ALGÈBRE
MAT 7600

Luc Bélair

Automne 2007

Table des matières

Introduction

Ces notes couvrent quelques sujets de base classiques en algèbre. Après avoir introduit les notions appropriées, chaque sujet est approfondi à travers un théorème, ou un petit groupe de théorèmes. Chaque fois, ces théorèmes peuvent être considérés comme le but à atteindre. Ce seront : les applications classiques du lemme de Zorn ; la dualité de Stone ; le théorème de Krull-Schmidt ; le théorème des zéros de Hilbert, l'existence d'équations polynomiales non résolubles par radicaux à partir du degré 5, le 17^e problème de Hilbert. Le chapitre sur les modules a été rédigé en tentant de prendre pour fil conducteur ce qui peut être préservé de la théorie de la dimension en passant des espaces vectoriels aux modules.

Ce recueil est une quatrième version. Je remercie mon collègue Christophe Reutenauer de m'avoir signalé plusieurs éléments à corriger. Je remercie d'avance les personnes qui prendront la peine de me signaler les erreurs de toute nature. J'apprécie aussi tous les commentaires ; ils contribueront à améliorer les prochaines versions.

Luc Bélair
Automne 2007

Chapitre 1

Le lemme de Zorn

Max Zorn[1] a mis en évidence l'utilité d'un principe, maintenant courant en mathématiques, le lemme de Zorn.

1.1 Chaînes dans les ensembles ordonnés

Définition 1.1 *Soit $(X, \geq)$ un ensemble partiellement ordonné.*

(1) Une chaîne *de $(X, \geq)$ est un sous-ensemble dont tous les éléments sont comparables.*

(2) Une chaîne, disons Y, est majorée *si il existe $x_0 \in X$ tel que $y \leq x_0$, pour tout $y \in Y$.*

(3) Un élément maximal *de $(X, \geq)$ est un élément qui n'a pas d'élément plus grand que lui.*

Exemple 1.2 *L'ensemble des nombres naturels $\mathbb{N}$ est partiellement ordonné par la relation de divisibilité, $x \mid y \leftrightarrow \exists z \in \mathbb{N}\,(xz = y)$. Dans cet ensemble ordonné, $\{2^n : n \geq 0\}$ est une chaîne. Il n'y a pas d'élément maximal.*

Proposition 1.3 (Lemme de Zorn) *Soit $(X, \geq)$ un ensemble partiellement ordonné non vide tel que toute chaîne est majorée. Alors $(X, \geq)$ possède au moins un élément maximal.*

Définition 1.4 *On appelle* ensemble inductif *un ensemble partiellement ordonné satisfaisant les hypothèses du lemme de Zorn.*

[1] Max Zorn, 1906-1993.

Le lemme de Zorn est équivalent à l'axiome du choix, qui est indépendant des axiomes de base de la théorie des ensembles.

Axiome du choix *Soit X un ensemble non vide et $P^*(X)$ l'ensemble des parties non vides de X. Alors il existe une application $f : P^*(X) \to X$ tel que pour tout $Y \in P^*(X)$, $f(Y) \in Y$.*

1.2 Applications du lemme de Zorn

Dans les applications, on essaie de représenter un objet cherché comme un élément maximal dans un ensemble partiellement ordonné approprié.

(1) **Tout espace vectoriel non nul possède une base.**

On sait en effet qu'une base d'un espace vectoriel est un ensemble linéairement indépendant maximal. Soit V un espace vectoriel, posons

$$\mathcal{F} = \{S \in \mathcal{P}(V) : S \text{ est linéairement indépendant}\}.$$

On a que $(\mathcal{F}, \subseteq)$ est un ensemble inductif. En effet $\mathcal{F}$ est non vide puisqu'un ensemble formé d'un seul vecteur non nul est linéairement indépendant. D'autre part, si C est une chaîne de $\mathcal{F}$ alors en posant $S_0 = \bigcup C = \{v \in V : \exists Y \in C, v \in Y\}$, on a bien que S_0 est un sous-ensemble de V qui est linéairement indépendant et qui majore tous les éléments de C. Ainsi on peut appliquer le lemme de Zorn à $(\mathcal{F}, \subseteq)$ et on obtient un sous-ensemble de V linéairement indépendant maximal qui fournit une base.

(2) **Tout anneau unitaire possède un idéal (bilatère) maximal propre.**

Soit A un anneau unitaire et posons

$$\mathcal{F} = \{I \in \mathcal{P}(A) : I \lhd A \text{ et } I \neq A\}$$

On a que $(\mathcal{F}, \subseteq)$ est un ensemble inductif. En effet $\mathcal{F}$ est non vide puisqu'on a au moins l'idéal nul (0). D'autre part, si C est une chaîne de $\mathcal{F}$ alors en posant $I_0 = \bigcup C = \{a \in A : \exists I \in C, a \in I\}$, on a bien que I_0 est un idéal ; il est propre, sinon $1 \in I_0$ et alors $1 \in I$ pour un certain $I \in C$, mais les idéaux de la chaîne C sont propres ; donc $I_0 \neq A$. Ainsi on peut appliquer le lemme de Zorn à $(\mathcal{F}, \subseteq)$ et on obtient l'idéal maximal voulu.

(3) **Toute surjection admet une section.**

Soit $f : X \to Y$ une surjection, on cherche une fonction $g : Y \to X$ tel que $fg = id_Y$. Considérons

$$\mathcal{F} = \{(Z, g) : Z \subseteq Y, g : Z \to X \text{ et } fg = id_Z\}$$

On vérifie que la relation suivante définit un ordre partiel sur $\mathcal{F}$: $(Z_1, g_1) \leq (Z_2, g_2)$ ssi $Z_1 \subseteq Z_2$ et $g_2|_{Z_1} = g_1$. On a que $(\mathcal{F}, \leq)$ est un ensemble inductif. En effet, $\mathcal{F}$ est non vide car on peut toujours prendre un singleton $Z = \{y\}$ et un élément x tel que $f(x) = y$ et définir un g par $g(y) = x$. On laisse en exercice la vérification de la condition sur les chaînes. Ainsi on peut appliquer le lemme de Zorn à $(\mathcal{F}, \leq)$ et obtenir un élément maximal, disons (Z_0, g_0). Alors on doit avoir $Z_0 = Y$, sinon soit $b \in Y \setminus Z_0$ et $a \in X$ tel que $f(a) = b$, on peut définir $g : Z_0 \cup \{b\} \to X$ par $g|_{Z_0} = g_0$ et $g(b) = a$, de sorte que $(Z_0 \cup \{b\}, g) \in \mathcal{F}$ et $(Z_0, g_0) < (Z_0 \cup \{b\}, g)$ ce qui contredit la maximalité de (Z_0, g_0). Ainsi $Z_0 = Y$ et g_0 est la section cherchée.

(4) **(Théorème de Zermelo[2]) Tout ensemble non vide peut être bien ordonné.**

Soit X un ensemble non vide et considérons

$$\mathcal{F} = \{(Y, \leq) : Y \subseteq X \text{ et } (Y, \leq) \text{ est un bon ordre}\}$$

On vérifie que la relation suivante définit un ordre partiel sur $\mathcal{F}$: $(Y_1, \leq_1) \preceq (Y_2, \leq_2)$ ssi $(Y_1, \leq_1)$ est un segment initial de $(Y_2, \leq_2)$. On a que $(\mathcal{F}, \preceq)$ est un ensemble inductif. En effet, $\mathcal{F}$ est non vide puisqu'on peut prendre un sous-ensemble fini Y de X. On laisse en exercice la vérification de la condition sur les chaînes. Ainsi on peut appliquer le lemme de Zorn et obtenir un élément maximal de $(\mathcal{F}, \preceq)$, disons $(Y_0, \leq_0)$. Alors on doit avoir $Y_0 = X$, sinon soit $a \in X \setminus Y_0$ alors on obtient un bon ordre sur $Y_0 \cup \{a\}$ en mettant a à la fin de Y_0 et dont $(Y_0, \leq_0)$ est un segment initial, ce qui contredit la maximalité de $(Y_0, \leq_0)$. Ainsi $Y_0 = X$ et $\leq_0$ est le bon ordre cherché.

[2]Ernst Zermelo, 1871-1953.

(5) **Étant donné deux ensembles X, Y alors il existe ou une injection $X \hookrightarrow Y$ de X dans Y, ou une injection $Y \hookrightarrow X$ de Y dans X.**

On peut supposer les deux ensembles non vides. Considérons

$$\mathcal{F} = \{Z \in \mathcal{P}(X \times Y) : Z \text{ définit le graphe d'une injection d'une partie de } X \text{ dans } Y \text{ ou vice versa}\}$$

On a que $(\mathcal{F}, \subseteq)$ est un ensemble inductif. En effet $\mathcal{F}$ est non vide puisqu'on peut prendre un couple (x, y) et $Z = \{(x, y)\}$. On laisse en exercice la vérification de la condition sur les chaînes. Ainsi on peut appliquer le lemme de Zorn et obtenir un élément maximal, disons G. Soit A la projection de G sur X et B celle sur Y, alors on doit avoir $A = X$ ou $B = Y$. Sinon, disons $x_0 \in X \setminus A, y_0 \in Y \setminus B$, alors $G \cup \{(x_0, y_0)\} \in \mathcal{F}$ et $G \subset G \cup \{(x_0, y_0)\}$ ce qui contredirait la maximalité de G. Ainsi on a le résultat voulu puisque par exemple si $A = X$ alors G donne une injection de X dans Y.

Ce dernier exemple assure en particulier que tous les ensembles ont des cardinalités comparables.

1.3 Zorn, Zermelo, l'axiome du choix et l'induction

On a montré que le lemme de Zorn entraîne le théorème de Zermelo. Par ailleurs, si on a un ensemble non vide X et un bon ordre $\leq$ sur X on peut définir la fonction $f : \mathcal{P}^*(X) \to X$, $f(Y) = \min_{\leq} Y$, qui est bien telle que $f(Y) \in Y$. Donc le théorème de Zermelo entraîne à son tour l'axiome du choix. Vous aurez à vérifier dans une série d'exercices que l'axiome du choix entraîne le lemme de Zorn. Le lemme de Zorn, le théorème de Zermelo et l'axiome du choix sont donc tous équivalents. Notons qu'on peut voir le théorème de Zermelo comme un principe d'induction. En effet, soit $(X, \leq)$ un bon ordre et $\varphi(x)$ une propriété telle que $\varphi(\min X)$ est vrai et aussi telle que $\forall x \in X(\forall_{y<x}\varphi(y) \Rightarrow \varphi(x))$ $(*)$. Alors on a $\forall x \in X\varphi(x)$, car sinon $\{x \in X : \varphi(x) \text{ est faux}\}$ est non vide, différent de X et son minimum contredit la propriété $(*)$ ci-dessus. On peut donc voir le lemme de Zorn comme une espèce de principe d'induction, comme l'indique plusieurs des arguments ci-dessus qui pourraient être reformulés en termes de cette induction[3] à l'aide du théorème de Zermelo.

[3]Ce type d'induction est appelée *induction transfinie*.

Plusieurs propriétés sont formellement équivalentes au lemme de Zorn et à l'axiome du choix[4]. On peut mentionner le théorème de Tykhonov[5] sur le produit d'espaces compacts, et le théorème de Hahn-Banach[6] de l'analyse fonctionnelle.

[4]Voir H. Rubin et J.E. Rubin, *Equivalents of the axiom of choice I (1963),II (1985).*
[5]Andrei Tykhonov, 1906-1993.
[6]Hans Hahn, 1879-1934, Stefan Banach, 1892-1945.

Chapitre 2

Catégories et foncteurs

> « En un sens métamathématique, notre théorie fournit des concepts généraux applicables à toutes les branches des mathématiques abstraites, et contribue ainsi à la tendance actuelle vers un traitement uniforme des différentes disciplines mathématiques. En particulier, elle fournit des occasions de comparer les constructions et les isomorphismes qui interviennent dans différentes branches des mathématiques ; de cette façon elle peut éventuellement suggérer par analogie de nouveaux résultats. »

Eilenberg et Maclane, 1945.

2.1 Introduction

Le mythe fondateur de la théorie des catégories est l'article de Eilenberg et Maclane[1] de 1945, « General theory of natural equivalences ».

On peut rattacher les notions de catégorie et foncteur à deux idées de base. La première, est celle de *passage entre différentes branches des mathématiques*. Un premier exemple est le passage de la géométrie à l'algèbre à travers les coordonnées : de cette façon, une question géométrique est transformée en une question algébrique, par exemple résoudre une équation. Un autre exemple est fourni par la théorie de Galois[2], où cette fois on passe des corps aux groupes : une question sur des corps est transformée en une question sur des groupes (les groupes de Galois). Nous aurons l'occasion de

[1] Samuel Eilenberg, 1913-1998, Saunders Maclane, 1909-2005 ; General theory of natural equivalences, *Transactions of the American Mathematical Society*, vol. 58, 1945, p. 231-294.

[2] Évariste Galois, 1811-1832.

revenir sur cet exemple dans un chapitre ultérieur. La seconde idée, est la *considération des applications dans les constructions mathématiques*. Ainsi lorsque, avec deux groupes H, K on construit le groupe produit $H \times K$, il nous vient en même temps les homorphismes de projection p_H ,sur H, et p_K, sur K. Ce groupe produit peut être caractérisé à isomorphisme près par la propriété remarquable suivante du triplet $(H \times K, p_H, p_K)$: pour tout groupe G et homomorphismes $h : G \to H$, $g : G \to K$, il existe un seul et unique homomorphisme $f : G \to H \times K$ tel que $h = p_K f$ et $g = p_H f$. Cette propriété met aussi en évidence le rôle des applications entre les objets étudiés.

Nous avons besoin de quelques remarques préliminaires de nature ensembliste. Nous allons distinguer les *classes*, qui seront des collections d'objets au sens habituel, des *ensembles*, qui seront les classes qui appartiennent au moins à une autre classe. On suppose a priori que les constructions habituelles ne s'appliquent qu'aux *ensembles*. Alors, par exemple, la classe, disons E, de tous les ensembles n'est pas un ensemble. Car sinon, posons $R = \{x \in E : x \notin x\}$, alors R est un ensemble puisqu'il appartient à l'ensemble des parties de E, donc $R \in E$. Cependant on vérifie qu'on a alors $R \in R \leftrightarrow R \notin R$, ce qui est absurde. On peut voir les ensembles comme étant de $\ll$ petites $\gg$ classes. Ces considérations sont nécessaires à certains moments lorsqu'on utilise les catégories. Nous n'aurons pas à les utiliser de façon précise, elles ne seront pour nous qu'une précaution[3].

2.2 Catégories

Définition 2.1 *Une* catégorie*, disons $\mathcal{C}$, est la donnée de*

(1) Une classe, dont les éléments sont appelés les objets *de la catégorie. On la note $Ob(\mathcal{C})$.*

(2) Pour chaque couple d'objets, disons (A, B), une classe, dont les éléments sont appelés les flèches*, ou* morphismes*,* de A vers B*, tel que des couples distincts n'ont pas de flèches en commun. On note cette classe $Hom_{\mathcal{C}}(A, B)$ et on représente un $u \in Hom_{\mathcal{C}}(A, B)$ par $A \xrightarrow{u} B$. On dit que u est une flèche de A vers B.*

(3) Pour chaque triplet d'objets, disons (A, B, C), une fonction

$$\begin{array}{ccc} Hom_{\mathcal{C}}(A,B) \times Hom_{\mathcal{C}}(B,C) & \longrightarrow & Hom_{\mathcal{C}}(A,C) \\ (u,v) & \longmapsto & vu \end{array}$$

[3]Pour une discussion plus précise de ce formalisme de la théorie des ensembles voir, par exemple, J. D. Monk, *Introduction to set theory.*

appelée produit (composition) *des flèches. Considérant tous les triplets d'objets, le produit des flèches a les propriétés suivantes.*

(3.1) Associativité. *Pour tous triplets de flèches* $A \xrightarrow{u} B \xrightarrow{v} C \xrightarrow{w} D$, *on a* $w(vu) = (wv)u$.

(3.2) Éléments neutres. *Pour tout objet* A *il existe* $e \in Hom_{\mathcal{C}}(A, A)$ *tel que pour tous objets* B, C *et tous* $u \in Hom_{\mathcal{C}}(B, A)$, $v \in Hom_{\mathcal{C}}(A, C)$, *on a* $eu = u$ *et* $ve = v$.

On vérifie en utilisant l'associativité qu'il y a une seule flèche « élément neutre » associé à chaque objet. On l'appelle la *flèche unité* (*identité*) de l'objet, et pour un objet A on la note 1_A . La définition évoque les ensembles et les applications entre les ensembles, et en effet ils fournissent un exemple de catégorie.

Exemple 2.2 *On a la catégorie des ensembles, notée* $\mathcal{ENS}$, *dont les objets sont les ensembles, les flèches sont les applications entre les ensembles, la composition des flèches est la composition habituelle des applications, et les flèches unités sont données par les applications identités.*

Toutefois, cela est trompeur sur le degré de généralité de la notion de catégorie. Une perspective sans doute un peu plus juste est la façon plus abstraite de voir une catégorie, à savoir comme un graphe dont les sommets sont les objets et les arêtes sont les flèches, mais avec des relations sur les flèches qui sont données par la composition. On exploite d'ailleurs cette vision géométrique des choses en représentant des configurations de flèches d'une catégorie à l'aide de *diagrammes* correspondant au graphe associé décrit ci-dessus. On dit alors qu'*un diagramme commute* si tous les chemins entre deux sommets du diagramme donnent toujours, par composition, des flèches égales.

Exemple 2.3 Catégories de structures mathématiques.

(1) La catégorie des groupes, notée $\mathcal{GR}$ *: les objets sont les groupes, les flèches sont les homomorphismes de groupes, la composition est la composition habituelle des homomorphismes, les flèches unités sont les homomorphismes identités.*

(2) La catégorie des anneaux, notée $\mathcal{AN}$ *: les objets sont les anneaux, et on continue comme en (1).*

(3) La catégorie des anneaux unitaires, notée $\mathcal{ANN}$ *: les objets sont les anneaux unitaires etc., mais on prend les homomorphismes qui préserve* 1.

(4) *La catégorie des espaces vectoriels sur un corps fixé, disons k, notée $\mathcal{V}_k$: les objets sont les espaces vectoriels sur k, les flèches sont les applications linéaires etc.*

(5) *La catégorie des espaces topologiques, notée $\mathcal{TOP}$: les objets sont les espaces topologiques, les flèches sont les applications continues etc.*

Et ainsi de suite...

Rappelons qu'un préordre sur un ensemble non vide X est une relation binaire, noté $\leq$, qui est réflexive et transitive (il ne manque donc que l'antisymétrie pour avoir un ordre partiel) ; on dira qu'on a un ensemble préordonné. Les ensembles ordonnés sont en particuliers des ensembles préordonnés. La relation de divisibilité dans un anneau intègre fournit d'autres exemples : ainsi dans $\mathbb{Z}$, avec $x \leq y \leftrightarrow x \mid y$ (notons qu'ici $(x \mid y \,\&\, y \mid x) \rightarrow x = \pm y$).

Exemple 2.4 Catégories associées aux ensembles préordonnés.
Soit $(E, \leq)$ un ensemble préordonné. On associe à ce préordre la catégorie suivante. Les objets sont les éléments de E, on pose $Hom(x, y) = \{f_{x \rightarrow y}\}$, si $x \leq y$, et $Hom(x, y) = \emptyset$, sinon. On vérifie que ces données définissent bien une catégorie. On la notera $\overline{E}$.

On peut remarquer que dans la catégorie $\overline{E}$ il y a au plus une flèche d'un objet vers un autre. On note aussi qu'on peut récupérer $(E, \leq)$ à partir de $\overline{E}$. Ainsi un ensemble préordonné peut être considéré comme une catégorie.

Exemple 2.5 Catégories associés aux monoïdes.
Soit $(M, \bullet, e)$ un monoïde, où $\bullet$ est l'opération et e est l'élément neutre. On associe à ce monoïde la catégorie suivante. Il y a un seul objet qui est M lui-même. Les flèches sont les éléments de M, la composition des flèches est donnée par l'opération $\bullet$ et l'unique flèche unité est e. On vérifie que ces données définissent bien une catégorie. On la notera $\overline{M}$.

On peut récupérer le monoïde de départ à partir de $\overline{M}$. On peut donc considérer un monoïde, en particulier un groupe, comme une catégorie. On peut vérifier que réciproquement, une catégorie qui possède un seul objet peut être identifié à un monoïde (au nom, donc, prédestiné !).

Définition 2.6 *Une catégorie $\mathcal{C}$ est dite une* sous-catégorie *d'une catégorie $\mathcal{D}$ si on a $Ob(\mathcal{C}) \subseteq Ob(\mathcal{D})$, pour tous objets A, B de $\mathcal{C}$, $Hom_{\mathcal{C}}(A, B) \subseteq Hom_{\mathcal{D}}(A, B)$ et la composition des flèches coïncide, et $\mathcal{C}$ a les mêmes flèches unités que $\mathcal{D}$.*

On écrit $\mathcal{C} \subseteq \mathcal{D}$ pour désigner que $\mathcal{C}$ est une sous-catégorie de $\mathcal{D}$.

