = 0$. Mais par ailleurs $1 - P(a_1,\dots,a_n)b = 0$: contradiction. Ainsi $V(J) = \emptyset$, et la version faible du théorème des zéros de Hilbert assure que $J = K[X_1,\dots X_n,Z]$. Il existe donc $Q \in I$, $R,S \in K[X_1,\dots X_n,Z]$ tels que $RQ + S(1-PZ) = 1$. La surjection canonique $\pi : K[X_1,\dots X_n] \to K[X_1,\dots X_n]/I = B$ induit un morphisme d'anneaux $\tilde{\pi} : K[X_1,\dots X_n,Z] \simeq K[X_1,\dots X_n][Z] \longrightarrow B[Z]$. En appliquenat $\tilde{\pi}$ à l'identité précédente, on voit que $1 - \pi(P)Z$ est inversible dans $B[Z]$. Le lemme suivant assure alors que $\pi(P)$ est nilpotent.

Lemme D.5. Soit B un anneau commutatif et $b \in B$. Alors $1-bZ$ est inversible dans $B[Z]$ si et seulement si b est nilpotent.

La preuve est laissée en exercice. Il existe donc $m \in \mathbb{N}^*$ tel que $\pi(P)^m = 0$, c'est-à-dire que $P^m \in I$, et on a bien $P \in \mathrm{Rad}(I)$. □

Corollaire D.6. Soit K un corps algébriquement clos. On a une correspondance bijective (renversant les inclusions)

$$\begin{array}{c} \{\text{ideaux radicaux de } K[X_1,\dots,X_n]\} \rightleftarrows \{\text{ensembles algebriques affines} \subset K^n\} \\ I \mapsto V(I) \\ \mathcal{J}(X) \hookleftarrow X \end{array}$$

Preuve. On sait déjà du théorème des zéros de Hilbert que si I est un idéal, $\mathcal{J}(V(I)) = \mathrm{Rad}(I)$, donc si I est radical, on a $\mathcal{J}(V(I)) = I$. Il reste à vérifier que si X est un ensemble algébrique affine, on a $X = V(\mathcal{J}(X))$. L'inclusion $X \subset V(\mathcal{J}(X))$ est facile à voir (et est valable pour n'importe quelle partie de K^n). On peut écrire $X = V(I)$, et puisque $I \subset \mathcal{J}(V(I)$, on a $V(\mathcal{J}(V(I))) \subset V(I)$, d'où $V(\mathcal{J}(X)) \subset X$, et $V(\mathcal{J}(X)) = X$. □

A Appendice : le corps des fractions d'un anneau intègre

Soit A un anneau intègre. Il peut être commode de plonger A dans un corps. Un tel plongement est toujours possible, et il existe même un plongement minimal.

On fixe donc un anneau *intègre commutatif* A. On définit sur l'ensemble $A \times A^*$ une relation $\mathcal{R}$ par

$$(a,s)\mathcal{R}(a',s') \iff as' = a's.$$

On vérifie, en utilisant l'intégrité de A, que $\mathcal{R}$ est une relation d'équivalence sur $A \times A^*$. On note $[\frac{a}{s}]$ la classe d'equivalence d'un élément (a,s) de $A \times A^*$.

Théorème .7. L'ensemble $(A \times A^*)/\mathcal{R}$ est un corps, pour les lois $(a,b \in A, s,t \in A^*)$:

$$[\frac{a}{s}] + [\frac{b}{t}] = [\frac{at+bs}{st}],$$

$$[\frac{a}{s}][\frac{b}{t}] = [\frac{ab}{st}].$$

Le corps $(A \times A^*)/\mathcal{R}$ est appelé **le corps des fractions de** A, et est noté $\mathrm{Fr}(A)$. L'application $i : A \longrightarrow \mathrm{Fr}(A)$, $a \longmapsto [\frac{a}{1}]$, est un morphisme injectif d'anneaux.

Schéma de preuve. On montre d'abord que les lois en question sont bien définies, c'est-à-dire ne dépendent pas des choix des représentants des classes d'équivalence considérées. On vérifie ensuite que muni de ces lois, $\mathrm{Fr}(A)$ est bien un anneau (neutre pour $+$: $[\frac{0}{1}]$; symétrique d'un élément $[\frac{a}{s}]$ pour $+$: $[\frac{-a}{s}]$; neutre pour $\times$: $[\frac{1}{1}]$), puis que $\mathrm{Fr}(A)$ est un corps (inverse d'un élément $[\frac{a}{s}] \neq 0$ $(a \neq 0)$: $[\frac{s}{a}]$). Il est ensuite immédiat que i est un morphisme d'anneaux, et est injectif. □

Notation. On abandonne assez souvent la notation $[\frac{a}{s}]$ pour la notation plus simple $\frac{a}{s}$. De même on note $1 = [\frac{1}{1}]$.

Exemples. 1) $\mathrm{Fr}(\mathbb{Z}) = \mathbb{Q}$.
2) Soit K un corps : $\mathrm{Fr}(K[X]) = K(X)$, le corps des fractions rationnelles en une indéterminée à coefficients dans K.