Exemple 2.7 *On a $\mathcal{ANN} \subseteq \mathcal{AN}$.*

2.3 Isomorphismes, sections, rétractions

Définition 2.8 *Soit $\mathcal{C}$ une catégorie. Une flèche $A \xrightarrow{f} B$ est dite un* isomorphisme *si il existe une flèche $B \xrightarrow{g} A$ tel que $fg = 1_B$ et $gf = 1_A$.*

Exemple 2.9

(1) Dans $\mathcal{ENS}$, les isomorphismes sont les bijections.

(2) Dans les catégories $\mathcal{GR}, \mathcal{AN}, \mathcal{ANN}, \mathcal{V}_k$, on retrouve les notions habituelles.

(3) Dans $\mathcal{TOP}$, les isomorphismes sont les homéomorphismes.

(4) Soit $(E, \leq)$ un ensemble préordonné. Dans la catégorie associé $\overline{E}$, $x \to y$ est un isomorphisme si et seulement si $x \leq y \,\&\, y \leq x$. Par exemple pour $(\mathbb{Z}, |)$, $k_1 \to k_2$ est un isomorphisme ssi k_1, k_2 sont associés.

(5) Soit $(M, \bullet, e)$ un monoïde. Dans la catégorie associé $\overline{M}$, $M \xrightarrow{x} M$ est un isomorphisme si et seulement si x est inversible dans M.

Lemme 2.10 *La composition de deux isomorphismes donne un isomorphisme.*

Définition 2.11 *Soit $\mathcal{C}$ une catégorie. Deux objets sont dits* isomorphes *si il existe au moins un isomorphisme entre les deux.*

Définition 2.12 *Soit $\mathcal{C}$ une catégorie. Soit deux flèches $A \underset{g}{\overset{f}{\rightleftarrows}} B$ tel que $fg = 1_B$. On dit alors que g est une* section *de f, et que f est une* rétraction *de g.*

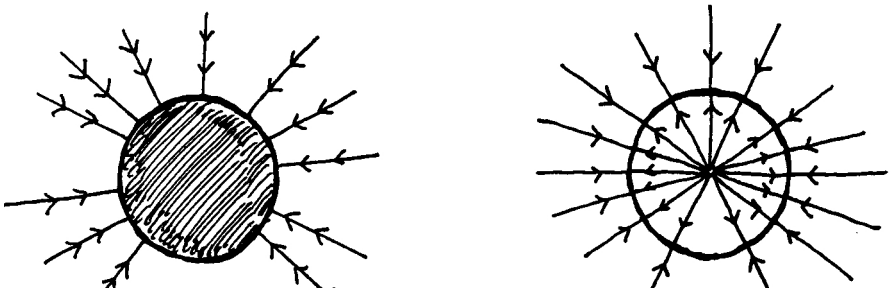
Exemple 2.13 *Dans $\mathcal{ENS}$ on a la situation suivante.*

(1) On vérifie que si une application possède une section alors elle doit être surjective. Réciproquement, toute surjection admet une section (voir chapitre 1).

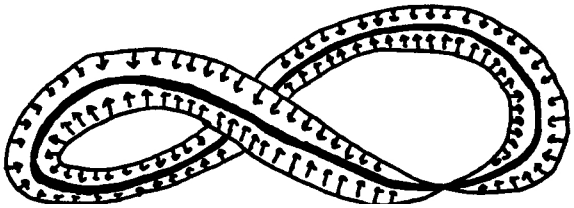
(2) On vérifie que si une application possède une rétraction alors elle doit être injective. Réciproquement, toute injection non triviale admet une rétraction. En effet, soit une injection $f : A \to B$, où A, B sont non vides. Fixons un $a_0 \in A$, et soit $h : B \to A$ définie par $h(b) = f^{-1}(b)$, si b appartient à l'image de f, et $h(b) = a_0$, sinon. On a bien $hf = 1_A$, et donc h est bien une rétraction de f.
Ainsi dans $\mathcal{ENS}$, section est essentiellement synonyme d'application injective et rétraction d'application surjective.

Exemple 2.14 *Dans $\mathcal{TOP}$, considérons l'application d'inclusion $i : B^2 \to \mathbb{R}^2$, du disque unité centré à l'origine dans le plan. Cette application admet une rétraction $r : \mathbb{R}^2 \to B^2$, comme l'indique le dessin de gauche ci-dessous.*

Exemple 2.15 *Encore dans $\mathcal{TOP}$, considérons l'application d'inclusion $i : S \to \mathbb{R}^2 \setminus \{(0,0)\}$, du cercle unité centré à l'origine dans le plan privé de l'origine. Cette application admet une rétraction $r : \mathbb{R}^2 \setminus \{(0,0)\} \longrightarrow S$, comme l'indique le dessin de droite ci-dessous.*



Exemple 2.16 *Toujours dans $\mathcal{TOP}$, considérons l'application d'inclusion $i : S \to M$, d'un grand cercle dans une bande de Moebius. Cette application admet une rétraction $r : M \to S$, comme l'indique le dessin ci-dessous.*



Exemple 2.17 *Dans $\mathcal{GR}$, considérons un groupe G , un sous-groupe normal H de G et la suite d'homomophismes formée de l'inclusion et de l'application canonique*

$$H \xrightarrow{i} G \xrightarrow{\nu} G/H$$

On vérifie que i admet une rétraction (disons r) si et seulement si H est un facteur direct de G , c'est-à-dire qu'il existe un autre sous-groupe normal *L (à savoir* $\ker r$*) tel que $G = HL$ et $H \cap L = \{e\}$. On vérifie que ν admet une section (disons s), si et seulement si G est égal au produit semi-direct de H avec un autre sous-groupe, c'est-à-dire qu'il existe un autre sous-groupe (peut-être pas normal) L (à savoir $s(G/K)$) tel que $G = HL$ et $H \cap L = \{e\}$.*

Exemple 2.18 *Encore dans $\mathcal{GR}$, considérons $\mathbb{C}(T)^*$ le groupe multiplicatif du corps des fonctions rationnelles sur $\mathbb{C}$, et $\mathbb{Z}$ le groupe additif des entiers. On a l'homomorphisme $ord_0 : \mathbb{C}(T)^* \to \mathbb{Z}$, qui associe à une fonction rationnelle l'ordre de 0 comme zéro ou pôle, autrement dit $ord_0(f) = k$ ssi 0 est un zéro d'ordrek ≥ 0 ou un pôle de f d'ordre $-k$. Cet homomorphisme admet la section $\gamma : \mathbb{Z} \to \mathbb{C}(T)^*$ définie par $\gamma(k) = T^k$: c'est bien un homomorphisme, $T^{k_1+k_2} = T^{k_1}T^{k_2}$, et on a bien $ord_0 \circ \gamma = 1_{\mathbb{Z}}$.*

Exemple 2.19 *Dans $\mathcal{ANN}$, considérons l'homomorphisme $év_0 : \mathbb{C}[T] \to \mathbb{C}$, qui associe à chaque polynôme sa valeur en 0. Cet homomorphisme admet la section $\varphi : \mathbb{C} \to \mathbb{C}[T]$, qui associe à chaque nombre complexe le polynôme constant correspondant. Il est immédiat que φ est un homomorphisme et on a bien $év_0 \circ \varphi = 1_{\mathbb{C}}$.*

2.4 Foncteurs

ÊNous allons maintenant définir les « homomorphismes » de catégories, c'est-à-dire les *foncteurs*. Du point de vue des catégories de structures mathématiques, c'est la notion de foncteur qui précise l'idée de passage d'une discipline mathématique à une autre.

Définition 2.20 *Soit $\mathcal{C}, \mathcal{D}$ deux catégories. Un* foncteur*, disons F, de $\mathcal{C}$ dans $\mathcal{D}$ est la donnée des choses suivantes.*

(1) Pour tout $A \in Ob(\mathcal{C})$, un objet de $\mathcal{D}$, noté $F(A)$.

(2) Pour toute flèche $f \in Hom_{\mathcal{C}}(A_1, A_2)$, une flèche de $\mathcal{D}$,

$$F(f) \in Hom_{\mathcal{D}}(F(A_1), F(A_2))$$

tel que pour tout objet A et toutes flèches f, g :

(2.1) $F(1_A) = 1_{F(A)}$

(2.2) $F(gf) = F(g)F(f)$.

On écrit habituellement $F : \mathcal{C} \to \mathcal{D}$ pour désigner que F est un foncteur de $\mathcal{C}$ dans $\mathcal{D}$. Un foncteur est donc une application à la fois sur les objets et les flèches, qui envoie les flèches unités sur les flèches unités appropriées et qui préserve la composition des flèches. On voit qu'un foncteur transformera un diagramme de la catégorie de départ en un diagramme semblable de la catégorie d'arrivée. Puisqu'il préserve la composition des flèches, il transformera en général un diagramme commutatif en un diagramme commutatif. L'effet d'un foncteur sur les flèches en constitue la clé.

Exemple 2.21 Les foncteurs d'inclusion.
L'inclusion d'une sous-catégorie dans une autre est un foncteur.

(1) Le foncteur d'inclusion $i : \mathcal{ANN} \to \mathcal{AN}$*, de la catégorie des anneaux unitaires dans la catégorie des anneaux.*

(2) Celui $i : \mathcal{AB} \to \mathcal{GR}$ *de la catégorie des groupes abéliens dans la catégorie des groupes.*

(3) Celui $i : \mathcal{ENS}_f \to \mathcal{ENS}$ *de la catégorie des ensembles finis dans la catégorie des ensembles.*

(4) Le foncteur identité $id : \mathcal{C} \to \mathcal{C}$ *d'une catégorie dans elle-même !*

Exemple 2.22 Les foncteurs d'oubli.

(1) Si à chaque groupe on associe l'ensemble sous-jacent et à chaque homorphisme de groupes l'application entre les ensembles sous-jacents, on vérifie qu'on obtient un foncteur $U : \mathcal{GR} \to \mathcal{ENS}$*. On l'appelle foncteur d'oubli, puisqu'en quelque sorte on oublie la structure de groupe au passage.*
Sur le même modèle on a les foncteurs d'oubli suivants.

(2) $\mathcal{ANN} \to \mathcal{ENS}$

(3) $\mathcal{V}_k \to \mathcal{ENS}$

(4) $\mathcal{TOP} \to \mathcal{ENS}$

(5) $\mathcal{ANN} \to \mathcal{AB}$

(6) $\mathcal{V}_k \to \mathcal{AB}$.

Exemple 2.23 *Soit* $(E_1, \leq_1), (E_2, \leq_2)$ *deux ensembles préordonnés et* $\overline{E_1}, \overline{E_2}$ *les catégories associés. Considérons un foncteur* $F : \overline{E_1} \to \overline{E_2}$*. Par l'effet sur les flèches on voit qu'on doit avoir pour tous* $x, y \in E_1$*,* $x \leq_1 y \Rightarrow F(x) \leq_2 F(y)$*. Ainsi le foncteur* F *induit une fonction croissante (au sens large) de* E_1 *dans* E_2*. Réciproquement, on vérifie qu'une fonction croissante induit un foncteur.*

Exemple 2.24 *Soit* $(M_1, \bullet, e_1), (M_2, \bullet, e_2)$ *deux monoïdes et* $\overline{M_1}, \overline{M_2}$ *les catégories associées. Les foncteurs* $F : \overline{M_1} \to \overline{M_2}$ *correspondent exactement aux homomorphismes de monoïdes de* M_1 *dans* M_2 *:* $F(e_1) = e_2$ *et* $F(gf) = F(g)F(f)$ *!*

Rappelons que si G est un groupe alors $[G, G]$ désigne le sous-groupe engendré par les commutateurs $[x, y] = xyx^{-1}y^{-1}$, c'est un sous-groupe normal et le groupe quotient $G/[G, G]$ est abélien.

Exemple 2.25 Les groupes rendus abéliens.
À chaque groupe G associons le groupe quotient $G/[G,G]$. Notons ν_G l'application canonique de G dans $G/[G,G]$. Si $f : G_1 \to G_2$ est un homomorphisme de groupes alors il existe un unique homomorphisme

$$\overline{f} : G_1/[G_1,G_1] \to G_2/[G_2,G_2]$$

tel que $\nu_2 f = \overline{f}\nu_1$. On vérifie que ces correspondances donnent un foncteur $ab : \mathcal{GR} \to \mathcal{AB}$, en posant $ab(G) = [G,G]$ et $ab(f) = \overline{f}$.

Notons $\mathcal{TOP}_*$ la catégorie des espaces topologiques pointés avec comme flèches $f : (X,x^*) \to (Y,y^*)$ les applications continues $f : X \to Y$ tel que $f(x^*) = y^*$.

Exemple 2.26 Le groupe fondamental.
À chaque espace topologique pointé (X,x^*) associons le groupe fondamental $\pi_1(X,x^*)$. On sait qu'une fonction continue $f : X \to Y$ induit un homomorphisme

$$f_* : \pi_1(X,x^*) \to \pi_1(Y,f(x^*))$$

tel que $id_* = id$ et pour toutes fonctions continues $f, g\,, (gf)_* = g_* f_*$. On obtient donc un foncteur

$$\pi_1 : \mathcal{TOP}_* \to \mathcal{GR}$$

en posant $\pi_1(f) = f_*$.

Si X est un espace topologique et A un sous-espace de X qui en est un rétracte , c'est-à-dire que l'inclusion $i : A \to X$ admet une rétraction, alors en fixant un point $a \in A$ on aura que $i_* : \pi_1(A,a) \to \pi_1(X,a)$ admet aussi une rétraction , du seul fait que π_1 soit un foncteur. On peut en déduire alors que $\pi_1(X,a)$ est produit semi-direct de $i_*(\pi_1(A,a))$ avec $ker(r_*)$. Ce phénomène est utilisé dans le calcul des groupes fondamentaux.

Exemple 2.27 Les anneaux de matrices.
Fixons un entier $n \geq 1$ et à chaque anneau unitaire A associons l'anneau $M_n(A)$ des matrices carrées de format $n \times n$. Si $f : A \to B$ est un homomorphisme d'anneaux unitaires alors on obtient l'application

$$M_n(f) : M_n(A) \to M_n(B)$$

qui associe à la matrice $[a_{i,j}]$ la matrice $[f(a_{i,j})]$. On vérifie que $M_n(f)$ est bien un homomorphisme d'anneaux unitaires et qu'on obtient un foncteur

$$M_n : \mathcal{ANN} \to \mathcal{ANN}$$

Les foncteurs se composent de la façon naturelle. En particulier on peut parler d'isomorphisme de catégories : un foncteur F est un *isomorphisme* si il existe un foncteur G tel que les compositions FG et GF donnent les foncteurs identités. Il se trouve que la notion d'*équivalence de catégories*, que nous verrons plus loin, est cependant plus riche.

Un autre élément à l'origine des catégories est la question de donner un sens précis à l'idée d'isomorphisme « naturel ». La réponse est la notion de *transformation naturelle*. Nous ne donnerons qu'un exemple ici et renvoyons à l'exercice qui suit pour plus de précision.

Exemple 2.28 *Considérons la construction du bidual d'un espace vectoriel. On peut la présenter par un foncteur* $^{**} : \mathcal{V}_k \to \mathcal{V}_k$. *On sait que si* V *est un espace vectoriel de dimension finie,* V *est isomorphe à son bidual* V^{**} *par l'isomorphisme qui associe à un vecteur* $v \in V$ *la fonctionnelle linéaire* $év(v)$ *sur* V^* *qui consiste en l'évaluation en* v. *On dit que cet isomorphisme est naturel car il ne dépend pas du choix d'une base de* V. *Cette idée se traduit en termes du foncteur bidual* ** *de la façon suivante, qui plus généralement explicite comment la construction du bidual est une construction « naturelle ». Considérons pour chaque espace vectoriel* $V \in \mathcal{V}_k$, *quelle que soit sa dimension, l'application linéaire* $\eta_V : V \to V^{**}$ *qui associe à un vecteur* $v \in V$ *la fonctionnelle d'évaluation en* v. *Alors pour tout homomorphisme d'espaces vectoriels* $f : V \to W$ *on a que* $\eta_W f = f^{**}\eta_V$. *En effet, pour* $v \in V$ *on a d'une part* $\eta_W f(v) = év(f(v))$ *et d'autre part* $f^{**}\eta_V(v) = év(v)f^*$, *où* f^* *est l'homomorphisme* $W^* \to V^*$ *de composition avec* f. *Ainsi pour* $\varphi \in W^*$ *on a*

$$év(v)f^*(\varphi) = év(v)(\varphi f) = \varphi(f(v))$$

donc $év(v)f^*$ *est bien égal à* $év(f(v))$. *On peut voir cette relation comme exprimant un « morphisme » entre le foncteur identité de* $\mathcal{V}_k$ *et le foncteur bidual* **.

$$\begin{array}{ccc} V & \xrightarrow{\eta_V} & V^{**} \\ f \downarrow & & \downarrow f^{**} \\ W & \xrightarrow{\eta_W} & W^{**} \end{array}$$

Exercice 2.29 Transformations naturelles.
Soit $F, G : \mathcal{C} \to \mathcal{D}$ des foncteurs. Une transformation naturelle*, disons η, de F dans G est la donnée pour chaque objet $A \in \mathcal{C}$ d'une flèche $F(A) \stackrel{\eta_A}{\to} G(A)$ dans $\mathcal{D}$, tel que pour toute flèche $A \stackrel{f}{\to} B$ dans $\mathcal{C}$ on ait $\eta_B F(f) = G(f)\eta_A$. On utilise la notation $\eta : F \to G$.*

(1) Vérifiez que le η de l'exemple précédent définit une transformation naturelle du foncteur identité sur $\mathcal{V}_k$ dans le foncteur bidual **.

(2) Pour chaque groupe G, soit $\eta_G : G \to G/[G,G]$ le passage de G à son quotient par $[G,G]$. Vérifiez qu'on obtient ainsi une transformation naturelle du foncteur identité de $\mathcal{GR}$ dans le foncteur ab des groupes rendus abéliens.

(3) Soit F un foncteur. Vérifiez que $1_F : F \to F$ définie par $1_F(A) = 1_{F(A)}$ est une transformation naturelle de F dans lui-même.

(4) Soit $F, G, H : \mathcal{C} \to \mathcal{D}$ des foncteurs, et $\eta : F \to G, \nu : G \to H$ des transformation naturelles. Vérifiez que $\chi : F \to H$ définie par $\chi_A = \nu_A \eta_A$ est une transformation naturelle.

(5) Soit $\mathcal{C}, \mathcal{D}$ des catégories et considérons la classe de tous les foncteurs de $\mathcal{C}$ dans $\mathcal{D}$. Vérifiez qu'en utilisant (4) pour définir une composition de foncteurs on peut faire de tous ces foncteurs une catégorie.

On sait que tout homomorphisme d'espaces vectoriels $V \stackrel{f}{\to} W$ induit un homomorphisme entre leurs espaces duaux mais dans le sens inverse $W^* \stackrel{f^*}{\to} V^*$, où $f^*(\varphi) = \varphi f$. Notons qu'on a $1_V{}^* = 1_{V^*}$ et $(gf)^* = f^* g^*$. On dit alors qu'on a un *foncteur contravariant* , $^* : \mathcal{V}_k \to \mathcal{V}_k$, en associant à chaque espace vectoriel V son espace dual V^* et à chaque flèche $V \stackrel{f}{\to} W$ la flèche $W^* \stackrel{f^*}{\to} V^*$. Un foncteur contravariant est donc essentiellement un foncteur qui renverse le sens des flèches. Pour mettre en évidence le contraste avec les foncteurs contravariants on appellera quelquefois aussi les foncteurs déjà définis, *foncteurs covariants*.

Exemple 2.30

(1) On vérifie qu'on a le foncteur contravariant

$$\mathcal{P} : \mathcal{ENS} \to \mathcal{ENS}$$

défini sur les objets par $\mathcal{P}(X)$ = l'ensemble des parties de X et sur les flèches en associant à une application $X \xrightarrow{f} Y$ l'application $\mathcal{P}(Y) \xrightarrow{f^*} \mathcal{P}(X)$ qui donne l'image réciproque, c'est-à-dire $f^*(A) = \{x \in X : f(x) \in A\}$[4]

(2) Soit $\mathcal{C}$ une catégorie tel que pour tous objets A, B , $Hom_{\mathcal{C}}(A, B)$ est un ensemble (par exemple $\mathcal{GR}$). Fixons un objet A de $\mathcal{C}$. On vérifie qu'on a le foncteur contravariant

$$h_A : \mathcal{C} \to \mathcal{ENS}$$

défini sur les objets par $h_A(B) = Hom_{\mathcal{C}}(B, A)$, et sur les flèches en associant à une flèche $B \xrightarrow{f} C$ l'application $h_A(f) : Hom_{\mathcal{C}}(C, A) \to Hom_{\mathcal{C}}(B, A)$ qui consiste en la composition par f, c'est-à-dire $h_A(f)(\varphi) = f\varphi$.

On définit les transformations naturelles pour les foncteurs contravariants de façon analogue à ce qu'on a déjà pour les foncteurs. Considérons les foncteurs $\mathcal{P}$ et $\mathrm{h}_{\mathbf{2}}$, où $\mathbf{2} = \{0, 1\}$, on peut vérifier (exercice 5.2.6) qu'il existe des transformations naturelles $\eta : \mathcal{P} \to \mathrm{h}_{\mathbf{2}}$, $\xi : \mathrm{h}_{\mathbf{2}} \to \mathcal{P}$ telles que $\eta\xi = 1_{\mathrm{h}_{\mathbf{2}}}$ et $\xi\eta = 1_{\mathcal{P}}$; autrement dit $\mathcal{P}$ et $\mathrm{h}_{\mathbf{2}}$ sont *isomorphes*.

On peut transformer un foncteur contravariant en un foncteur covariant d'une façon assez naturelle, en « redressant » les flèches dans la catégorie d'arrivée. Soit $F : \mathcal{C} \to \mathcal{D}$ un foncteur contravariant. Nous allons changer le sens des flèches dans $\mathcal{D}$ en définissant la *catégorie opposée* de $\mathcal{D}$, notée $\mathcal{D}^{op}$. Les objets de $\mathcal{D}^{op}$ sont les mêmes que ceux de $\mathcal{D}$, pour des objets A, B on pose $Hom_{\mathcal{D}^{op}}(A, B) = Hom_{\mathcal{D}}(B, A)$, les flèches unités sont les mêmes que celles de $\mathcal{D}$ et la composition est celle héritée de $\mathcal{D}$. On vérifie directement qu'on obtient bien une catégorie. On peut maintenant voir le foncteur F comme un foncteur covariant $F : \mathcal{C} \to \mathcal{D}^{op}$. Notons qu'on peut aussi faire le travail sur la catégorie de départ pour obtenir un foncteur covariant $F : \mathcal{C}^{op} \to \mathcal{D}$.

[4] Parfois aussi noté $f^{-1}[A]$.

Exemple 2.31 *Soit $(E, \leq)$ un ensemble préordonné et $\overline{E}$ la catégorie associée. On aura une flèche $x \to y$ dans $\overline{E}$ si et seulement si on a la flèche $y \to x$ dans $\overline{E}^{op}$. Soit $\leq^{op}$ l'ordre inverse de $\leq$ sur E, alors $\overline{E}^{op}$ est la catégorie associée à $(E, \leq^{op})$. On illustre élégamment cette discussion avec l'ordre des nombres naturels.*

2.5 Équivalences de catégories

Si $F : \mathcal{C} \to \mathcal{D}$ est un isomorphisme de catégories alors F induit une bijection au niveau des objets, de $Ob(\mathcal{C})$ sur $Ob(\mathcal{D})$, et aussi au niveau des flèches. La notion d'équivalence de catégories reflète le fait que ce sont les *flèches* qui sont vraiment au coeur de la structure de catégorie.

Définition 2.32 *On dit qu'un foncteur $F : \mathcal{C} \to \mathcal{D}$ est une* équivalence *de $\mathcal{C}$ dans $\mathcal{D}$ si on a :*

(1) pour tout $X \in Ob(\mathcal{D})$ il existe $A \in Ob(\mathcal{C})$ tel que X est isomorphe à $F(A)$;

(2) F induit une bijection sur les flèches, c'est-à-dire :

(2.1) pour toutes flèches $A \overset{f}{\underset{g}{\rightrightarrows}} B$, $F(f) = F(g)$ entraîne $f = g$;

(2.2) pour toute flèche $F(A) \xrightarrow{\varphi} F(B)$ il existe une flèche $A \xrightarrow{f} B$ tel que $\varphi = F(f)$.

Définition 2.33 *Avec la notation ci-dessus, on dit que le foncteur F est* fidèle *si il satisfait (2.1), et qu'il est* plein *si il satisfait (2.2).*

On remarque que tout isomorphisme de catégories est une équivalence.

Exemple 2.34 *Soit $\mathcal{C}$ la catégorie dont les objets sont les ensembles finis suivants*

$$\emptyset, \{0\}, \{0, 1\}, \{0, 1, 2\}, \ldots$$

et dont les flèches sont toutes les applications entre ces ensembles, avec la composition habituelle des fonctions. On voit que $\mathcal{C}$ est une sous-catégorie de la catégorie $\mathcal{ENS}_f$ des ensembles finis. Considérons le foncteur d'inclusion $i : \mathcal{C} \to \mathcal{ENS}_f$, alors on vérifie directement que i est une équivalence.

D'une certaine façon on peut dire que toutes les propriétés catégoriques des ensembles finis apparaissent déjà dans la catégorie $\mathcal{C}$. Notons que ces catégories ne sont sûrement pas isomorphes puisque $Ob(\mathcal{C})$ est dénombrable alors que $Ob(\mathcal{ENS}_f)$ ne l'est pas ; c'est d'ailleurs une classe qui n'est pas un ensemble.

Proposition 2.35 *Soit $F : \mathcal{C} \to \mathcal{D}$ un foncteur. On a que F est une équivalence si et seulement si il existe un foncteur $G : \mathcal{D} \to \mathcal{D}$ tel que FG soit isomorphe au foncteur identité $id_{\mathcal{D}}$ et GF isomorphe au foncteur identité $id_{\mathcal{C}}$.*

LA DUALITÉ DE STONE[5]

Rappelons qu'une algèbre de Boole est un ensemble partiellement ordonné qui a les propriétés suivantes : (1) il possède un élément minimum, habituellement noté 0, et un élément maximum, habituellement noté 1, (2) deux éléments y ont toujours une borne inférieure ou infimum, noté $x \wedge y$, et une borne supérieure ou suprémum, noté $x \vee y$, (3) pour tout élément x il existe un élément y unique tel que $x \vee y = 1$ et $x \wedge y = 0$, (4) vues comme opérations binaires $\vee$ et $\wedge$ sont distributives l'une sur l'autre. L'exemple fondamental est l'ensemble des parties d'un ensemble donné, partiellement ordonné par l'inclusion : le minimum est l'ensemble vide, le maximum est l'ensemble de départ au complet, l'infimum est donné par l'intersection et le suprémum par la réunion, le complémentaire d'un ensemble assure la propriété (3) et on sait bien que la réunion et l'intersection de deux ensembles sont distributives l'une sur l'autre. Ces structures tirent leur origine des travaux de Boole[6] sur la logique.

Le théorème de Stone[7], que nous allons voir, assure en quelque sorte que l'exemple fondamental des parties d'un ensemble révèle bien la structure des algèbres de Boole. Il montre en effet que toute algèbre de Boole peut être représentée comme une sous-algèbre de Boole d'une algèbre de parties. Les travaux de Stone furent motivés par les opérateurs de projection dans un espace de Hilbert[8]. En effet, ces opérateurs forment une algèbre de Boole en posant

$$P_1 \leq P_2 \leftrightarrow P_1P_2 = P_1 \, , \, P_1 \wedge P_2 = P_1P_2 \, , P_1 \vee P_2 = P_1 + P_2 + P_1P_2.$$

Il est sans doute plus clair que ces opérateurs forment un sous-anneau de l'anneau de tous les opérateurs. Cependant on voit le lien en passant aux

[5]Marshall H. Stone, 1903-1989.

[6]George Boole, 1815-1864 ; *The mathematical analysis of logic*, 1847 ; *An investigation of the laws of thoughts*, 1854. Pour les axiomes, voir E.U. Huntingdon, Sets of independent postulates for the algebra of logic, Transactions of the American Mathematical Society, vol.5, 1904.

[7]M. H. Stone, The theory of representations for Boolean algebras, Transactions of the American Mathematical Society, vol. 40, 1936, p. 37-111.

[8]David Hilbert, 1862-1943.

sous-espaces correspondant aux opérateurs de projection : à une projection P on associe le sous-espace fermé $P(H)$, où H est l'espace total. C'est une correspondance biunivoque entre les opérateurs de projection et les sous-espaces fermés. Les opérations ci-dessus se transposent dans des opérations correspondantes sur les sous-espaces : $\wedge$ devient l'intersection, $\vee$ devient la somme et $\leq$ devient l'inclusion, autrement dit $P_1 \leq P_2 \leftrightarrow P_1(H) \subseteq P_2(H)$, $(P_1 \wedge P_2)(H) = P_1(H) \cap P_2(H)$, $(P_1 \vee P_2)(H) = P_1(H) + P_2(H)$. L'anneau des opérateurs de projection possèdent une propriété remarquable en ce que tous ses éléments sont idempotents.

Définition 2.36 *Un anneau de Boole est un anneau unitaire dont tous les éléments sont idempotents.*

Stone remarqua que les algèbres de Boole correspondent en fait exactement aux anneaux de Boole par le même genre de traduction des opérations que pour les opérateurs de projection et leurs sous-espaces associés (voir la propositon 2.38). La représentation des algèbres de Boole par des algèbres d'ensembles se fait au moyen d'un espace topologique associé à l'algèbre de départ. Stone montre de surcroît que les homomorphismes d'algèbre se traduisent en des fonctions continues entre les espaces associés et que les correspondances entre algèbres et espaces d'une part et homomorpismes et fonctions continues d'autre part est très serrée. Au moment où le concept de catégorie fera son apparition, le théorème de représentation de Stone sera un des premiers exemples non triviaux d'équivalence de catégories qu'on pourra se mettre sous les yeux (voir le théorème 2.41).

Définition 2.37

(1) La catégorie des anneaux de Boole *est la catégorie dont les objets sont les anneaux de Boole, les flèches sont les homomorphismes d'anneaux unitaires, les flèches unités sont les applications identités et la composition est la composition habituelle des homomorphismes. On la notera* $\mathcal{ANNB}$.

(2) La catégorie des algèbres de Boole *est la catégorie dont les objets sont les algèbres de Boole, les flèches sont les homomorphismes d'algèbres de Boole, les flèches unités sont les applications identités et la composition est la composition habituelle des homomorphismes. On la notera* $\mathcal{BOOLE}$.

Proposition 2.38 (Stone,1935) *Les catégories* $\mathcal{ANNB}$ *et* $\mathcal{BOOLE}$ *sont isomorphes.*

Démonstration. Voir, par exemple, [1], chap. 2, pp. 91-98. □

Rappelons qu'un espace topologique totalement discontinu est un espace où les seuls sous-ensembles connexes sont les points. Par exemple $\mathbb{Q}$ avec la topologie de l'ordre. Une propriété de base des espaces totalement discontinus est qu'ils possèdent une base d'ouverts fermés. Ainsi dans l'exemple précédent les intervalles à extrémités irrationelles fournissent une base d'ouverts fermés de $\mathbb{Q}$.

Définition 2.39 *La* catégorie des espaces compacts totalement discontinus *est la catégorie dont les objets sont les espaces topologiques séparés compacts et totalement discontinus, les flèches sont les applications continues, les flèches unités sont les applications identités et la composition est la composition habituelle des fonctions continues. On la notera $\mathcal{COMPTD}$.*

Exemple 2.40 *Les espaces suivants sont des espaces compacts totalement discontinus.*

(1) L'ensemble de Cantor.

(2) L'espace de fonctions $\mathbf{2}^{\mathbb{N}}$ avec la topologie produit héritée de la topologie discrète sur $\mathbf{2}$.

(3) Le groupe des automorphismes de corps $Aut(\tilde{\mathbb{Q}})$ comme sous-espace de l'espace de fonctions $\mathbb{Q}^{\tilde{\mathbb{Q}}}$ avec la topologie analogue à celle de (2), où $\tilde{\mathbb{Q}}$ est la clôture algébrique de $\mathbb{Q}$.

(4) Les entiers p-adiques, $\mathbb{Z}_p$, avec la topologie p-adique. On peut voir cet espace de la façon suivante :

$$\mathbb{Z}_p = \{(x_n) \in \prod_{n\geq 1} \mathbb{Z}/(p^n) : x_m \text{ congru à } x_n \text{ modulo } p^n, \text{ si } m \geq n\}$$

et la topologie est la topologie induite par la topologie produit sur $\prod_{n\geq 1} \mathbb{Z}/(p^n)$ héritée de la topologie discrète sur chacun des ensembles finis $\mathbb{Z}/(p^n)$.

Pour tout espace topologique, disons X, la famille de ses ouverts fermés, partiellement ordonnés par l'inclusion, forme une algèbre de Boole. L'élément minimum est $\emptyset$, l'élément maximum est X lui-même, le suprémum de deux éléments est leur l'union et l'infimum leur intersection. On notera cette algèbre de Boole $Ouf(X)$.

Théorème 2.41 (Stone,1936) *Le foncteur $F : \mathcal{COMPTD} \to \mathcal{BOOLE}^{op}$, qui associe à chaque espace compact totalement discontinu X son algèbre de Boole d'ouverts fermés $Ouf(X)$ et à chaque application continue $X \xrightarrow{f} Y$ l'application d'image réciproque $Ouf(Y) \xrightarrow{f^*} Ouf(X)$, est une équivalence.*

On appelle aussi les espaces de la catégorie $\mathcal{COMPTD}$, les espaces *booléens*. Ce genre d'équivalence, à travers un foncteur contravariant, est aussi appelée une *dualité*. On note qu'un atome[9] de l'algèbre $Ouf(X)$ correspond à un point isolé de X .

Corollaire 2.42

(1) Toute algèbre de Boole est isomorphe à une algèbre de Boole d'ensembles, c'est-à-dire à une sous-algèbre d'une algèbre des parties d'un ensemble.

(2) Deux espaces booléens sont homéomorphes si et seulement si leurs algèbres d'ouverts fermés sont isomorphes.

(3) Deux algèbres de Boole sont isomorphes si et seulement si leurs « espaces de Stone » associés sont homéomorphes.

(4) En sachant que toutes les algèbres de Boole infinis dénombrables et sans atome sont isomorphes (voir [1], chap. 2, exercices 11-12)), on en déduit que tous les espaces booléens infinis sans point isolé et avec une base dénombrable d'ouverts fermés sont homéomorphes. Par exemple l'ensemble de Cantor, $\mathbf{2}^{\mathbb{N}}$ et les entiers p-adiques.

Démonstration du théorème 2.41. On vérifiera successivement que

(1) F est un foncteur

(2) F est fidèle

(3) F est plein

(4) F est « essentiellement surjectif », c'est-à-dire que toute algèbre de Boole est *isomorphe* à l'algèbre des ouverts fermés d'un espace compact totalement discontinu.

(1) *F est un foncteur.* Il est immédiat que $F(\ 1_X) =\ 1_{Ouf(X)}$. En général, on a bien que si $X \xrightarrow{f} Y$ est une fonction continue alors l'image réciproque par f d'un ouvert fermé de Y est bien un ouvert fermé de X . D'autre part l'application d'image réciproque préserve toutes les opérations booléennes

[9] Un atome d'une algèbre de Boole est un élément non nul minimal.

sur les ensembles. Ainsi on a bien que $F(f)$ définit un homomorphisme de $Ouf(Y)$ dans $Ouf(X)$. On a vu déjà à l'exercice 2.30 la relation $F(fg) = F(g)F(f)$. Donc F est bien un foncteur contravariant.

(2) *F est fidèle.* Soit $X, Y \in \mathcal{COMPTD}$ et $X \overset{f}{\underset{g}{\rightrightarrows}} Y$ deux flèches tel que $F(f) = F(g)$. Il faut voir que $f = g$. Or si ce n'était pas le cas on aurait $x \in X$ tel que $f(x) \neq g(x)$, donc des ouverts fermés, disons W_1, W_2 tel que $f(x) \in W_1, g(x) \in W_2$ et $W_1 \cap W_2 = \emptyset$. Puisque $F(f) = F(g)$, on a $f^*(W_i) = g^*(W_i)$. Mais alors

$$x \in f^*(W_1) \cap g^*(W_2) = f^*(W_1) \cap f^*(W_2) = f^*(W_1 \cap W_2) = f^*(\emptyset) = \emptyset$$

ce qui est absurde. Donc $f = g$ et F est bien fidèle.

(3) *F est plein.* Soit une flèche $F(X) \overset{\varphi}{\to} F(Y)$ dans $\mathcal{BOOLE}^{op}$, c'est-à-dire un homomorphisme d'algèbre de Boole $\varphi : Ouf(Y) \to Ouf(X)$. Il faut voir qu'il existe une application continue, disons $f : X \to Y$, tel que $f^* = \varphi$. Soit $x \in X$ et considérons $\mathcal{F}_x = \{W \in Ouf(Y) : x \in \varphi(W)\}$. Puisque $\varphi(\emptyset) = \emptyset$, la famille $\mathcal{F}_x$ est une famille de fermés de X dont l'intersection de toute sous-famille finie est non vide. Par compacité, l'intersection de la famille $\mathcal{F}_x$ entière est non vide. Cette intersection ne peut contenir qu'un seul élément. En effet, sinon, disons $y_1, y_2 \in \cap\mathcal{F}_x$ tel que $y_1 \neq y_2$, on aurait $W \in Ouf(Y)$ tel que $y_1 \in W$ et $y_2 \in W^c$, mais alors $x \in \varphi(W)$ entraînerait $W \in \mathcal{F}_x$ ce qui est absurde car $y_2 \notin W$, et $x \notin \varphi(W)$ entraînerait $x \in \varphi(W)^c = \varphi(W^c)$ et donc $W^c \in \mathcal{F}_x$ ce qui est aussi absurde car $y_1 \notin W^c$. On peut donc définir l'application $f_\varphi : X \to Y$ en posant $f_\varphi(x)$ égal à l'unique élément dans $\cap\mathcal{F}_x$. Notons que ${f_\varphi}^* = \varphi$ entraîne automatiquement que f_φ est continue. Il suffit donc de vérifier que ${f_\varphi}^* = \varphi$, c'est-à-dire que pour tout $W \in Ouf(Y), {f_\varphi}^*(W) = \varphi(W)$. Or d'une part on a que $x \in \varphi(W)$ entraîne $W \in \mathcal{F}_x$ qui entraîne $f_\varphi(x) \in W$, c'est-à-dire $x \in {f_\varphi}^*(W)$. Et d'autre part $x \notin \varphi(W)$ entraîne $x \in \varphi(W)^c = \varphi(W^c)$ qui entraîne $f_\varphi(x) \in W^c$, c'est-à-dire $x \notin {f_\varphi}^*(W)$. Ainsi $f_\varphi^*(W)$ et $\varphi(W)$ ont toujours exactement les mêmes éléments et sont donc toujours égaux, ce qui achève la démonstration.