Le corps des fractions de A est le plongement minimal de A dans un corps : cela s'exprime par la propriété universelle suivante.

Théorème .8. Soit $f : A \longrightarrow B$ un morphisme d'anneaux tel que $\forall s \in A^*$, on a $f(s) \in U(B)$. Alors il existe un unique morphisme d'anneaux $\overline{f} : \mathrm{Fr}(A) \longrightarrow B$ tel que $\overline{f} \circ i = f$.

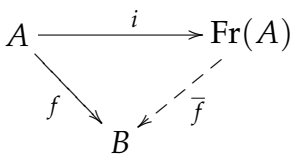


Schéma de preuve. On pose $\overline{f}([\frac{a}{s}]) = f(a)f(s)^{-1}$. On vérifie que $\overline{f}$ est bien définie, puis que $\overline{f}$ est un morphisme d'anneaux satisfaisant $\overline{f} \circ i = f$, et que c'est l'unique tel morphisme. □

Exercices. 1. Soit $A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$. Montrer que $\mathrm{Fr}(A)$ est isomorphe à $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$.
2. Vérifier que si A est una anneau intègre, alors $\mathrm{Fr}(A[X]) \cong \mathrm{Fr}(A)(X)$.

B Appendice : une autre preuve du théorème de la base adaptée

Dans cet appendice on donne une preuve du théorème de la base adaptée indépendante des opérations matricielles sur les lignes et colonnes, et donc valable dans un anneau principal général. Elle est plus aride que celle que nous avons présenté dans le chapitre VI.

Définition-Proposition .9. Soient A un anneau principal, M un A-module libre de rang fini et $x \in M$. Soit $\{e_1, \dots, e_n\}$ une base de M, avec $x = \sum_{i=1}^n a_i.e_i$. Soit

$$c(x) = \text{PGCD}(a_1, \dots, a_n) \in A$$

(défini à un inversible près). On a alors

$$\forall a \in A,\ a|c(x) \iff [\exists y \in M \text{ tq } x = a.y]$$

et $c(x)$ ne dépend pas du choix de la base de M. On dit que $c(x)$ est le **contenu de** x.

Preuve. On peut écrire $x = c(x).(\sum_{i=1}^n b_i.e_i)$, donc si $a|c(x)$ on a $x = a.y$ pour un $y \in M$. Réciproquement, si $x = a.y$ pour $y \in A$, si on écrit $y = \sum_{i=1}^n b_i e_i$, on obtient $a|a_i$, $\forall i$, et donc $a|c(x)$.

Un élément $d \in A$ satisfaisant la propriété

$$\forall a \in A,\ a|d \iff [\exists y \in M \text{ tq } x = a.y]$$

est clairement unique (à multiplication par un inversible près), ce qui assure que la construction de $c(x)$ ne dépend pas du choix d'une base. □.

Proposition .10. Soient A un anneau principal, M un A-module libre de rang fini et $x \in M$.

1. Il existe une application A-linéaire $u : M \longrightarrow A$ telle que $u(x) = c(x)$.
2. Pour toute application A-linéaire $v : M \longrightarrow A$, on a $c(x)|v(x)$.

Preuve. 1. Soit $\{e_1, \dots, e_n\}$ une base de M, avec $x = \sum_{i=1}^n a_i.e_i$. Par le théorème de Bezout il existe $b_1, \dots, b_n \in A$ tels que $c(x) = \sum_{i=1} b_i a_i$. Si $u : M \longrightarrow A$ est l'unique application A-linéaire telle que $u(e_i) = 1$, $\forall i$, on a bien $u(x) = c(x)$.

2. En reprenant les notations précédentes, on a, pour $v \in \text{Hom}_A(M, A)$,

$$v(x) = \sum_{i=1}^n a_i v(e_i) \in \sum_{i=1} Aa_i = Ac(x)$$

ce qui donne le résultat. □

Proposition .11. Soient A un anneau principal, M un A-module libre de rang fini et $x \in M$. Les assertions suivantes sont équivalentes.

1. $c(x) = 1$
2. Il existe $u \in \text{Hom}_A(M, A)$ tel que $u(x) = 1$.
3. $x \neq 0$ et il existe $N \subset M$ un sous-module tel que $M = Ax \oplus N$.
4. Il existe une base $\{e_1, \dots, e_n\}$ de M telle que $x \in \{e_1, \dots, e_n\}$.

Preuve. On a (1) $\Rightarrow$ (2) par la proposition précédente, et (4) $\Rightarrow$ (1) est immédiat. Supposons (2) vérifiée et soit $u \in \mathrm{Hom}_A(M, A)$ tel que $u(x) = 1$. Alors on voit facilement que $M = \mathrm{Ker}(u) \oplus Ax$, et ainsi (3) est vérifiée. Supposons finalement que (3) est vérifiée. Soit $e_2, \ldots, e_n$ une base de N (N est libre par le théorème B.3 du chapitre VI). La partie $\{x, e_2, \ldots, e_n\}$ engendre M et on voit facilement qu'elle est libre (en utilisant le lemme B.2, chap. VI). □

Proposition .12. Soient A un anneau principal, M un A-module libre de rang fini non nul. Alors M contient un élément non nul de contenu minimal, c'est-à-dire un élément $x \in M \setminus \{0\}$ tel que $\forall y \in M \setminus \{0\}$, $c(y)|c(x) \Rightarrow c(y) \sim c(x)$.