(4) *F est « essentiellement surjectif ».* Pour construire l'espace topologique adéquat associé à une algèbre de Boole nous allons passer par l'anneau de Boole sous-jacent et ses idéaux maximaux. Il est possible, et maintenant classique, de travailler directement sur les algèbres de Boole et leurs « ultrafiltres », qui sont les pendants des idéaux maximaux ; nous passons par les anneaux par commodité et renvoyons à Cori-Lascar [1] pour l'autre formulation. Le lecteur pourra faire l'exercice instructif de faire le passage de l'un

à l'autre.
Soit A une algèbre de Boole. Il faut trouver un espace séparé compact totalement discontinu dont les ouverts fermés forment une algèbre isomorphe à A. Nous allons (4.1) décrire cet espace et (4.2) montrer que son algèbre d'ouverts fermés est isomorphe à A.
(4.1) L'anneau de Boole sous-jacent à A est obtenu en définissant les opérations algébriques suivantes sur A lui-même :

$$xy = x \wedge y\,,\; x + y = (x \wedge y^*) \vee (x^* \wedge y)$$

où a^* désigne l'élément tel que $a \wedge a^* = 0$ et $a \vee a^* = 1$. On voit que l'élément minimum 0 sera l'élément neutre de l'addition et l'élément maximum 1 sera l'élément neutre du produit. On voit aussi que tous les éléments sont idempotents. Cela entraîne que l'anneau A est commutatif. En effet pour tous x, y on a les relations suivantes

$$(-1)^2 = -1\,,\; (-1)^2 = 1$$

$$(x+y)^2 = x + y\,,\; (x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$$

d'où on tire que

$$-1 = 1\,,\; xy + yx = 0\,,\; xy = -yx = yx.$$

D'autre part on note que 1 est le seul élément inversible. En effet, soit x inversible alors on a

$$x^2 = x\,,\; x^2 - x = 0\,,\; x(x-1) = 0$$

et il découle de la dernière égalité que $x = 1$, puisque x est inversible. Ces remarques ont pour conséquence que si M est un idéal maximal de A alors le quotient A/M est nécessairement isomorphe au corps à deux éléments, que nous allons noter ici $\mathbf{2}$, et qu'ainsi les idéaux maximaux de A sont en correspondance biunivoque avec $Hom_{\mathcal{ANNB}}(A, \mathbf{2})$. Posons

$$S(A) = \{M \lhd A : M \text{ est un idéal maximal de } A\}.$$

Pour mettre une topologie sur $S(A)$ nous allons l'identifier avec $Hom_{\mathcal{ANNB}}(A, \mathbf{2})$. Avec la topologie discrète sur $\mathbf{2}$, on obtient l'espace produit $\mathbf{2}^A$ dont $Hom_{\mathcal{ANNB}}(A, \mathbf{2})$ est un sous-espace. On prend la topologie sur $S(A)$ induite par celle de $Hom_{\mathcal{ANNB}}(A, \mathbf{2})$ comme sous-espace de $\mathbf{2}^A$. On note que $\mathbf{2}^A$ est séparé compact totalement discontinu. Donc on sait déjà que $S(A)$ est séparé et totalement discontinu. Puisque $S(A)$ est un sous-espace d'un espace séparé

compact, il suffit de vérifier que c'est un sous-ensemble fermé pour montrer qu'il est compact. Notons qu'une base d'ouverts fermés de $S(A)$ est fournie par les ensembles de la forme

$$V(a) = \{f \in S(A) : f(a) = 1\}.$$

En effet, on a $V(1) = S(A)$, $V(0) = \emptyset$ et

$$\begin{aligned} V(a_1) \cap \ldots \cap V(a_n) &= \{f \in S(A) : f(a_1) = 1, \ldots, f(a_n) = 1\} \\ &= \{f \in S(A) : f(a_1)f(a_2)\ldots f(a_n) = 1\} \\ &= \{f \in S(A) : f(a_1a_2\ldots a_n) = 1\} \\ &= V(a_1 \ldots a_n) \\ V(a)^c &= \{f \in S(A) : f(a) \neq 1\} \\ &= \{f \in S(A) : f(a) = 0\} \\ &= \{f \in S(A) : f(a^*) = 1\} \\ &= V(a^*) \end{aligned}$$

Du point de vue des idéaux maximaux, $V(a) = \{M \in S(A) : a \notin M\}$. On note qu'une application $f : A \to \mathbf{2}$ est un homomorphisme si et seulement si $f(1) = 1$ et pour tous $a, b \in A$,

$$f(a + b) = f(a) + f(b), f(ab) = f(a)f(b).$$

Déjà on a que $\{f : f(1) = 1\}$ est un fermé de $\mathbf{2}^A$. Par ailleurs si on fixe $a, b \in A$, il n'y a qu'un nombre fini de configurations possibles pour remplir les autres conditions à savoir

$$\begin{array}{llll} f(a) = 0, & f(b) = 0, & f(a + b) = 0, & f(ab) = 0 \\ f(a) = 1, & f(b) = 1, & f(a + b) = 0, & f(ab) = 1 \\ f(a) = 0, & f(b) = 1, & f(a + b) = 1, & f(ab) = 0 \\ f(a) = 1, & f(b) = 0, & f(a + b) = 1, & f(ab) = 0 \end{array}$$

Ainsi, si on pose pour $a, b \in A$

$$\begin{array}{l} F_{a,b,1} = \{f \in \mathbf{2}^A : f(a) = 0,\ f(b) = 0,\ f(a + b) = 0,\ f(ab) = 0\} \\ F_{a,b,2} = \{f \in \mathbf{2}^A : f(a) = 1,\ f(b) = 1,\ f(a + b) = 0,\ f(ab) = 1\} \\ F_{a,b,3} = \{f \in \mathbf{2}^A : f(a) = 0,\ f(b) = 1,\ f(a + b) = 1,\ f(ab) = 0\} \\ F_{a,b,4} = \{f \in \mathbf{2}^A : f(a) = 1,\ f(b) = 0,\ f(a + b) = 1,\ f(ab) = 0\}. \end{array}$$

on obtient quatre fermés, et on peut décrire $S(A)$ de la façon suivante

$$S(A) = \{f \in \mathbf{2}^A : f(1) = 1\} \cap \bigcap\nolimits_{a,b \in A} (F_{a,b,1} \cup F_{a,b,2} \cup F_{a,b,3} \cup F_{a,b,4})$$

ce qui en fait un sous-ensemble fermé de $\mathbf{2}^A$. Donc, tel que voulu, $S(A)$ est bien un espace séparé compact totalement discontinu. Il reste à voir qu'il fait bien ce qu'on lui demande.
(4.2) Soit l'application

$$\varphi : A \to Ouf(S(A))$$

définie par $\varphi(a) = V(a)$.
(4.2.1) *φ est un homomorphisme.* En effet, on a

$$\varphi(0) = \emptyset,\ \varphi(1) = S(A)$$

$$\varphi(a \wedge b) = \varphi(ab) = V(ab) = V(a) \cap V(b) = \varphi(a) \cap \varphi(b)$$

$$a \leq b \Rightarrow a \wedge b = a \Rightarrow \varphi(a) \cap \varphi(b) = \varphi(a) \Rightarrow \varphi(a) \subseteq \varphi(b)$$

$$\varphi(a^*) = V(a^*) = V(a)^c = \varphi(a)^*$$

$$\varphi(a \vee b) = \varphi((a^* \wedge b^*)^*) = (\varphi(a)^* \cap \varphi(b)^*)^* = \varphi(a) \cup \varphi(b).$$

(4.2.2) *φ est surjectif.* Soit $W \in Ouf(V(A))$. Alors W, étant fermé, est aussi compact. Donc il peut s'exprimer comme une réunion finie d'ouverts fermés de base et on a

$$W = V(a_1) \cup \ldots \cup V(a_n) = V(a_1 \vee \ldots \vee a_n) = \varphi(a_1 \vee \ldots \vee a_n).$$

(4.2.3) *φ est injectif.* Soit $a, b \in A$ distincts. Alors $a + b \neq 0$, mais on a la relation

$$a+b = a+b+ab+ab+a(1+a)b(1+b) = a(1+b)+(1+a)b+a(1+b)(1+a)b$$

d'où $a(1+b) \neq 0$ ou $(1+a)b \neq 0$; disons $a(1+b) = a+ab \neq 0$. Alors $1+a+ab$ est différent de 1 et il n'est pas inversible. Il appartient donc à au moins un idéal maximal propre et il existe $f \in S(A)$ tel que $f(1 + a + ab) = 0$. La seule possibilité est que $f(a) = 1$ et $f(b) = 0$. Ainsi $f \in V(a)$ mais $f \notin V(b)$, ce qui assure que $V(a)$ et $V(b)$ sont distincts.

Ceci conclut la démonstration du théorème 2.41.

Chapitre 3

Les modules

Un module est en quelque sorte un « espace vectoriel sur un anneau ». Cette théorie a été introduite par Emmy Noether[1] pour fournir un contexte général dans lequel on pourrait « linéariser » les situations, c'est-à-dire se ramener à un contexte proche de l'algèbre linéaire.

3.1 La catégorie des modules sur un anneau

Définition 3.1 *Soit A un anneau unitaire. Un* module (à gauche) *sur A est la donnée de*

1) un groupe abélien $(M, +, 0)$

2) une fonction

$$A \times M \to M$$

$$(a, m) \mapsto am$$

tel que pour tous $a, a_1, a_2 \in A$ et $m, m_1, m_2 \in M$

2.1) $a(m_1 + m_2) = am_1 + am_2$

2.2) $a_1 a_2(m) = a_1(a_2 m)$

2.3) $(a_1 + a_2)m = a_1 m + a_2 m$

2.4) $1m = m$

On désigne habituellement un module par son ensemble sous-jacent ; pour mettre en évidence l'anneau on parle de *A-module*. De façon semblable on définit un *module à droite*. Nous renvoyons à [4] pour le lien entre les

[1] Emmy Noether, 1882-1935.

deux. Si A est un anneau commutatif on peut identifier module à gauche et module à droite. Par commodité, nous ne considérerons ici que les modules à gauche ; les résultats que nous allons voir se transposent directement aux modules à droite.

Exemple 3.2

1) *Si $A = K$ est un corps on obtient les espaces vectoriels habituels.*
2) *Pour $A = \mathbb{Z}$, on obtient les groupes abéliens. En effet, si M est un groupe abéliens on a toujours l'action $\mathbb{Z} \times M \to M$, $1m = m$,$km = \underbrace{m + \ldots + m}_{k fois, k \geq 0}$, $km = - \mid k \mid m$, si $k \leq 0$. D'autre part l'action donnée par une structure de $\mathbb{Z} -$ module sur M coïncide nécessairement avec l'action ci-dessus.*
3) *Un anneau A est naturellement un module sur lui-même par l'action du produit.*
4) *Un idéal à gauche d'un anneau A est un module sur A par l'action du produit dans A. C'est un exemple fondamental de E. Noether.*
5) *Soit A, B des anneaux tel que A est un sous-anneau unitaire de B. Alors B est un module à gauche sur A par l'action du produit dans B.*

Pour un anneau A fixé on a les notions naturelles de sous-module, combinaison linéaire, sous-module engendré, homomorphisme de A-modules. On voit aussi que la classe des A-modules à gauche avec leurs homomorphismes forment naturellement une catégorie. On la notera ${}_A\mathcal{M}$. Ainsi pour un corps K on a ${}_K\mathcal{M} = \mathcal{V}_K$ et on vérifie que ${}_{\mathbb{Z}}\mathcal{M}$ est isomorphe à $\mathcal{AB}$.

On note que si on fixe un élément a d'un anneau, la condition (2.1) de la définition de module assure que l'action de a sur M donne un endomorphisme du groupe abélien M. Les autres conditions assurent qu'en associant à chaque a son action sur M on obtient un homomorphisme d'anneaux unitaires de A dans l'anneau d'endomorphismes $End(M, +)$. On vérifie (exercice 5.3.1) qu'il y a correspondance biunivoque entre les A-modules à gauche et les homorphismes d'anneaux de A dans les anneaux d'endomorphismes de groupes abéliens. À un A-module M on associe l'homomorphisme $\rho_M : A \to End(M, +)$, qui associe à chaque $a \in A$ son action sur M. À chaque homomorphisme d'anneaux unitaires $\rho : A \to End(M, +)$, où M est un groupe abélien, on associe la structure de A-module à gauche $A \times M \to M$ donnée par $am = (\rho(a))(m)$. On peut utiliser cette correspondance pour donner une interprétation de la théorie des représentations en

termes de modules sur des anneaux appropriés. Par exemple, un homomorphisme $G \to GL(V)$ d'un groupe fini G dans le groupe des automorphismes d'un espace vectoriel de dimension finie V sur un corps k correspond à un module sur l'anneau de groupe $k[G]$ par le procédé ci-dessus (voir [4]).

Dans le reste du chapitre module sera synonyme de module à gauche et on travaillera la plupart du temps avec un anneau unitaire A quelconque. On note l'image d'une application f, $im(f)$.

Définition 3.3 *Soit $f : M \to N$ un homorphisme de A-module. On définit le* noyau *de f, noté $ker(f)$, par $ker(f) = \{x \in M : f(x) = 0\}$.*

Lemme 3.4 *Le noyau et l'image d'un homomorphisme de A-modules forment des sous-modules.*

Définition 3.5 *Soit M un A-module et N_1, N_2 deux sous-modules de M. On définit la* somme *de N_1 et N_2, notée $N_1 + N_2$, par*

$$N_1 + N_2 = \{x \in M : x = x_1 + x_2, \text{ pour certains } x_1 \in N_1, x_2 \in N_2\}$$

Lemme 3.6 *Soit M un A-module et N_1, N_2 deux sous-modules de M.*
1) L'intersection $N_1 \cap N_2$ est un sous-module de M.
2) La somme $N_1 + N_2$ est un sous-module de M et c'est le sous-module engendré par $N_1 \cup N_2$.

Soit M un A-module et N un sous-module de M. Alors le groupe abélien quotient M/N est un module de la façon naturelle. En effet si $x_1 - x_2 \in N$ et $a \in A$ alors $ax_1 - ax_2 \in N$, de sorte que l'action $a(x + N) = ax + N$ sur M/N est bien définie. On vérifie directement que M/N devient bien ainsi un A-module. On l'appelle *module quotient* de M par N. On vérifie aussi directement que le passage au quotient $M \to M/N$ est un homomorphisme de A-modules. Nous allons passer en revue les théorèmes fondamentaux sur les modules quotients et les homomorphismes, qui sont entièrement analogues à ceux que vous connaissez déjà pour les anneaux et les groupes.

Théorème 3.7 *Soit M un A-module et N un sous-module. Alors le passage au quotient $\nu : M \to M/N$ établit une correspondance biunivoque entre les sous-modules de M/N et les sous-modules de M qui contiennent N.*

Théorème 3.8 *Soit $f : M \to M_1$ et $g : M \to M_2$ des homomorphismes de A-modules tel que $ker(g) \subseteq ker(f)$ alors il existe un homomorphisme $\overline{g} : M_2 \to M_1$ unique tel que $\overline{g}g = f$. De plus $\overline{g}$ est injectif si et seulement si $ker(g) = ker(f)$.*

Corollaire 3.9 *Soit $f : M \to N$ un homomorphisme de A-modules alors $M/ker(f)$ est isomorphe à $im(f)$ par l'isomorphisme $\overline{f}(x + ker(f)) = f(x)$.*

Théorème 3.10 *Soit M un A-module et N_1, N_2 deux sous-modules. Alors l'homomorphisme naturel $f : N_1/N_1 \cap N_2 \to N_1 + N_2/N_2$, $f(x + N_1 \cap N_2) = x + N_2$, est un isomorphisme de A-modules.*

Théorème 3.11 *Soit M un A-module et N, P des sous-modules de M tel que $P \subseteq N$. Alors l'homomorphisme naturel $f : (M/P)/(N/P) \to M/N$, $f((x + P) + (N/P)) = x + N$, est un isomorphisme de A-modules.*

Nous allons définir le produit direct et la somme directe de modules en toute généralité. Rappelons qu'une famille $(X_i)_{i\in I}$, ou suite indexée par un ensemble I, peut être vue comme une fonction f de domaine I tel que $f(i) = X_i$.

Définition 3.12 *Soit $(M_i)_{i\in I}$ une famille de A-modules.*

1) Le produit direct, ou produit*, de la famille $(M_i)_{i\in I}$, noté $\prod_{i\in I} M_i$, est le A-module formé de toutes les fonctions $f : I \to \bigcup_{i\in I} M_i$ tel que pour tout i, $f(i) \in M_i$, avec les opérations suivantes définies point par point. Ainsi la somme de deux telles fonctions f, g est la fonction $f + g$ définie par $(f + g)(i) = f(i) + g(i)$, et l'action de $a \in A$ sur une fonction f donne la fonction af définie par $(af)(i) = a(f(i))$.*

2) La somme directe, ou somme*, de la famille $(M_i)_{i\in I}$, noté $\bigoplus_{i\in I} M_i$, est le A-module obtenu en prenant le sous-module de $\prod_{i\in I} M_i$ formé des fonctions f tel que $\{i \in I : f(i) \neq 0\}$ est fini.*

On désigne parfois un élément du produit $\prod_{i\in I} M_i$ ou de la somme $\bigoplus_{i\in I} M_i$ par une famille $(x_i)_{i\in I}$ où $x_i \in M_i$. Si tous les M_i sont égaux, disons $M_i = M$ pour tout i, alors le produit est l'ensemble M^I de toutes les fonctions de I dans M. La somme est alors notée $M^{(I)}$. L'ensemble $\{i \in I : f(i) \neq 0\}$ est parfois appelé support de f. Notons que si I est fini alors $\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i$.

Exemple 3.13 *1) Disons $I = \{1, 2\}$. Alors $\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i$ est isomorphe au produit cartésien $M_1 \times M_2$ avec les opérations définies composante à*

composante. On retrouve ainsi une construction analogue aux constructions habituelles dans les groupes abéliens par exemple. Dans un cas comme celui-ci on utilisera aussi la notation $M_1 \oplus M_2$ pour désigner la somme etc.
2) On sait que tout groupe abélien fini est isomorphe à une somme directe de groupes cycliques finis.

Notons qu'on a les projections $p_j : \prod_{i\in I} M_i \to M_j$, définies par l'évaluation en j, qui sont surjectives. De même, on a les injections $\iota_j : M_j \to \bigoplus_{i\in I} M_i$, où $\iota(x)$ est la fonction définie par $\iota(x)(i) = 0$, si $i \neq j$, $\iota(x)(j) = x$. On vérifie que toutes ces applications sont des homomorphismes de A-modules. Le produit muni de toutes ses projections et la somme munie de toutes ses injections possèdent les propriétés remarquables suivantes.

Théorème 3.14 (Propriétés universelles) *Soit $(M_i)_{i\in I}$ une famille de A-modules.*
1) Pour tout A-module M et toute famille $(f_i)_{i\in I}$ d'homomorphismes

$$M \xrightarrow{f_i} M_i$$

il existe un homomorphisme

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

unique tel que pour tout i, $p_i\overline{f} = f_i$.
2) Pour tout A-module M et toute famille $(f_i)_{i\in I}$ d'homomorphismes

$$M_i \xrightarrow{f_i} M$$

il existe un homomorphisme

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

unique tel que pour tout $i \in i$, $\overline{f}\iota_i = f_i$.

On peut montrer (exercice 5.3.6) que la propriété ci-dessus caractérise la donnée du produit et de ses projections $(\prod_{i\in I} M_i, (p_i)_{i\in I})$ à isomorphisme près, et de même pour la somme avec ses injections $(\bigoplus_{i\in I} M_i, (\iota_i)_{i\in I})$.

Définition 3.15 (Suite exacte) *On définit la notion de* suite exacte de modules *dans* ${}_A\mathcal{M}$.

(1) Une suite $M \xrightarrow{f} N \xrightarrow{g} P$ *est exacte si* $ker(g)=im(f)$.

(2) Une suite finie ou infinie (indexée par un intervalle de $\mathbb{Z}$*)*

$$\dots M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \dots$$

est exacte si pour tout i, $ker(f_{i+1}) = im(f_i)$.

(3) Une suite $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ *est exacte si* $ker(f)=0$ *(*f *est injective),* $im(g)=P$ *(*g *est surjective) et* $ker(g)=im(f)$.

Définition 3.16 *Soit* M *un* A*-module et* N *un sous-module de* M*. On dit que* N *est un* facteur direct *de* M *si* N *est non nul et si il existe un autre sous-module* N' *tel que* $M = N + N'$ *et* $N \cap N' = 0$.

Proposition 3.17 *Soit* $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ *une suite exacte. Alors* g *possède une section si et seulement si* f *possède une rétraction si et seulement si* $f(M)$ *est facteur direct de* N*. Dans ce cas,* $N \cong M \oplus P$.

Démonstration. Exercice. Soit s une section de g, alors $N = f(M) \oplus s(P)$ par la représentation $x = (x - s(g(x))) + s(g(x))$.

Définition 3.18 *Une suite exacte du type* $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ *qui satisfait les conditions de la proposition précédente est dite* scindée.

3.2 Modules libres et rang

Définition 3.19 *Un module est dit* libre *si il possède une* base*, c'est-à-dire un ensemble de générateurs linéairement indépendants.*

Les modules libres sont les modules qui ressemblent le plus aux espaces vectoriels.

Exemple 3.20

(1) Si $A = K$ *est un corps alors tout module est libre.*

(2) Considérons $A = \mathbb{Z}$.

(2.1) $\mathbb{Z}$*, comme module sur lui-même, est libre : 1 forme une base.*

(2.2) $\mathbb{Z} \oplus \mathbb{Z}$ *est un module libre :* $(1,0),(0,1)$ *forment une base.*

(2.3) $\mathbb{Z}^{(I)}$ *est un module libre : l'ensemble des* $e_i, i \in I$*, forment une base, où* $e_i = (\delta_{ij})_{j\in I}$ *(*$\delta_{ij} = 1$ *si* $i = j, \delta_{ij} = 0$ *sinon).*

(2.4) $\mathbb{Z}(n)(= \mathbb{Z}/n\mathbb{Z})$ *n'est pas un* $\mathbb{Z}$*-module libre : un élément non nul n'est pas même linéairement indépendant sur* $\mathbb{Z}$*.*

(2.5) $\mathbb{Q}$ *n'est pas un* $\mathbb{Z}$*-module libre : il ne peut être engendré sur* $\mathbb{Z}$ *par un seul élément et n'importe quels deux éléments sont linéairement dépendants sur* $\mathbb{Z}$*.*

(3) $\mathbb{Z}(n)$ *est un module libre comme module sur lui-même : 1 forme une base.*

(4) Si A *est un anneau unitaire, alors pour tout ensemble* I*,* $A^{(I)}$ *est un* A*-module libre : on obtient une base comme ci-dessus en (2.3) ; on l'appelle la base* canonique*.*

Proposition 3.21 *Soit* A *un anneau unitaire et* M *un* A*-module. Alors* M *est un* A*-module libre si et seulement si il existe un ensemble* I *tel que* M *soit isomorphe au* A*-module* $A^{(I)}$*.*

Démonstration. Si M est libre, alors soit B une base de M. On obtient un isomorphisme de M sur $A^{(B)}$ en envoyant un élément b de la base sur e_b, avec la notation de l'exemple 3.20 (2.3), et en prolongeant par linéarité. Si $f : A^{(I)} \to M$ est un isomorphisme de A-modules, alors, toujours avec la notation ci-dessus, $\{f(e_i) : i \in I\}$ donne une base de M. □

Proposition 3.22 *Soit* A *un anneau unitaire. Tout* A*-module est image d'un* A*-module libre par un homomorphisme de* A*-module.*

Démonstration. Soit M un A-module. On obtient un homomorphisme de $A^{(M)}$ sur M en envoyant pour chaque $m \in M$ l'élément e_m de la base canonique sur m même, et en prolongeant par linéarité.□

Proposition 3.23 *Soit* L *un module libre. Alors toute suite exacte de modules du type* $0 \to M \xrightarrow{f} N \xrightarrow{g} L \to 0$ *est scindée.*

Démonstration. Soit $(l_i)_{i\in I}$ une base de L et $(x_i)_{i\in I}$ tel que $g(x_i) = l_i$. Alors la fonction $s : L \to M$ donnée par $s(l_i) = x_i$ et prolongée par linéarité est une section de g. □

Corollaire 3.24 *Dans* $\mathcal{V}_k$ *toute suite exacte du type* $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ *est scindée.*

Que peut-on préserver dans les modules de la théorie de la dimension des espaces vectoriels ? Nous allons d'abord considérer la généralisation directe pour les modules libres : la dimension serait la cardinalité d'une base. Mais pour cela il faudrait que toutes les bases d'un même module libre ait la même cardinalité, ce qui n'est pas toujours le cas avec les bases finies. C'est ce que nous allons un peu élucider.

Proposition 3.25 *Si un module possède un ensemble fini de générateurs alors il ne peut pas posséder de base infinie.*

Démonstration. Soit M un module et $x_1, \ldots, x_n$ un ensemble fini de générateurs de M. Si B était une base infinie de M, alors on aurait $x_1, \ldots, x_n \in <y_1, \ldots, y_m>$ pour certains $y_1, \ldots, y_m$ dans B. Mais alors $M = <y_1, \ldots, y_m>$ et cela contredirait qu'il existe un autre y dans B tel que $y_1, \ldots, y_m, y$ sont linéairement indépendants. □

Proposition 3.26 *Deux bases infinies d'un module possèdent nécessairement la même cardinalité.*

Démonstration. Supposons B, B' deux bases infinies d'un module. Pour chaque $b \in B$ fixons J_b un sous-ensemble fini de B' tel que b appartienne au sous-module engendré par J_b. Notons d'abord que $B' = \bigcup_{b\in B} J_b$, car sinon $\bigcup_{b\in B} J_b$ serait une base strictement incluse dans B' ce qui contredirait que B' est linéairement indépendant. Mais on a aussi que

$$|\bigcup_{b\in B} J_b| \leq |B \times \mathbb{N}| = |B|$$

d'où $|B'| \leq |B|$. De même $|B'| \leq |B|$ et ainsi $|B'| = |B|$. □

Ainsi la notion naturelle de « dimension » est bien définie en général pour les modules libres ayant une base infinie, on l'appellera le « rang ».

Définition 3.27 *Soit M un module libre ayant une base infinie. On définit le* rang *de M comme étant la cardinalité d'une base infinie de M.*

Définition 3.28 *Un module est dit* de type fini*, ou finiment engendré, si il possède au moins un ensemble fini de générateurs.*

L'exercice 5.3.8 donne un exemple d'un module libre de type fini mais avec des bases finies de cardinalité différentes ! Cependant, avec les anneaux commutatifs tout se passe bien.

Proposition 3.29 *Soit A un anneau unitaire commutatif. Alors deux bases finies d'un A-module libre de type fini possède toujours le même nombre d'éléments.*

Démonstration. Soit M un A-module libre de type fini et $B = \{x_1, \ldots, x_n\}$, $B' = \{y_1, \ldots, y_m\}$ deux bases de M. Il faut voir que $n = m$. On passe par les espaces vectoriels sur un corps qui soit un quotient de A. En effet, soit J un idéal maximal propre de A de sorte que A/J est un corps (l'hypothèse que A est commutatif est ici essentielle) et posons

$$JM =< \{ax : a \in J, x \in M\} > .$$

C'est un sous-module de M. Alors M/JM est un espace vectoriel sur A/J de la façon naturelle. On vérifie directement que $x_1 + JM, \ldots, x_n + JM$ et $y_1 + JM, \ldots, y_m + JM$ sont des bases de cet espace vectoriel, d'où on tire que $n = m$. □

3.3 Modules noethériens et modules artiniens

On continue de s'intéresser à transposer aux modules les propriétés des espaces vectoriels de dimension finie.

Définition 3.30 *Un module est dit* noethérien *si il ne possède pas de suite infinie strictement croissante de sous-modules, ou autrement dit si toute suite croissante de sous-modules est stationnaire : si*

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$$

est une suite croissante de sous-modules alors il existe n_0 tel que pour tout $n \geq n_0$, $M_n = M_{n_0}$.

Définition 3.31 *Un module est dit* artinien[2] *si il ne possède pas de suite infinie strictement décroissante de sous-modules, ou autrement dit si toute suite décroissante de sous-modules est stationnaire : si*

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \ldots$$

est une suite décroissante de sous-modules alors il existe n_0 tel que pour tout $n \geq n_0$, $M_n = M_{n_0}$.

[2]Emil Artin, 1898-1962.

Exemple 3.32 *Pour $A = k$ un corps, tout espace vectoriel de dimension finie disons V est noethérien et artinien. En effet, on ne peut augmenter indéfiniment la dimension d'un sous-espace à l'intérieur de V, il est donc noethérien, et on ne peut diminuer indéfiniment non plus la dimension d'un sous-espace à l'intérieur de V, il est donc artinien. En fait on vérifie que dans ce cas, les deux notions coïncident et sont équivalentes à être de dimension finie.*

Exemple 3.33 *Considérons $A = \mathbb{Z}$ et $\mathbb{Z}$ comme module sur lui-même. Alors ${}_{\mathbb{Z}}\mathbb{Z}$ est noethérien. En effet, les sous-modules sont les idéaux de $\mathbb{Z}$ de sorte que si on a une suite d'idéaux*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

alors la réunion $I = \bigcup_n I_n$ est aussi un idéal et donc $I = (d)$ pour un certain entier d. Mais d doit apparaître à un certain moment dans la suite et la suite sera dès lors stationnaire. Par contre, ${}_{\mathbb{Z}}\mathbb{Z}$ n'est pas artinien. En effet, on a au moins la suite infinie strictement décroissante

$$(2) \supset (2^2) \supset (2^3) \supset \dots$$

De même, tout anneau principal en tant que module sur lui-même est un module noethérien mais pas artinien ,à moins d'être un corps.

Exemple 3.34 *Tout groupe abélien fini est un $\mathbb{Z}$-module noethérien et artinien.*

Exemple 3.35 *Pour $A = \mathbb{Z}$, considérons $P = \{\frac{m}{p^k} : m \in \mathbb{Z}, k \geq 0\}$, qui est un sous-groupe additif de $\mathbb{Q}$ et donc un $\mathbb{Z}$-module. On note que $\mathbb{Z}$ est un sous-module de P. En particulier cela entraîne que P n'est pas artinien puisqu'une suite de sous-modules qui témoigne que $\mathbb{Z}$ n'est pas un $\mathbb{Z}$-module artinien témoigne aussi que P ne l'est pas. À cause de la suite*

$$\mathbb{Z} \subset < \frac{1}{p} > \subset < \frac{1}{p^2} > \subset \ \dots$$

on voit que P n'est pas un $\mathbb{Z}$-module noethérien. On vérifie que les sous-modules de cette suite sont les seuls sous-modules de P qui contiennent $\mathbb{Z}$. Cela permet de voir que le quotient $P/\mathbb{Z}$ est un $\mathbb{Z}$-module artinien mais pas noethérien.

On a les propriétés suivantes des modules noethériens et des modules artiniens. On laisse les démonstrations en exercices.

Proposition 3.36 (Propriétés)

(1) Tout sous-module d'un module noethérien est noethérien.

(2) Tout quotient d'un module noethérien est noethérien.

(3) Toute famille non vide de sous-modules d'un module noethérien possède un élément maximal par rapport à l'inclusion.

(4) Tout sous-module d'un module artinien est artinien.

(5) Tout quotient d'un module artinien est artinien.

(6) Toute famille non vide de sous-modules d'un module artinien possède un élément minimal par rapport à l'inclusion.

(7) Un module M est noethérien si et seulement si tout sous-module de M est de type fini.

Théorème 3.37 *(1) Soit N un sous-module d'un module M tel que N et M/N sont noethériens. Alors M est noethérien.*
(2) Soit N un sous-module d'un module M tel que N et M/N sont artiniens alors M est artinien.

Démonstration. (1) Soit

$$P_1 \subseteq P_2 \subseteq P_3 \subseteq \dots$$

une suite croissante de sous-modules de M. Alors on la suite croissante

$$N \cap P_1 \subseteq N \cap P_2 \subseteq N \cap P_3 \subseteq \dots$$

de sous-modules de N et la suite croissante

$$(N + P_1)/N \subseteq (N + P_2)/N \subseteq (N + P_3)/N \subseteq \dots$$

de sous-modules de M/N. Il s'ensuit qu'il existe un entier n_0 tel que pour tout $n \geq n_0$, $N \cap P_n = N \cap P_{n_0}$ et $(N + P_n)/N = (N + P_{n_0})/N$. Vérifions que pour tout $n \geq n_0$, $P_n = P_{n_0}$. Soit $n \geq n_0$. On sait déjà que $P_{n_0} \subseteq P_n$. Par ailleurs soit $x \in P_n$, alors x s'exprime $x = z + y$, où $z \in N$ et $y \in P_{n_0}$, et on a $z = x - y \in N \cap P_n = N \cap P_{n_0}$. D'où $x \in P_{n_0}$. Ainsi $P_n = P_{n_0}$.
(2) Exercice.□

Corollaire 3.38 *Soit $0 \to M \to N \to P \to 0$ une suite exacte de modules. Alors*
(1) N est noethérien si et seulement si M et P sont noethériens.
(2) N est artinien si et seulement si M et P sont artiniens.

Corollaire 3.39 *Soit M un module et N, P des sous-modules de M tel que $M = N + P$. Alors*
(1) Si N et P sont noethériens alors M est noethérien.
(2) Si N et P sont artiniens alors M est artinien.

Démonstration. Il suffit de voir que M/N est noethérien (artinien) dès que N et P le sont. Or on note que $M/N = (N + P)/N \simeq P/N \cap P$. □

Définition 3.40

(1) Un anneau A est dit noethérien (à gauche) *si il est noethérien comme module (à gauche) sur lui-même, autrement dit si le A-module ${}_AA$ est noethérien.*

(2) Un anneau A est dit artinien (à gauche) *si il est artinien comme module (à gauche) sur lui-même, autrement dit si le A-module ${}_AA$ est artinien.*

Théorème 3.41 *(1) Si A est un anneau noethérien alors tout A-module de type fini est noethérien.*
(2) Si A est un anneau artinien alors tout A-module de type fini est artinien.

Démonstration. Par exemple pour (1). Supposons A noethérien et disons $M = Ax_1 + \ldots + Ax_n$. L'application $f : A \to Ax_i$ définie par $f(a) = ax_i$ est un homomorphisme surjectif. Ainsi tous les Ax_i sont noethériens et, par récurrence, on obtient que la somme $Ax_1 + \ldots + Ax_n$ est aussi un module noethérien. □

Il est bon de rappeler le théorème suivant de Hilbert sur les anneaux noethériens commutatifs.

Théorème 3.42 *Soit A un anneau commutatif et $X_1, \ldots, X_n$ un nombre fini d'indéterminées. Si A est un anneau noethérien, alors l'anneau de polynômes $A[X_1, \ldots, X_n]$ est aussi un anneau noethérien.*

En particulier, un corps K étant manifestement un anneau noethérien, un anneau de polynômes $K[X_1, \ldots, X_n]$ sur le corps K est toujours noethérien. Ce qui fait en sorte que tout idéal de $K[X_1, \ldots, X_n]$ est finiment engendré.

3.4 Modules irréductibles, modules indécomposables

On continue de chercher à transposer dans les modules les propriétés des espaces vectoriels de dimension finie. Les propriétés d'être noethérien ou artinien sont déjà deux façons de le faire, mais elles ne disent pas grand chose

sur la structure des modules. On peut chercher à capturer cette structure à partir d'une généralisation de « la dimension 1 », du fait qu'un espace vectoriel de dimension finie est somme directe de sous-espaces de dimension 1. Il y a au moins deux propriétés qui se présentent pour généraliser « la dimension 1 » : n'avoir aucun sous-espace non trivial ou n'avoir aucun facteur direct.

Définition 3.43

(1) Un A-module $M \neq 0$ est dit irréductible *si les seuls sous-modules de M sont 0 et M.*

(2) Un A-module $M \neq 0$ est dit indécomposable *si M ne possède pas de facteur direct non trivial.*

On note qu'un module irréductible est nécessairement indécomposable.

Exemple 3.44

(1) ${}_{\mathbb{Z}}\mathbb{Z}$ n'est pas irréductible mais il est indécomposable. En effet, supposons ${}_{\mathbb{Z}}\mathbb{Z}$ somme directe de deux sous-modules, disons ${}_{\mathbb{Z}}\mathbb{Z} = N_1 \oplus N_2$, et supposons $x_1 \in N_1, x_2 \in N_2$ non nuls. Alors x_1, x_2 devraient être linéairement indépendants sur $\mathbb{Z}$ ce qui serait absurde puisque $x_2 x_1 - x_1 x_2 = 0$.

(2) De même, $\mathbb{Q}$ est un $\mathbb{Z}$-module indécomposable, mais pas irréductible.

(3) $\mathbb{Z}(p)$ est un $\mathbb{Z}$-module irréductible.

(4) $\mathbb{Z}(p^n)$, $n \geq 2$, n'est pas un $\mathbb{Z}$-module irréductible mais il est indécomposable. En effet, ses sous-modules sont tous emboîtés dans la suite suivante :

$$0 \subset < p^{n-1} > \subset < p^{n-2} > \subset \ \ldots \subset < p > \subset \ \mathbb{Z}(p^n)$$

.

(5) Vérifiez que le p-groupe de racines de l'unité $\mu(p^\infty) = \{z \in \mathbb{C} : \exists n \in \mathbb{N}, z^{p^n} = 1\}$ est un $\mathbb{Z}$-module indécomposable.

(6) Soit K un corps, et $n \in \mathbb{N}, n \neq 0$. Alors K^n est un $M_n(K)$-module irréductible (par l'action naturelle).

Proposition 3.45 *(1) Un A-module M est irréductible si et seulement si pour tout $x \in M, x \neq 0$, $M = Ax$.*
(2) Un A-module est irréductible si et seulement si M est isomorphe à un A-module A/J, pour un certain idéal à gauche maximal $J \lhd_g A$.

Démonstration. (2) Si $J \lhd_g A$ est maximal alors A/J est un A-module irréductible car les sous- modules correspondent aux idéaux à gauche contenant J. Réciproquement, si M est irréductible alors $M = Ax$ pour n'importe quel $x \in M$ non nul et on a l'homomorphisme surjectif $f : A \to M$, $f(a) = ax$. Le noyau de f est un idéal à gauche de A et $A/ker(f) \simeq M$, ce qui entraîne que $A/ker(f)$ est un A-module irréductible et donc que $ker(f)$ est maximal. □

Proposition 3.46 (Lemme de Schur) [3] *Soit M, N des A-modules non nuls irréductibles, alors tout homomorphisme de A-modules $M \to N$ est soit nul, soit un isomorphisme. En particulier, l'anneau des endomorphismes de A-modules $End_A(M, \circ, +, id, 0)$ est un corps gauche, c'est-à-dire que tout A-endomorphisme non nul est un isomorphisme.*

Démonstration. Soit $f : M \to N$ un homomorphisme. On a que $ker(f)$ est un sous-module de M et $im(f)$ un sous-module de N. Ainsi soit $ker(f) = 0$ soit $ker(f) = M$. Si $ker(f) = M$ alors f est nul. Si $ker(f) = 0$ alors f est injectif et on doit avoir $im(f) \neq 0$. Mais alors on doit avoir $im(f) = N$ et dans ce cas f est un isomorphisme. □

Le théorème de Krull-Schmidt[4] permet de voir comment les modules à la fois noethériens et artiniens permettent une généralisation de la structure des espaces vectoriels de dimension finie. Nous en verrons la démonstration à la section suivante.

Théorème 3.47 (Théorème de Krull-Schmidt) *Si M est un module artinien et noethérien, alors M est somme directe finie de sous-modules indécomposables. De plus, deux décompositions de ce type ont nécessairement le même nombre de facteurs et, à une permutation près, leurs facteurs sont isomorphes.*

Dans notre analogie avec les espaces vectoriels de dimension finie, le nombre de facteurs indécomposables apparaissant dans la décomposition d'un module artinien et noethérien correspondrait à la « dimension ».

Exemple 3.48 *Dans le cas des $\mathbb{Z}$-modules finis, c'est-à-dire des groupes abéliens finis, qui sont certainement artiniens et noethériens, on sait déjà que tout groupe abélien fini est somme directe de sous-groupes cycliques*

[3] Issaï Schur, 1875-1941.

[4] Wolgang Krull, 1899-1970, Otto Schmidt, 1891-1956.

d'ordre une puisance d'un nombre premier. Or on a vu aussi que les p-groupes finis sont indécomposables. Il s'agit donc de la décomposition qui est assurée par le théorème de Krull-Schmidt.

Dans le théorème de Krull-Schmidt et du point de vue de notre analogie, le rôle des espaces vectoriels de dimension 1 est rempli par les modules indécomposables. Nous allons nous attarder un peu sur un autre aspect, où ce rôle sera davantage joué par les modules irréductibles. Cette discussion sera d'ailleurs utilisée dans la démonstration du théorème de Krull-Schmidt. Considérons la décomposition d'un *espace vectoriel de dimension finie*, disons V en une somme de sous-espaces de dimension 1, disons V_i, comme dans le théorème de Krull-Schmidt :

$$V = V_1 \oplus \ldots \oplus V_k.$$

Notons qu'on obtient une « filtration » de V :

$$V \supset V_2 \oplus \ldots V_k \supset V_3 \oplus \ldots V_k \supset \ldots \supset V_k \supset 0$$

En posant $W_i = V_i \oplus \ldots V_k$, $W_1 = V$ et $W_{k+1} = 0$ on a :

$$V \supset W_2 \supset W_3 \supset \ldots \ W_k \supset 0$$

tel que $W_i/W_{i+1} \simeq V_i$, et les quotients successifs sont donc irréductibles. Ceci entraîne que cette filtration est *maximale* : on ne peut y insérer d'autres termes. Elle est aussi de longueur maximale, ce qui ici coïncide avec la dimension de V. Avec cela en tête, nous allons passer au contexte des modules.

Définition 3.49 *Soit M un A-module.*

(1) Une suite normale *de M est une suite finie décroissante de sous-modules commençant en M et se terminant en 0 :*

$$M_1 = M \supseteq M_2 \supseteq M_3 \supseteq \ldots \ M_n \supseteq M_{n+1} = 0 \tag{3.1}$$

(2) Les quotients *d'une suite normale comme en (3.1) sont les modules quotients M_i/M_{i+1}.*

(3) Une suite normale plus fine *que (3.1) est une suite normale dont (3.1) est une sous-suite. On dit aussi que c'est un* raffinement *de (3.1).*

(4) Deux suites normales sont équivalentes *si elles ont la même longueur et si il existe une permutation des indices tel que les quotients correspondants soient isomorphes.*

Exemple 3.50 *Les deux suites normales suivantes du groupe abélien* $\mathbb{Z}(6)$ *sont équivalentes*

$$\mathbb{Z}(6) \supseteq <2> \supseteq 0$$
$$\mathbb{Z}(6) \supseteq <3> \supseteq 0$$

Définition 3.51 *Une suite normale d'un module* M *qui est strictement décroissante et dont les quotients sont irréductibles est appelée une* suite de composition *de* M.

Théorème 3.52 (Théorème de Jordan-Hölder) [5] *Pour tout module, deux suites de compositions sont toujours équivalentes.*

Théorème 3.53 *Un module non nul possède une suite de composition si et seulement si il est à la fois artinien et noethérien.*

Démonstration. On ne vérifiera pour l'instant que le fait que les modules artiniens et noethériens possèdent une suite de composition. En effet, on construit une suite strictement décroissante de sous-modules avec des quotients irréductibles à l'aide du principe de maximalité noethérien. Cette suite doit stopper en 0 après un nombre fini d'étapes car le module de départ est artinien.□

D'après ces résultats on peut alors parler sans ambiguïté de la *longueur* d'un module artinien et noethérien : c'est la longueur d'une suite de composition. Dans notre analogie avec les espaces vectoriels de dimension finie, la longueur d'un module artinien et noethérien correspondrait à la « dimension ».