Preuve. On considère la famille $\{Ac(y)\}_{y \in M \setminus \{0\}}$ d'idéaux de A. Elle admet un élément maximal $Ac(x)$, $x \in M \setminus \{0\}$, car A est principal, et on a alors, $\forall y \in M \setminus \{0\}$, $c(y)|c(x) \Rightarrow (c(x)) \subset (c(y)) \Rightarrow (c(x)) = (c(y)) \Rightarrow c(y) \sim c(x)$. □

Proposition .13. Soient A un anneau principal, M un A-module libre de rang fini, N un sous-module non nul de M, $x \in N \setminus \{0\}$ un élément non nul de contenu minimal (calculé dans N) et $e \in M$ tel que $x = c(x).e$. Alors

1. Il existe $M_1 \subset M$ un sous-module tel que $M = Ae \oplus M_1$;
2. Posons $N_1 = M \cap M_1$. On a $N = Ax \oplus N_1$;
3. $c(x)$ est le plus petit élément de $\{c(y)\}_{y \in N \setminus \{0\}}$.

Preuve. 1. On a $c(x) \sim c(x)c(e)$, d'où $c(e) = 1$ et donc la première assertion résulte d'une proposition précédente.

2. Soit $p : M \longrightarrow Ae$ la surjection A-linéaire de noyau M_1 avec $p(e) = e$. Le sous-module $p(N)$ de Ae est de la forme Abe, $b \in A$, car A est principal. On a $x = c(x)e$ donc $p(x) = x$ et $x \in p(N) = Abe$, d'où $b|c(x)$. Il existe $y \in N$ tel que $p(y) = be$, donc $b = \varphi(y)$, pour une certaine forme linéaire φ sur M, et $c(y)|b$.

On a $c(y)|b|c(x)$, et comme $c(x)$ est minimal, on a $c(y) \sim c(x) \sim b$. Ainsi $p(N) = Abe = Ac(x)e = Ax \subset N$. Ainsi p induit un projecteur A-linéaire de N dans N, d'image Ax et de noyau $N \cap M_1 = N_1$, d'où $N = Ax \oplus N_1$.

3. Par hypothèse, $c(x)$ est minimal. Montrons que $\forall y \in N \setminus \{0\}$, on a $c(x)|c(y)$. Soit $y \in N \setminus \{0\}$: $y = \lambda x + y_1$, avec $\lambda \in A$ et $y_1 \in N_1$. En prenant une base de M formée de e et d'éléments de M_1, on voit que $c(y) = \mathrm{PGCD}(\lambda c(x), c(y_1))$. Pour montrer que $c(x)|c(y)$, il suffit donc de voir que $c(x)|c(y_1)$. Soit $y' = x + y_1 \in N$. On a $c(y') = \mathrm{PGCD}(c(x), c(y_1))|c(x)$ et $c(y') \sim c(x)$ par minimalité de $c(x)$, et ainsi $c(x)|c(y_1)$. □

Preuve du théorème de la base adaptée. Soit M un A-module libre de rang fini et $N \subset M$ un sous-module libre de rang p (théorème B.2, chap. VI). On raisonne par récurrence sur p, le rang de N. Si $p = 0$, il n'y a rien à démontrer. Supposons $p \neq 0$ et le résultat montré pour tous les sous-modules de rang $< p$. Soit $x_1 \in N \setminus \{0\}$ de contenu minimal. Soit $e_1 \in M$ tel que $x_1 = c(x_1)e_1$. D'après la proposition précédente on a $M = Ae_1 \oplus M_1$ et $N = Ax_1 \oplus N_1$, où M_1 est un sous-module de M et $N_1 = N \cap M_1$. Les modules M_1 et N_1 sont libres par le théorème B.3 du chapitre VI. D'autre part $\mathrm{rg}(N) = \mathrm{rg}(N_1) + 1$ et $\mathrm{rg}(M) = \mathrm{rg}(M) = \mathrm{rg}(M_1) + 1$, d'où $\mathrm{rg}(N_1) = p - 1$ et on peut appliquer l'hypothèse de récurrence au sous-module $N_1 \subset M_1$. Il existe une base $\{e_2, \ldots, e_n\}$ de M_1 et des éléments $a_2, \ldots, a_p$ de A^* tels que $\{a_2e_2, \ldots, a_pe_p\}$ soit une base de N_1 et $a_2|\cdots|a_p$. Alors $\{e_1, \ldots, e_n\}$ est une base de M ($M = Ae_1 \oplus M_1$), et si on pose $a_1 = c(x)$, $\{a_1e_1, a_2e_2, \ldots, a_pe_p\}$ est une base de N ($N = Ax_1 \oplus N_1 = Aa_1e_1 \oplus N_1$). Finalement $c(x) = a_1|a_2 = c(a_2e_2)$ par le 3 de la dernière proposition, car a_2 est un contenu de $a_2e_2 \in N$. □