Le théorème de Jordan-Hölder se déduit du théorème de Schreier, qui lui-même se déduit du lemme de Zassenhauss.

Théorème 3.54 (Théorème de Schreier) [6] *Deux suites normales d'un module possèdent toujours des raffinements qui sont des suites normales équivalentes.*

Lemme 3.55 (Lemme de Zassenhauss) [7] *Soit* M *un module et* N_1, N_2, K_1, K_2 *des sous-modules de* M *tel que* $K_i \subseteq N_i$. *Alors on a l'isomorphisme*

$$\frac{(N_1 \cap N_2) + K_1}{(N_1 \cap K_2) + K_1} \simeq \frac{(N_1 \cap N_2) + K_2}{(K_1 \cap N_2) + K_2}$$

[5] Camille Jordan, 1838-1922, Otto Hölder, 1859-1937.
[6] Otto Schreier, 1901-1929.
[7] Hans Zassenauss, 1912-1991.

Le théorème de Schreier permet de compléter la démonstration laissée en suspens qu'un module non nul qui possède une suite de composition est artinien et noethérien. En effet, soit M un module non nul ayant une suite de composition. Par exemple pour voir qu'il est noethérien, on considère une suite finie strictement croissante de sous-modules qu'on complète facilement en une suite normale. Par le théorème de Schreier une telle suite et une suite de composition possèdent des raffinements équivalents. Or une suite de composition ne peut pas posséder de raffinement propre. Ainsi le nombre de termes de la suite croissante de départ est au plus celui de la suite de composition. Il ne peut donc y avoir dans M de suite infinie strictement croissante de sous-modules. De façon semblable on vérifie que M est aussi artinien.

Démonstration que le théorème de Schreier entraîne le théorème de Jordan-Hölder. Considérons deux suites de composition d'un même module. On remarque qu'elles ont des quotients non nuls. De plus, des raffinements de ces suites ne peuvent rajouter que des redondances, donc que des quotients nuls. Deux raffinements de ces suites qui sont équivalents auront les mêmes quotients nuls et donc les mêmes quotients non nuls. En comparant avec les suites de départ on obtient qu'elles doivent avoir des quotients isomorphes, à une permutation près. □

Démonstration que le lemme de Zassenhaus entraîne le théorème de Schreier. Soit M un module et deux suites normales de M :

$$M = M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots \ M_s \supseteq M_{s+1} = 0 \tag{3.2}$$

$$M = M'_1 \supseteq M'_2 \supseteq M'_3 \supseteq \dots \ M'_t \supseteq M'_{t+1} = 0 \tag{3.3}$$

Considérons la suite de sous-modules

$$M_1 = (M_1 \cap M'_1) + M_2 \supseteq (M_1 \cap M'_2) + M_2 \supseteq \dots \supseteq (M_1 \cap M'_t) + M_2$$

$$\supseteq M_2 \supseteq (M_2 \cap M'_1) + M_3 \supseteq (M_2 \cap M'_2) + M_3 \supseteq \dots \supseteq (M_2 \cap M'_t) + M_3$$

$$\vdots$$

$$\supseteq M_s \supseteq (M_s \cap M'_1) \supseteq (M_s \cap M'_2) \supseteq \dots \supseteq (M_s \cap M'_t) \supseteq 0$$

En posant $M_{ij} = (M_i \cap M'_j) + M_{i+1}$, on a la suite normale de M

$$M_{11} \supseteq M_{12} \supseteq \dots \supseteq M_{21} \supseteq \dots \supseteq M_{s,t+1} = 0$$

où $M_{i1} = M_i$, qui est un raffinement de la suite normale (3.2) de longueur st. De même, en posant $M'_{ji} = (M'_j \cap M_i) + M'_{j+1}$ on obtient une suite normale de M où $M'_{j1} = M'_j$, qui est un raffinement de la suite normale (3.3) de longueur st. Comparons les facteurs correspondants de ces deux raffinements. On a

$$M_{ij}/M_{i,j+1} = \frac{(M_i \cap M'j) + M_{i+1}}{(M_i \cap M'_{j+1}) + M_{i+1}}$$

et

$$M'_{ji}/M'_{j,i+1} = \frac{(M'_j \cap M_i) + M'_{j+1}}{(M'_j \cap M_{i+1}) + M'_{j+1}}$$

qui sont isomorphes par le lemme de Zassenhauss. □

Démonstration du lemme de Zassenhauss. Il suffit de montrer les deux isomorphismes suivants :

$$\frac{(N_1 \cap N_2) + K_1}{(N_1 \cap K_2) + K_1} \simeq \frac{N_1 \cap N_2}{(N_1 \cap K_2) + (K_1 \cap N_2)}$$

et

$$\frac{(N_1 \cap N_2) + K_2}{(K_1 \cap N_2) + K_2} \simeq \frac{N_1 \cap N_2}{(N_1 \cap K_2) + (K_1 \cap N_2)}$$

Par symétrie il suffit de montrer le premier. Considérons le diagramme suivant d'inclusions :

$$\begin{array}{ccc} & (N_1 \cap N_2) + K_1 & \\ / & & \backslash \\ N_1 \cap N_2 & & (N_1 \cap K_2) + K_1 \\ \backslash & & / \\ & (N_1 \cap K_2) + (K_1 \cap N_2) & \end{array}$$

Notons que (cf. théorème 3.11)

$$\frac{(N_1 \cap N_2) + K_1}{(N_1 \cap K_2) + K_1} \simeq \frac{\frac{(N_1 \cap N_2) + K_1}{K_1}}{\frac{(N_1 \cap K_2) + K_1}{K_1}}$$

Considérons l'application naturelle

$$f : N_1 \cap N_2 \to ((N_1 \cap N_2) + K_1)/K_1$$

$$f(x) = x + K_1$$

On a que

$$\begin{aligned} f((N_1 \cap K_2) + (K_1 \cap N_2)) &= ((N_1 \cap K_2) + (K_1 \cap N_2) + K_1)/K_1 \\ &= ((N_1 \cap K_2) + K_1)/K_1 \end{aligned}$$

D'autre part on a aussi

$$f^{-1}(\,((N_1 \cap K_2) + K_1)\ /K_1\,) = (N_1 \cap K_2) + (K_1 \cap N_2)$$

En effet, l'inclusion $\supseteq$ est directe. Pour l'inclusion $\subseteq$, supposons $x \in N_1 \cap N_2$ tel que $f(x) = x + K_1 = y + K_1$, où $y \in N_1 \cap K_2$. Alors $x = y + z$, pour un certain $z \in K_1$. Ainsi $z = x - y \in K_1 \cap N_2$ et $x \in (N_1 \cap K_2) + (K_1 \cap N_2)$.

Il s'ensuit que $(N_1 \cap K_2) + (K_1 \cap N_2)$ est le noyau de l'homomorphisme surjectif $N_1 \cap N_2 \to (\frac{(N_1 \cap N_2)+K_1}{K_1})/(\frac{(N_1 \cap K_2)+K_1}{K_1})$ obtenu de f en composant avec l'application de passage au quotient. On obtient alors l'isomorphisme suivant :

$$\frac{N_1 \cap N_2}{(N_1 \cap K_2) + (K_1 \cap N_2)} \simeq \frac{\frac{(N_1 \cap N_2)+K_1}{K_1}}{\frac{(N_1 \cap K_2)+K_1}{K_1}}$$

d'où le résultat. □

3.5 Le théorème de Krull-Schmidt

Rappelons l'énoncé du théorème de Krull-Schmidt.

Théorème 3.56 (Krull-Schmidt) *Soit M un module non nul artinien et noethérien. Alors M contient des sous-modules indécomposables $M_i, 1 \leq i \leq n$, tel que*

$$M = M_1 \oplus \ldots \oplus M_n$$

et si on a une autre décomposition

$$M = M_1 \oplus \ldots \oplus M_n = N_1 \oplus \ldots \oplus N_m$$

alors $n = m$ et il existe une bijection $i \rightsquigarrow j$ tel que $M_i \simeq N_j$.

À l'aide des résultats de la section précédente on peut déjà montrer l'existence de la décomposition en somme directe de sous-modules indécomposables.

Démonstration d'une décomposition en somme directe d'indécomposables. Nous allons utiliser la notion de longueur d'un module artinien et noethérien, c'est-à-dire la longueur d'une suite de composition (voir la discussion après le théorème de Jordan-Hölder (3.52)). On désignera la longueur d'un module K par $l(K)$. On note d'abord que si N est un sous-module propre de M alors $l(N) < l(M)$: en effet la suite normale $M \supset N \supseteq 0$ possède un raffinement en une suite de composition de M, qui fournira une suite de composition de N. On peut ainsi utiliser la récurrence sur la longueur. Si M est indécomposable, on a fini. Sinon, $M = M_1 \oplus M_2$, où $M_i \neq 0$. Alors $l(M_i) < l(M)$ et par récurrence il existe des sous-modules indécomposables M_{ij} tel que

$$M_1 = M_{11} \oplus \ldots \oplus M_{1,n_1}$$
$$M_2 = M_{21} \oplus \ldots \oplus M_{2,n_2}$$

Il s'ensuit que

$$M = M_{11} \oplus \ldots \oplus M_{1,n_1} \oplus M_{21} \oplus \ldots \oplus M_{2,n_2}$$

□

L'unicité de la décomposition se démontre en plusieurs étapes et dépend des propiétés des anneaux d'endomorphismes.

Proposition 3.57 *Un module non nul M est indécomposable si et seulement si l'anneau d'endomorphismes $End(M)$ ne contient pas d'idempotent différent de 0 et 1.*

Démonstration. Soit M un module non nul. Si M est somme directe de deux sous-modules propres alors la projection sur chacun des facteurs est un idempotent non trivial de $End(M)$. Réciproquement, si f est un idempotent non trivial de $End(M)$, alors on vérifie que $im(f) \neq 0$ et $im(1-f) \neq 0$, et que $M = im(f) \oplus im(1-f)$. □

Définition 3.58 *Soit M un module et f un endomorphisme de M. On définit les sous-modules*

$$f^{\infty}(M) = \bigcap_{n=1}^{\infty} f^n(M)$$

et

$$f^{-\infty}(0) = \bigcup_{n=1}^{\infty} ker(f^n)$$

Théorème 3.59 (Lemme de Fitting) [8] *Soit M un module non nul artinien et noethérien, et $f \in End(M)$. Alors*

$$M = f^{\infty}(M) \oplus f^{-\infty}(0)$$

De plus, la restriction $f|_{f^{\infty}(M)}$ est un automorphisme et la restriction $f|_{f^{-\infty}(0)}$ est nilpotente.

Démonstration. Comme M est artinien il existe un entier s tel que $f^s(M) = f^{s+1}(M) = \ldots = f^{\infty}(M)$, et comme il est noethérien il existe un entier r tel que $ker(f^t) = ker(f^{t+1}) = \ldots = f^{-\infty}(0)$. Soit $r = \max(s,t)$, de sorte que $f^{\infty}(M) = f^r(M)$ et $f^{-\infty}(0) = ker(f^r)$. Voyons que $f^{\infty}(M) \cap f^{-\infty}(0) = 0$. Soit $z \in f^{\infty}(M) \cap f^{-\infty}(0)$, alors $z = f^r(y)$ pour un $y \in M$. Mais $f^r(z) = 0$, donc $f^{2r}(y) = 0$ et $y \in ker(f^{2r}) = ker(f^r)$. Ainsi $z = 0$. Voyons que $M = f^{\infty}(M) + f^{-\infty}(0)$. Soit $x \in M$. Comme $f^r(M) = f^{2r}(M)$, on a $f^r(x) = f^{2r}(y)$ pour un certain $y \in M$, et ainsi $x - f^r(y) \in ker(f^r) = f^{-\infty}(0)$. On a donc $x = f^r(y) + (x - f^r(y))$, où $f^r(y) \in f^{\infty}(M)$ et $x - f^r(y) \in f^{-\infty}(0)$. La restriction de f à $f^{-\infty}(0)$ est nilpotente car $f^{-\infty}(0) = ker(f^r)$. La restriction de f à $f^{\infty}(M)$ est surjective car $f^{\infty}(M) = f^r(M) = f^{r+1}(M)$. Elle est aussi injective car $f^{\infty}(M) \cap f^{-\infty}(0) = 0$ entraîne aussi $f^{\infty}(M) \cap ker(f) = 0$. □

Corollaire 3.60 *Si M est un module indécomposable artinien et noethérien alors tout endomorphisme $f \in End(M)$ est soit nilpotent, soit un automorphisme de M.*

Définition 3.61 *Un anneau est dit* local *si l'ensemble de ses éléments non inversibles forme un idéal bilatère.*

Exemple 3.62

(1) Fixons un nombre premier p. On vérifie que

$$\mathbb{Z}_{(p)} = \{\frac{m}{n} : m, n \in \mathbb{Z}, p \not| n\}$$

est un sous-anneau de $\mathbb{Q}$ qui est un anneau local.

[8] Hans Fitting, 1906-1938.

(2) *Soit $\mathcal{C}(\mathbb{R})$ l'anneau des fonctions continues réelles. Alors $J = \{f : f$ s'annule sur un voisinage de $0\}$ est un idéal et le quotient $\mathcal{C}(\mathbb{R})/J$ est un anneau local.*

(3) *Un anneau dont tout élément non nul est soit nilpotent, soit inversible, est un anneau local (voir la preuve du lemme 3.65).*

Définition 3.63 *Un module M est dit* fortement indécomposable *si $End(M)$ est un anneau local.*

Lemme 3.64 *Un module fortement indécomposable est indécomposable.*

Démonstration. Un anneau local a la propriété suivante : pour tout x, x ou $1-x$ est inversible. Si e est un idempotent alors on a $e(1-e) = 0$, d'où soit $1-e = 0$, soit $e = 0$. Un anneau local ne peut donc posséder d'idempotent non trivial. □

Lemme 3.65 *Un module indécomposable artinien et noethérien est fortement indécomposable.*

Démonstration. Soit M un module indécomposable artinien et noethérien. Il s'agit de voir que l'ensemble J des endomorphismes de M qui ne sont pas des automorphismes est un idéal. Soit $f \in J$. Par le lemme de Fitting f est nilpotent, donc f ne peut être ni injectif ni surjectif. Donc pour pour tout $g \in End(M)$, gf ne peut être injectif et fg ne peut être surjectif, et ils appartiennent à J. D'autre part, soit $f_1, f_2 \in J$ et supposons $f_1 + f_2 \notin J$. Alors $f_1 + f_2$ est inversible. Posons $h_i = f_i(f_1 + f_2)^{-1} \in J$, de sorte que $h_1 + h_2 = 1$. Or h_2 est nilpotent, disons $h_2^n = 0$, d'où $(1-h_2)(1 + h_2 + \ldots + h_2^{n-1}) = 1 = (1 + h_2 + \ldots + h_2^{n-1})(1-h_2)$. Cela est absurde puisque $1 - h_2 = h_1 \in J$ n'est pas inversible. Donc J est bien un idéal. □

L'unicité de la décomposition dans le théorème de Krull-Schmidt découle alors du théorème suivant.

Théorème 3.66 *Soit des modules M, N avec des décompositions*

$$M = M_1 \oplus \ldots \oplus M_n$$

$$N = N_1 \oplus \ldots \oplus N_m$$

tel que les M_i sont fortement indécomposables et les N_j indécomposables, et supposons que $M \simeq N$. Alors $m = n$ et il existe une permutation $i \rightsquigarrow i'$ tel que $M_i \simeq N_{i'}$.

Lemme 3.67 *Soit M,N des modules tel que M est non nul et N indécomposable. Soit des homomorphismes $M \xrightarrow{f} N \xrightarrow{g} M$ tel que gf est un automorphisme de M. Alors f et g sont des isomorphismes.*

Démonstration. Soit s l'inverse de gf et posons $t = sg$ ($N \xrightarrow{t} M$) et $e = ft$. Alors on a $tf = 1_M$ et $e^2 = ftft = f\,1_M t = ft = e$. Comme N est indécomposable on doit avoir $e = 1$ ou $e = 0$. Or $e = 0$ entraînerait $1_M = 1_M^2 = tftf = tef = 0$, ce qui n'est pas le cas puisque $M \neq 0$. Ainsi $ft = 1_N$. Donc f est un isomorphisme et $g = s^{-1}f^{-1}$ aussi. □

Démonstration du théorème 3.66 On utilise la récurrence sur le nombre n de facteurs fortement indécomposables de M. C'est direct pour $n = 1$, on considère donc $n > 1$. Soit $M \xrightarrow{g} N$ un isomorphisme, e_i les projections sur les facteurs M_i de M, et f_j les projections sur les facteurs N_j de N. On procède en trois étapes.

(1) *On peut supposer que $M_1 \xrightarrow{f_1 g e_1|_{M_1}} N_1$ et $N_1 \xrightarrow{e_1 g^{-1} f_1|_{N_1}} M_1$ sont des isomorphismes.*
En effet, posons

$$h_j = f_j g e_1, \quad k_j = e_1 g^{-1} f_j, \quad 1 \leq j \leq m$$

On a $\sum_1^m k_j h_j = \sum_1^m e_1 g^{-1} f_j g e_1 = e_1 g^{-1} \sum f_j g e_1 = e_1 g^{-1}\, 1_N g e_1 = e_1$. Puisque $e_1(M_1) = M_1$ et $k_j h_j(M_1) \subseteq M_1$, on peut considérer les restrictions $e_1' = e_1|_{M_1}$ et $(k_j h_j)' = (k_j h_j)|_{M_1}$ comme des endomorphismes de M_1. Comme ${e_1}^2 = e_1$ on a en fait $e_1' = 1_{M_1}$. Ainsi on a $\sum (k_j h_j)' = 1_{M_1}$. Puisque $End(M_1)$ est local l'un des $(k_j h_j)'$ est inversible, c'est-à-dire un automorphisme de M_1. Sans perte de généralité on peut supposer $j = 1$. Posons $h_1' = h_1|_{M_1}$ et $k_1' = k_1|_{N_1}$ de sorte qu'on a les homomorphismes $M_1 \xrightarrow{h_1'} N_1 \xrightarrow{k_1'} M_1$ et $k_1' h_1' = (k_1 h_1)'$. On conclut par le lemme que h_1' et k_1' sont des isomorphismes, tel que voulu.

(2) *On a $M = g^{-1}(N_1) \oplus (M_2 \ldots \oplus M_n)$.*
En effet, vérifions d'abord que $g^{-1}(N_1) \cap (M_2 \oplus \ldots \oplus M_n) = 0$. Soit $x \in g^{-1}(N_1) \cap (M_2 \oplus \ldots \oplus M_n)$, disons $x = g^{-1}(y)$, $y \in N_1$. On a $e_1(x) = 0$, de sorte que $k_1'(y) = k_1(y) = e_1 g^{-1} f_1(y) = e_1 g^{-1}(y) = 0$. D'où $y = 0$ car $e_1 g^{-1} f_1$ est un isomorphisme d'après (1), et $x = 0$. Vérifions ensuite que $M = g^{-1}(N_1) + M_2 + \ldots M_n$. Notons que si $x \in g^{-1}(N_1)$ alors $x, e_2(x), \ldots, e_n(x) \in g^{-1}(N_1) + M_2 + \ldots M_n$, de sorte que $e_1(x) \in g^{-1}(N_1) + M_2 + \ldots M_n$ car $e_1(x) = x - e_2(x) - \ldots - e_n(x)$. Ainsi $e_1 g^{-1}(N_1) \subseteq g^{-1}(N_1) + M_2 + \ldots M_n$.

Or $e_1 g^{-1}(N_1) = e_1 g^{-1} f_1(N_1) = M_1$ d'après (1), ce qui permet de conclure.

(3) On peut maintenant terminer à l'aide de la récurrence. En effet, puisque $g(g^{-1}(N_1)) = N_1$, g induit un isomorphisme $M/g^{-1}(N_1) \to N/N_1$. Mais alors par (2) on a $M/g^{-1}(N_1) \simeq M_2 \oplus \ldots \oplus M_n$. Puisque $N/N_1 \simeq N_2 \oplus \ldots \oplus N_m$, on obtient un isomorphisme $M_2 \oplus \ldots \oplus M_n \simeq N_2 \oplus \ldots \oplus N_m$ et on peut appliquer la récurrence. □

Chapitre 4

Polynômes et corps

Dans ce chapitre nous abordons trois problèmes classiques de la théorie des corps : la notion algébrique de dimension pour les variétés algébriques affines, l'existence d'équations polynomiales non résolubles par radicaux, et le dix-septième problème de Hilbert sur la représentation en somme de carrés d'une fonction rationnelle positive.

4.1 Rappel de théorie des corps

On vérifie que pour un corps K et une famille de sous-corps $(K_i)_{i\in I}$ de K, $\cap_{i\in I}K_i$ est un sous-corps de K (exercice 5.4.1). Ceci assure que si S est une partie d'un corps K, alors il y a un plus petit sous-corps de K qui contienne S. On l'appelle le *sous-corps engendré* par S. En particulier si K_0 est un sous-corps de K, on notera $K_0(S)$ le sous-corps de K engendré par $K_0 \cup S$. Si $S = \{s_1, \ldots, s_n\}$ on utilisera aussi la notation $K(s_1, \ldots, s_n)$. Soit K_1 un corps et K un sous-corps de K_1, on vérifie que si S une partie de K alors $K(S)$ coïncide avec le corps des fractions de $K[S]$, c'est-à-dire que

$$K(S) = \{\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} : n \geq 1, x_i \in S, f, g \in K[X_1, \ldots, X_n], g(x_1, \ldots, x_n) \neq 0\}$$

et que pour S, S' des parties de K_1, $K(S \cup S') = (K(S))(S') = (K(S'))(S)$ (exercice 5.4.2).

Soit K et L des corps tels que $K \subseteq L$. En particulier on peut voir L comme un espace vectoriel sur K. On note L/K cette structure de module et on parle de l'*extension* L/K. Par abus de langage on parlera aussi d'une extension lorsque K est plongé dans L, en identifiant K avec son image dans L. Le *degré de l'extension* L/K, noté $[L : K]$, est la dimension de L comme

espace vectoriel sur K. On dit qu'on a une *extension finie* si elle est de degré fini. On utilise souvent la notation schématique suivante pour représenter une extension de corps.

$$\begin{array}{c} L \\ | \\ K \end{array}$$

Soit L/K et L'/K deux extensions du corps K. Un homomorphisme de corps $f : L \to L'$ est appelé un $K-$*homomorphisme* si $f(k) = k$ pour tout $k \in K$, ou autrement dit si c'est aussi un homomorphisme de K-modules.

Exemple 4.1

1) $\mathbb{C}/\mathbb{R}$ *est une extension finie de degré deux.*

2) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *est une extension finie de degré deux.*

3) $\mathbb{R}/\mathbb{Q}$ *est une extension de degré infini.*

4) Soit X *une indéterminée, alors* $\mathbb{Q}(X)/\mathbb{Q}$ *est une extension de degré infini. Pouvez-vous en trouver une base ?*

Proposition 4.2 *Soit* K,K' *et* L *des corps tels que* $K \subseteq K' \subseteq L$. *Alors* L/K *est une extension finie si et seulement si* L/K' *et* K'/K *sont des extensions finies, et alors* $[L : K] = [L : K'][K' : K]$.

Démonstration. Supposons que L/K' et K'/K soient des extensions finies. Soit $x_1, \ldots, x_n$ une base de K' sur K et $y_1, \ldots, y_m$ une base de L sur K'. Alors $x_1y_1, x_1y_2, \ldots, x_1y_m, \ldots, x_ny_m$ forment une base de L sur K. En effet, c'est un ensemble de générateurs puisque pour $a \in L$, $a = \sum k'_j y_j$, pour certains $k'_j \in K'$, et $k'_j = \sum k_{ij}x_i$ pour certains $k_{ij} \in K$, d'où $a = \sum k_{ij}x_iy_j$. C'est un ensemble linéaiement indépendant sur K puisque si $\sum k_{ij}x_iy_j = 0$, pour cerains $k_{ij} \in K$, alors pour tout j, $\sum_i k_{ij}x_i = 0$ car les y_j sont linéairement indépendants sur K', d'où pour tout i, j, $k_{ij} = 0$ car les x_i sont linéairement indépendants sur K. Supposons maintenant que L/K soit une extension finie. L'argument précédent montre que si $x_1, \ldots, x_n \in K'$ sont linéairement indépendants sur K et $y_1, \ldots, y_m \in L$ sont linéairement indépendants sur K', alors les x_iy_j, $1 \leq i \leq n, 1 \leq j \leq m$, sont linéairement indépendants sur K ; d'où le résultat. □

Corollaire 4.3 *Si* $[L : K]$ *est un nombre premier alors il n'y a pas de corps strictement compris entre* K *et* L.

Exemple 4.4 *Puisque* $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, *il n'y a pas de corps intermédiaire entre* $\mathbb{Q}$ *et* $\mathbb{Q}(\sqrt{2})$.

Dans une extension de corps L/K, on dit que x est *algébrique* sur K si il existe un polynôme $f \in K[X]$, non nul, tel que $f(x) = 0$. On dit que x est *transcendant* sur K sinon. Soit le K-homomorphisme $K[X] \stackrel{év_x}{\to} L$ d'évaluation en x, de sorte que $ker(év_x) = \{f \in K[X] : f(x) = 0\}$. On peut donc remarquer que x est algébrique sur L si et seulement si $ker(év_x) \neq 0$, et x est transcendant sur L si et seulement si $ker(év_x) = 0$.

Proposition 4.5 *Soit $K, L, x \in L$ comme ci-dessus. Alors x est transcendant sur L si et seulement si il existe un K-isomorphisme de $K(x)$ sur le corps des fonctions rationnelles $K(X)$, qui envoie x sur X .*

Soit L/K une extension et supposons $x \in L$ algébrique sur K. Soit $ker(év_x) = (f_0)$. En prenant f_0 unitaire, il est uniquement déterminé comme générateur de $ker(év_x)$. On l'appelle le *polynôme minimal* de x sur K. C'est le polynôme unitaire de plus petit degré qui s'annule en x. On vérifie que le polynôme minimal de x sur K est caractérisé par les propriétés suivantes : il est irréductible sur K, unitaire et x en est une racine.

Proposition 4.6 *Soit L/K une extension de corps, $x \in L$ algébrique sur K, f_0 le polynôme minimal de x sur K et n le degré de f_0. Alors $[K(x) : K] = n$, $K(x) = K[x] \simeq K[X]/(f_0)$, et $1, x, x^2, \ldots, x^{n-1}$ est une base linéaire de $K(x)$ sur K.*

Démonstration. Soit $f_0(X) = X^n + a_1X^{n-1} + \ldots + a^n$. Alors $1, x, x^2, \ldots, x^{n-1}$ sont linéairement indépendants sur K. En effet, une relation de dépendance linéaire non triviale sur K donnerait un polynôme sur K de degré plus petit que n dont x serait une racine, ce qui est absurde. Notons d'autre part que $x^n = -a_1x^{n-1} - \ldots - a_n$, $x^{n+1} = -a_1x_n - a_2x^{n-1} - \ldots - a_nx = b_1x^{n-1} + \ldots + b_n$, $x^{n+2} = b_1x^n + \ldots + b_nx$ etc. De sorte que pour tout j, x^j est une combinaison linéaire sur K de $1, x, x^2, \ldots, x^{n-1}$, et on a $K[x] =< 1, x, x^2, \ldots, x^{n-1} >_K$. Or $K[x]$ est un corps puisque f_0 est irréductible sur K et qu'on a l'isomorphisme $K[X]/(f_0) \simeq K[x]$. □

Corollaire 4.7 *Soit x_1, x_2 des éléments (dans des extensions de K) qui sont algébriques sur K et qui possèdent le même polynôme minimal sur K. Alors $K(x_1)$ et $K(x_2)$ sont K-isomorphes par un isomorphisme qui envoie x_1 sur x_2.*

Démonstration. En effet, chacune de ces extensions de K est K-isomorphe à $K[X]/(f_0)$, où f_0 est le polynôme minimal de x_1 et x_2. □

Une *extension algébrique* L/K est une extension où tous les éléments de L sont algébriques sur K. Dans le cas contraire, on dit qu'on a une *extension transcendante*.

Exemple 4.8

1) $\mathbb{C}/\mathbb{R}$ *est une extension algébrique.*

2) $\mathbb{R}/\mathbb{Q}$ *est une extension transcendante.*

3) $\mathbb{C}/\mathbb{Q}$ *est une extension transcendante.*

4) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *est une extension algébrique.*

Proposition 4.9 *Soit K un corps et x un élément dans une extension de K. Alors x est algébrique sur K si et seulement si $K(x)/K$ est une extension finie.*

Démonstration. Nous avons déjà vu que si x est algébrique sur K l'extension $K(x)/K$ est finie de degré égal au degré du polynôme minimal de x sur K. D'autre part, si $K(x)/K$ est une extension finie alors $1, x, x^2, x^3, \ldots$ ne sont pas linéairement indépendants sur K. Il existe donc un entier n et des $\lambda_i \in K$ tels que $\lambda_n \neq 0$ et $\lambda_n x^n + \lambda_{n-1} x^{n-1} + \ldots + \lambda_0 = 0$. □

Corollaire 4.10 *Toute extension finie est algébrique.*

N.B. Attention, la réciproque n'est pas vraie. Nous verrons dans quelques instants une extension algébrique qui n'est pas finie.

Proposition 4.11 *Soit L/K une extension et $x, y \in L$ algébriques sur K. Alors $x+y, x-y, xy, xy^{-1}$ sont algébriques sur K.*

Démonstration. Puisque x est algébrique sur K, $K(x)/K$ est une extension finie. Puisque y est algébrique sur K, il l'est aussi sur $K(x)$. Donc $K(x,y)/K$ est une extension finie puisqu'elle est obtenue par deux extensions finies successives. Il suffit alors de constater, par exemple, que $K(x+y)$ est contenu dans $K(x,y)$ et d'appliquer la proposition précédente. □

Corollaire 4.12 *Soit L/K une extension et $S \subseteq L$ tel que tous les éléments de S sont algébriques sur K. Alors $K(S)/K$ est une extension algébrique.*

Exemple 4.13 *Soit S l'ensemble de tous les nombres complexes qui sont algébriques sur $\mathbb{Q}$ et posons $\tilde{\mathbb{Q}} = \mathbb{Q}(S)$. C'est un sous-corps de $\mathbb{C}$ qui contient $\mathbb{Q}$ et l'extension $\tilde{\mathbb{Q}}/\mathbb{Q}$ est algébrique. Mais ce n'est par contre pas une extension finie. En effet, les polynômes $X^n - 2$ sont tous irréductibles sur $\mathbb{Q}$,*

ce sont donc les polynômes minimaux des $\sqrt[n]{2}$ *et on a* $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. *L'extension* $\tilde{\mathbb{Q}}/\mathbb{Q}$ *contient donc des sous-extensions de degré arbitrairement grand et ne peut donc pas être finie.*

On s'intéressera aux racines de polynômes sur un corps. On a le résultat suivant.

Proposition 4.14 *Soit* K *un corps et* $f \in K[X]$, $f \neq 0$. *Alors il existe une extension de* K *où* f *possède au moins une racine.*

Démonstration. Décomposons f en facteurs irréductibles sur K. En remplaçant f par un de ses facteurs irréductibles, on peut supposer f lui-même irréductible. Mais alors l'idéal (f) de $K[X]$ est maximal et le quotient $K[X]/(f)$, qui est un corps et peut être vu de façon naturelle comme une extension de K, est une extension de K où f possède une racine, à savoir $X + (f)$. □

En appliquant la proposition précédente un nombre suffisant de fois on obtient le corollaire suivant.

Corollaire 4.15 *Il existe une extension de* K *où* f *se factorise en facteurs linéaires.*

4.2 Corps algébriquement clos

Les corps algébriquement clos de caractéristique zéro sont ceux qui ont « essentiellement »les mêmes propriétés algébriques que les nombres complexes.

Définition 4.16 *Un corps* K *est dit* algébriquement clos *si tout polynôme* $f \in K[X]$ *non constant possède au moins une racine dans* K.

On vérifie (exercice 5.4.3) que chacune des propriétés suivantes est équivalente à ce que le corps K soit algébriquement clos.

(1) Tout polynôme non constant $f \in K[X]$ se décompose en facteurs linéaires.

(2) Les seuls polynômes irréductibles de $K[X]$ sont les polynômes linéaires.

(3) Il n'y a pas d'extension algébrique propre de K, ou autrement dit la seule extension algébrique de K est K lui-même.

Exemple 4.17

(1) Le corps des nombres complexes, $\mathbb{C}$, est algébriquement clos.

(2) Le corps $\tilde{\mathbb{Q}}$ est algébriquement clos. En effet, soit $f(X) = a_nX^n + \ldots + a_0$ un polynôme de degré n sur $\tilde{\mathbb{Q}}$. Ce polynôme possède une racine dans $\mathbb{C}$, disons z. Mais alors z appartient à $\mathbb{Q}(a_0, \ldots, a_n, z)$ qui est une extension finie de $\mathbb{Q}$ (pourquoi ?). Ainsi z est algébrique sur $\mathbb{Q}$. C'est donc un élément de $\tilde{\mathbb{Q}}$, et il est racine de f.

Proposition 4.18 *Soit K et L des corps tels que $K \subseteq L$ et L est algébriquement clos. Soit K^* l'ensemble des éléments de L qui sont algébriques sur K. Alors K^* est un sous-corps de L, c'est un corps algébriquement clos, et K^*/K est une extension algébrique.*

Définition 4.19 *Soit K un corps et K^*/K une extension de K tel que K^* soit algébriquement clos et K^*/K une extension algébrique. On dit alors que K^* est une* clôture algébrique *de K.*

Exemple 4.20 *Le corps $\tilde{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$.*

Théorème 4.21 (Steinitz) [1] *(1) Tout corps possède une clôture algébrique. (2) Soit K_1^* et K_2^* deux clôtures algébriques d'un corps K, alors K_1^* et K_2^* sont K-isomorphes. (3) Soient K_1 et K_2 deux corps isomorphes par un isomorphisme $K_1 \xrightarrow{\varphi} K_2$, et soient K_1^* et K_2^* des clôtures algébriques de K_1 et K_2. Alors K_1^* et K_2^* sont isomorphes par un isomorphisme $K_1^* \xrightarrow{\psi} K_2^*$ qui prolonge φ.*

Nous ne vérifions que les points (1) et (2) ; (3) s'obtient avec des ajustements mineurs. Pour l'existence, il suffit par la proposition 4.18 de plonger le corps de départ dans un corps algébriquement clos. Il suffit en fait de pouvoir plonger tout corps dans un corps où tous les polynômes sur le corps de départ ont au moins une racine. En effet, soit K un corps. Supposons qu'il y ait une extension K_1 de K telle que tout polynôme $f \in K[X]$ ait au moins une racine dans K_1. En itérant ce procédé on obtiendrait une extension K_2 de K_1 telle que tout polynôme $f \in K_1[X]$ ait au moins une racine dans K_2, et ainsi de suite, c'est-à-dire qu'on obtiendrait une suite croissante de corps

$$K \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \ldots \subseteq K_n \subseteq \ldots$$

[1] Ernst Steinitz, 1871-1928.

telle que pour tout n, tout polynôme $f \in K_n[X]$ possède au moins une racine dans K_{n+1}. Alors $K_\infty = \bigcup_{n=1}^{\infty} K_n$ est un corps algébriquement clos qui contient le corps de départ K.

Rappelons que si on fixe un polynôme $f \in K[X]$, on sait déjà trouver une extension de K où f possède une racine (proposition 4.14). Il n'est pas difficile de voir qu'on peut faire la même chose avec un nombre fini de polynômes. Il suffit de répéter le procédé autant de fois qu'il faut pour traiter chaque polynôme. La difficulté est donc de traiter tous les polynômes à la fois. Si le corps de départ est dénombrable, alors l'anneau $K[X]$ est aussi dénombrable et on peut énumérer les polynômes sur K en une suite $f_0, f_1, f_2, \ldots$. On peut alors raisonner de façon analogue au paragraphe précédent et obtenir une suite $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$ de corps telle que f_n possède une racine dans K_{n+1}. Alors la réunion $\bigcup_{n=1}^{\infty} K_n$ est une extension de K où tous les polynômes sur K ont une racine. En général, on peut utiliser un bon ordre sur $K[X]$ et imiter la construction par récurrence précédente. Nous allons procéder autrement.

Lemme 4.22 *Soit K un corps. Alors K possède une extension où tous les polynômes sur K ont au moins une racine.*

Démonstration. Pour chaque polynôme $f \in K[X]$, soit X_f une nouvelle indéterminée. Soit A l'anneau des polynômes sur K en ces indéterminées, qu'on pourrait noter $K[\{X_f : f \in K[X]\}]$. Soit I l'idéal de A engendré par les $f(X_f)$. Cet idéal est propre, c'est-à-dire que $1 \notin I$. En effet, sinon on aurait une relation $\sum_1^n h_i f_i(X_{f_i}) = 1$, où $h_i \in A$. Or on a déjà remarqué qu'il y a une extension de K, disons K_1, où les polynômes $f_1, \ldots, f_n$ ont chacun une racine, disons $r_i \in K_1$ tel que $f_i(r_i) = 0$. On obtient un K-homorphisme $A \xrightarrow{\varphi} K_1$ en envoyant X_{f_i} sur r_i et les autres X_f n'importe où. Mais alors on aurait $1 = \sum \varphi(h_i)\varphi(f_i(X_{f_i})) = \sum \varphi(h_i) f_i(r_i) = 0$, ce qui est absurde. Ainsi, l'idéal I est contenu dans un idéal maximal propre, disons M. Mais alors le quotient A/M est un corps qui est une extension de K et où chaque polynôme $f \in K[X]$ possède une racine, à savoir $X_f + M$. □

Nous avons maintenant établi l'existence de la clôture algébrique.

Pour l'unicité de la clôture algébrique, nous utiliserons le lemme de Zorn, « l'étape d'induction »résidant dans le corollaire 4.7. En effet, soit K un corps et considérons K_1^* et K_2^* deux clôtures algébriques de K. Considérons l'ensemble suivant

$$\mathcal{F} = \begin{array}{c} \{(L, g) : L \text{ est un sous-corps de } K_1^* \text{ contenant } K, \\ L \xrightarrow{g} K_2^* \text{ est un } K\text{-homomorphisme}\} \end{array}$$

On vérifie que la relation suivante définit un ordre partiel sur $\mathcal{F}$: $(L_1, g_1) \leq (L_2, g_2)$ ssi $L_1 \subseteq L_2$ et $g_2|_{L_1} = g_1$. On a que $(\mathcal{F}, \leq)$ est un ensemble inductif. En effet $\mathcal{F}$ est non vide car on peut toujours prendre $L = K$ et g =l'inclusion. On laisse en exercice de vérifier la condition sur les chaînes. Ainsi on peut appliquer le lemme de Zorn à $(\mathcal{F}, \leq)$ et obtenir un élément maximal, disons (L_0, g_0). Alors on doit avoir $L_0 = K_1^*$. Sinon, soit $x_1 \in K_1^* \setminus Z_0$, $f_1(X) = \sum a_i X^i$ le polynôme minimal de x_1 sur L_0, et $f_2(X) = \sum g_0(a_i)X^i$ son image par g_0. . Puisque K_2^* est algébriquement clos et contient K, f_2 possède une racine $x_2 \in K_2^*$. Mais f_2 est aussi irréductible sur $g_0(L_0)$ et donc est le polynôme minimal de x_2 sur $g_0(L_0)$. Par un calcul analogue au corollaire 4.7 on obtient un isomorphisme $L_0(x_1) \xrightarrow{g} g_0(L_0)(x_2)$ qui prolonge g_0, de sorte que $(L_0(x_1), g) \in \mathcal{F}$ et $(L_0, g_0) < (L_0(x_1), g)$ ce qui contredit la maximalité de (L_0, g_0). Ainsi $L_0 = K_1^*$. Or on doit aussi avoir que l'image de g_0 est K_2^* tout entier. En effet, $g_0(K_1^*)$ est aussi un corps algébriquement clos et l'extension $K_2^*/g_0(K_1^*)$ est algébrique, d'où l'égalité voulue. Cela complète la démonstration du théorème de Steinitz.

L'unicité de la clôture algébrique découle aussi du résultat suivant, plus fort, mais qui demande aussi plus de travail.

Théorème 4.23 (Lemme de Ax) *(1) Soit K un corps et L_1, L_2 deux extensions algébriques de K telles que tout polynôme $f \in K[X]$ a une racine dans L_1 exactement quand il en a une dans L_2 et vice versa, alors L_1 et L_2 sont K-isomorphes. (2) Soient K_1 et K_2 deux corps isomorphes par un isomorphisme $K_1 \xrightarrow{\varphi} K_2$, et soient L_1, L_2 des extensions algébriques de K_1 et K_2 telles que tout polynôme $f \in K_1[X]$ a une racine dans L_1 exactement quand son image $\varphi(f) \in K_2[X]$ en a une dans L_2 et vice versa, alors L_1 et L_2 sont isomorphes par un isomorphisme $L_1 \xrightarrow{\psi} L_2$ qui prolonge φ.*

On voit que l'unicité de la clôture algébrique est le cas particulier du lemme de Ax où les polynômes ont *toujours* une racine.

Nous utiliserons le lemme de Ax comme outil dans la solution du dix-septième problème de Hilbert.

Du lemme de Ax nous n'allons donner qu'un exposé succinct de la démonstration de (1), qui permettra d'illustrer les méthodes topologiques en algèbre. Nous avons besoin d'un peu plus de théorie des corps. Pour les résultats énoncés sans démonstration nous renvoyons à [8].

Définition 4.24 *Soit K un corps et $f \in K[X]$. Un* corps de rupture*, ou corps de décomposition, de f est une extension de K où f se factorise en facteurs linéaires et qui est engendrée par les racines de f. Autrement dit*

c'est une extension L/K où il existe $a_i \in L$ tels que $f(X) = (X-a_1)\dots(X-a_n)$ et $L = K(a_1, \dots, a_n)$.

On a que tout polynôme possède au moins un corps de rupture : il suffit d'aller à une extension où le polynôme donné se décompose en facteurs linéaires grâce au corollaire 4.15, et de prendre alors la sous-extension engendrée par les racines qui donnent la décomposition . On a l'unicité du corps de rupture, à K-isomorphisme près.

Proposition 4.25 *Soit K et K' deux corps isomorphes par un isomorphisme $K \xrightarrow{\varphi} K'$. Soit $f \in K[X]$ et soit $f^\varphi \in K'[X]$ le polynôme obtenu de f en appliquant φ aux coefficients de f. Soit L un corps de rupture de f et L' un corps de rupture de f^φ. Alors L et L' sont isomorphes par un isomorphisme $L \xrightarrow{\psi} L'$ qui prolonge φ.*

Démonstration. On utilise le corollaire 4.7 comme pour l'unicité de la clôture algébrique, mais en remplaçant le lemme de Zorn par la récurrence sur le degré de f. □

On obtient l'unicité du corps de rupture à isomorphisme près en prenant $K = K'$ et φ =l'identité. Soit K un corps et $f \in K[X]$. On dit que f est *séparable sur K* si f n'a que des racines simples dans un corps de rupture. Soit L/K une extension et $x \in L$ un élément algébrique sur K. On dit que x est *séparable* sur K si le polynôme minimal de x sur K est séparable sur K. Une extension algébrique est dite *extension séparable* si tous les éléments sont séparables. Cette notion prend tout son sens dans les corps de caractéristique non nulle. En effet, on vérifie (exercice 5.4.4) qu'en caractéristique zéro toute extension algébrique est séparable.

Exemple 4.26 *Soit $\mathbb{F}_p(X)$ le corps des fonctions rationnelles sur le corps à p éléments $\mathbb{F}_p$. Soit l'extension $\mathbb{F}_p(\alpha)/\mathbb{F}_p(X)$, où $\alpha^p = X$. Le polynôme minimal de α est $Y^p - X$, mais on a $Y^p - X = Y^p - \alpha^p = (Y-\alpha)^p$. Ainsi $\mathbb{F}_p(\alpha)$ est le corps de rupture de α et α n'est pas séparable sur $\mathbb{F}_p(X)$.*

Exercice 4.27 *En caractéristique zéro toute extension algébrique est séparable.*

Théorème 4.28 *Si L/K est une extension finie séparable alors il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Démonstration du lemme de Ax. Nous ne considérerons que la caractéristique zéro, où toutes les extensions algébriques sont séparables. À titre

d'illustration nous allons d'abord traiter le cas où L_1/K est une extension finie. Par le théorème 4.28, $L_1 = K(\alpha)$. Soit f le polynôme minimal de α sur K. Par hypothèse, il existe $\beta \in L_2$ tel que $f(\beta) = 0$. Or f est aussi le polynôme minimal de β sur K. Par le corollaire 4.7, il y a un K-isomorphisme $K(\alpha) \xrightarrow{\varphi} K(\beta)$ tel que $\varphi(\alpha) = \beta$. Il suffit maintenant de voir que $K(\beta) = L_2$. Soit $y \in L_2$ et g son polynôme minimal sur K. Soit $y_1 = y, y_2, \ldots, y_n$ les racines de g dans L_2. L'extension $K(\beta, y_1, \ldots, y_n)/K$ est aussi une extension finie séparable. Elle est donc de la forme $K(z)$; soit h le polynôme minimal de z sur K. Alors h a aussi au moins une racine dans L_1, disons x, et h est aussi le polynôme minimal de x sur K. Notons que $[K(z) : K] \geq [K(\beta) : K] = [K(\alpha) : K]$. Il existe un K-isomorphisme $K(z) \xrightarrow{\psi} K(x)$ tel que $\psi(z) = x$. On a $K(\psi(z)) \subseteq L_1 = K(\alpha)$. Or $[K(\psi(z)) : K] = [K(z) : K] \geq [K(\alpha) : K]$, ce qui entraîne que $K(\psi(z)) = K(\alpha)$. Ainsi $[K(z) : K] = [K(\psi(z)) : K] = [K(\alpha) : K] = [K(\beta) : K]$, d'où $K(z) = K(\beta)$ et $y \in K(\beta)$. Cela montre bien que $L_2 = K(\beta)$ et termine la démonstration dans ce cas particulier.

Pour le cas général nous avons besoin de la notion suivante. Soit E un corps intermédiaire entre K et L_1, qui est de la forme $E = K(x_1, \ldots, x_m)$ où les x_i sont les racines dans L_1 d'un polynôme irréductible sur K. Un tel corps a la propriété remarquable que si E'/K est une sous-extension de L_1/K tel que E' est K-isomorphe à E alors $E' = E$: en effet, un K-isomorphisme de E dans E' devra permuter les x_i entre eux de sorte que $E \subseteq E'$ et on conclut en comparant les degrés sur K. On dira qu'une sous-extension E/K de ce type est *normale par rapport à* L_1/K. Posons

$$I = \{E : E/K \text{ est normale par rapport à } L_1/K\}$$

$$J = \{F : F/K \text{ est normale par rapport à } L_2/K\}$$

Lemme 4.29 *Tout $H \in I$ est K-isomorphe à un $H' \in J$ et un seul, et vice versa.*

Démonstration. L'unicité est garantie par la remarque faite sur les extensions *normales par rapport à* L_i. Pour l'existence, on procède de façon semblable au cas particulier où $[L_1 : K]$ est fini, traité au tout début. □

Pour chaque $E \in I$ posons

$$Iso_{L_2/K}(E) = \{\sigma : \sigma \text{ est un } K\text{-isomorphisme } E \xrightarrow{\sigma} E' \text{ où } E' \in J\}$$

Lemme 4.30 *Pour tout $E \in I$, $Iso_{L_2/K}(E)$ est fini et non vide.*

Démonstration. On sait que $Iso_{L_2/K}(E)$ est non vide. Fixons un $\sigma_0 \in Iso_{L_2/K}(E)$. Alors pout tout $\sigma \in Iso_{L_2/K}(E)$, $\sigma_0^{-1}\sigma$ est un K-automorphisme de E. Puisque E/K est une extension finie, E n'a qu'un nombre fini de K-automorphismes et donc $Iso_{L_2/K}(E)$ doit être fini. □

En faisant le produit des $Iso_{L_2/K}(E)$, chacun muni de la topologie discrète, on obtient l'espace compact suivant.

$$X = \prod_{E \in I} Iso_{L_2/K}(E)$$

Pour $E_1, E_2 \in I$ tels que $E_1 \subseteq E_2$, posons

$$\mathcal{F}_{(E_1,E_2)} = \{(\sigma_E)_{E\in I} \in X : \sigma_{E_2}|_{E_1} = \sigma_{E_1}\}$$

Lemme 4.31 *Chaque $\mathcal{F}_{(E_1,E_2)}$ est un fermé non vide de X.*

Démonstration. Soit $E_1, E_2 \in I$ tels que $E_1 \subseteq E_2$ et soit $\sigma \in Iso_{L_2/K}(E_2)$. Alors $\sigma(E_1) = E_1' \in J$, car $E_1 \in I$. Pour $E \in I$: posons $\sigma_E = \sigma$ pour $E = E_2$, $\sigma_E = \sigma|_{E_1}$ pour $E = E_1$, et σ_E arbitraire autrement. Alors on a bien $(\sigma_E)_{E\in I} \in \mathcal{F}_{(E_1,E_2)}$. D'autre part $\mathcal{F}_{(E_1,E_2)}$ est bien fermé puisqu'il n'y a qu'un nombre fini de possibilités pour σ_{E_1} et σ_{E_2}. □

Lemme 4.32 *Toute intersection finie de $\mathcal{F}_{(E_1,E_2)}$ est non vide.*

Démonstration. Soit $E_{1i}, E_{2i} \in I, i = 1, \ldots, n$, tels que $E_{1i} \subseteq E_{2i}$. Alors $K(\cup_{i,j} E_{ij})$ est une extension finie de K et est contenue dans une certaine extension E_3/K où $E_3 \in I$. Pour tout $\sigma \in Iso_{L_2/K}(E_3), \sigma(E_{ij}) = E_{ij}' \in J$, de sorte que $(\sigma_E)_{E\in I}$ défini par $\sigma_E = \sigma|_{E_{ij}}$, pour $E = E_{ij}$, et σ_E arbitraire autrement, appartient à $\bigcap_{i=1}^n \mathcal{F}_{(E_{1i},E_{2i})}$. □

Par compacité, soit $(\sigma_E)_{E\in I} \in \bigcap_{E_1\subseteq E_2} \mathcal{F}_{(E_1,E_2)}$. Notons que $L_1 = \cup_{E\in I} E$ et que pour tout $E_k, E_l \in I$ il existe toujours $E_m \in I$ tel que $E_k, E_l \subseteq E_m$. Ainsi, par le choix de $(\sigma_E)_{E\in I}$, on obtient un K-homomorphisme $L_1 \xrightarrow{\sigma} L_2$ en posant $\sigma(x) = \sigma_E(x)$, si $x \in E$. Puisque $L_2 = \cup_{F\in J} F = \cup_{E\in I} \sigma(E)$, on a $\sigma(L_1) = L_2$, et σ est un K-isomorphisme de L_1 sur L_2. Cela termine la démonstration du lemme de Ax.

Le théorème des zéros de Hilbert, qui est une propriété fondamentale des corps algébriquement clos, nous dit qu'un système d'équations et d'inéquations polynomiales qui a une solution dans une extension d'un corps algébriquement clos possède déjà une solution dans ce corps algébriquement clos. Les corps algébriquement clos sont donc pleinement « algébriquement clos ». Le théorème est à la base d'une correspondance entre les variétés

algébriques affines et les idéaux premiers de polynômes, correspondance sur laquelle nous reviendrons dans la section consacrée à la dimension des variétés affines. Il est aussi connu sous le nom allemand « Nullstellensatz ».

Théorème 4.33 (Théorème des zéros) *Soit K un corps algébriquement clos et L une extension algébriquement close de K. Soit $f_1, \ldots, f_n, g \in K[X_1, \ldots, X_m]$. Alors le système polynomial*

$$\begin{aligned} f_1(X_1, \ldots, X_m) &= 0 \\ &\vdots \\ f_n(X_1, \ldots, X_m) &= 0 \\ g(X_1, \ldots, X_m) &\neq 0 \end{aligned}$$

possède une solution à valeurs dans L si et seulement si il en possède une à valeurs dans K.

Nous allons le déduire de l'élégant lemme suivant qu'on trouve dans le cours de Giraud [2]. Rappelons qu'un corps algébriquement clos est infini.

Lemme 4.34 *Soit K un corps infini et M un idéal propre maximal de $K[X_1, \ldots, X_m]$. Il existe un changement de variables linéaire homogène $X_i \mapsto Y_i$ tel que $M \cap K[Y_2, \ldots, Y_m]$ soit maximal dans $K[Y_2, \ldots, Y_m]$.*

Démonstration. Soit $f \in M$. Posons $f = F + \ldots$, où F est formé des termes de plus haut degré de f, et soit ν ce degré. Comme F n'est pas constant et K est infini, il existe $\alpha_1, \ldots, \alpha_m \in K$ non tous nuls tels que $F(\alpha_1, \ldots, \alpha_m) \neq 0$. Disons $\alpha_1 \neq 0$, et posons $X_1 = \alpha_1 Y_1$ et $X_i = \alpha_i Y_1 + Y_i$, $i \geq 2$. On a

$$f(\alpha_1 Y_1, \alpha_2 Y_1 + Y_2, \ldots, \alpha_m Y_1 + Y_m) = F(\alpha_1, \ldots, \alpha_m) Y_1^\nu + \ldots$$

Posons $R = K[Y_2, \ldots, Y_m]$ et $S = K[X_1, \ldots, X_m]$ et soit $P = M \cap R$. Je dis que P est un idéal propre maximal, ou ce qui est équivalent, que R/P est un corps. En effet, on a l'inclusion canonique $R/P \hookrightarrow S/M$ et si $a \in R/P$ est non nul, il admet un inverse a^{-1} dans S/M. Notons que S/M est un R/P-module noethérien, car R/P est un anneau noethérien et S/M est un module de type fini sur R/P qui est engendré sur R/P par $1, Y_1, Y_1^2, \ldots, Y_1^{\nu-1}$ (cf. preuve de la proposition 4.6). Considérons la suite de R/P-sous-modules de S/M :

$$R/P = < 1 > \subseteq < 1, a^{-1} > \subseteq < 1, a^{-1}, a^{-2} > \ldots$$

Cette suite doit être stationnaire. Cela entraîne qu'il existe un entier k et des $b_i \in R/P$ tels que

$$a^{-k} = b_1 a^{-(k-1)} + \ldots + b_{k-1} a^{-1} + b_k$$

d'où

$$a^{-1} = b_1 + b_2 a + \ldots + b_k a^{k-1}$$

et a^{-1} appartient donc à R/P. □

Corollaire 4.35 *Si K est algébriquement clos et si M est un idéal propre maximal de $K[X_1, \ldots, X_m]$, alors il existe $a_1, \ldots, a_m \in K$ tel que $M = (X_1 - a_1, \ldots, X_m - a_m)$.*

Démonstration. On procède par récurrence sur m. Le cas $m = 1$ est direct. Pour $m > 1$, avec la notation du lemme précédent, on obtient par récurrence que $P = (Y_2 - b_2, \ldots, Y_m - b_m)$, pour certains b_i dans K. Mais alors $R/P \simeq K$ de façon canonique et puisque S/M est une extension algébrique de R/P on a $R/P = S/M$. Soit a_i la classe résiduelle de X_i dans $S/M = K$. On voit directement que $M = (X_1 - a_1, \ldots, X_m - a_m)$. □

On peut alors déduire la direction non triviale du théorème des zéros. D'abord, en ajoutant une variable supplémentaire X_{m+1} et en remplaçant l'inéquation $g \neq 0$ par $X_{m+1} g - 1 = 0$, on obtient le système équivalent

$$f_1(X_1, \ldots, X_m) = 0$$

$$\vdots$$

$$f_n(X_1, \ldots, X_m) = 0$$

$$X_{m+1} g(X_1, \ldots, X_m) - 1 = 0.$$

On peut donc supposer qu'on n'a que des équations. Supposons que le système d'équations a une solution dans l'extension L. Alors l'idéal engendré par les f_i doit être un idéal propre. Soit M un idéal propre maximal contenant $f_1, \ldots, f_n$. Par le corollaire 4.35 il existe des $a_i \in K$ tels que $M = (X_1 - a_1, \ldots, X_m - a_m)$ et $a_1, \ldots, a_m$ fournissent la solution cherchée.

On considère le corollaire 4.35 comme une *version* du théorème des zéros. On peut montrer (exercice 5.4.5) que le théorème des zéros entraîne à son tour le corollaire 4.35.

4.3 Degré de transcendance

La notion de dépendance algébrique est le pendant dans la théorie des corps de la dépendance linéaire dans la théorie des espaces vectoriels. C'est donc une notion fondamentale. Elle sera utilisée à la section suivante, via le degré de transcendance qui en est issu, pour munir les variétés algébriques d'une notion algébrique de dimension.

Définition 4.36 *Soit L une extension d'un corps K.*

(1) Soient $x_1, \ldots, x_n$ des éléments de L. On dit que les x_i sont algébriquement dépendants *sur K s'il existe un polynôme $f \in K[X_1, \ldots, X_n]$ non nul tel que $f(x_1, \ldots, x_n) = 0$. Dans le cas contraire on dit qu'ils sont* algébriquement indépendants*.*

(2) Soit A un sous-ensemble de L. On dit que A est algébriquement dépendant sur K si un sous-ensemble fini de A l'est. Dans le cas contraire on dit que A est algébriquement indépendant.

Autrement dit, $x_1, \ldots, x_n$ sont algébriquement dépendants si le noyau de l'homomorphisme d'évaluation en $\underline{x} = (x_1, \ldots, x_n)$,

$$K[X_1, \ldots, X_n] \xrightarrow{év_{\underline{x}}} K[x_1, \ldots, x_n]$$

est non nul.

Exemple 4.37

(1) On peut remarquer que x est algébriquement dépendant sur K si et seulement si x est algébrique sur K, et donc algébriquement indépendant sur K si et seulement si il est transcendant sur K.

(2) On a le résultat suivant de Lindemann[2], que nous ne faisons qu'énoncer : soit $a_1, \ldots, a_n$ des nombres complexes algébriques, si $a_1, \ldots, a_n$ sont linéairement indépendants sur $\mathbb{Q}$, alors $e^{a_1}, \ldots, e^{a_n}$ sont algébriquement indépendants sur $\mathbb{Q}$. En particulier, on obtient la transcendance de e en prenant $a = 1$.

(3) Dans le corps des fractions rationelles $K(X_1, \ldots, X_n)$, $X_1, \ldots, X_n$ sont algébriquement indépendants sur K.

(4) On vérifie que $x_1, \ldots, x_n$ sont algébriquement indépendants sur K si et seulement si $K(x_1, \ldots, x_n)$ est isomorphe au corps des fractions rationnelles $K(X_1, \ldots, X_n)$, par un K-isomorphisme qui envoie X_i sur x_i.

[2]Ferdinand Lindemann, 1852-1939.

On peut remarquer que si $x_1, \ldots, x_n$ sont algébriquement indépendants sur K, alors il sont aussi linéairement indépendants sur K, puisqu'une relation de dépendance linéaire sur K est donnée par un polynôme $f \in K[X_1, \ldots, X_n]$ non nul de degré 1.

Lemme 4.38 *Si $x \in K$, alors x est algébriquement dépendant sur K.*

Lemme 4.39 *Si x est algébrique sur K, alors il existe $k_1, \ldots, k_n \in K$ tel que x est algébrique sur le sous-corps de K engendré par $k_1, \ldots, k_n$.*

Lemme 4.40 *Un ensemble $x_1, \ldots, x_n$ est algébriquement dépendant sur K si et seulement si il y a un x_i tel que x_i est algébrique sur $K(\{x_j : j \neq i\})$.*

Démonstration. Une direction est directe. Supposons $x_1, \ldots, x_n$ algébriquement dépendants sur K. On raisonne par récurrence. Si $n = 1$, il n'y a rien à voir. Pour la récurrence, on peut supposer que $x_2, \ldots, x_n$ sont algébriquement indépendants sur K. Soit $f \in K[X_1, \ldots, X_n]$, $f \neq 0$, tel que $f(x_1, \ldots, x_n) = 0$. Posons $f = \sum_{0 \leq i \leq n} f_i(X_2, \ldots, X_n) X_1^i$, $f_i \in K[X_2, \ldots, X_n]$. Puisque $f \neq 0$ l'un au moins des f_i est non nul, disons f_{i_0}. Alors $f_{i_0}(x_2, \ldots, x_n) \neq 0$ car $x_2, \ldots, x_n$ sont algébriquement indépendants sur K. Ainsi

$$g(X) = \sum_{0 \leq i \leq n} f_i(x_2, \ldots, x_n) X^i$$

est un polynôme non nul tel que $g(x_1) = 0$ et $g \in K(x_2, \ldots, x_n)[X]$. □

Le lemme suivant est analogue à la situation suivante dans les espaces vectoriels : si x est une combinaison linéaire de $y_1, \ldots, y_n$ mais pas de $y_2, \ldots, y_n$, alors y_1 est une combinaison linéaire de $x, y_2, \ldots, y_n$.

Lemme 4.41 *Si x est algébrique sur $K(y_1, \ldots, y_n)$ mais pas sur $K(y_2, \ldots, y_n)$, alors y_1 est algébrique sur $K(x, y_2, \ldots, y_n)$*

Démonstration. Soit $f \in K[X, Y_1, \ldots, Y_n]$, $f \neq 0$, tel que $f(x, y_1, \ldots, y_n) = 0$. Posons $f = \sum_{0 \leq i \leq d} f_i(Y_1, \ldots, Y_n) X^i$, où $d \geq 1, f_i \in K[Y_1, \ldots, Y_n]$ et $f_d(y_1, \ldots, y_n) \neq 0$. On peut aussi poser $f = \sum_{0 \leq j \leq s} g_j(X, Y_2, \ldots, Y_n) Y_1^j$, où les $g_j \in K[X, Y_2, \ldots, Y_n]$ ne sont pas tous nuls. Il doit y avoir un $j \geq 1$ tel que $g_j(x, y_2, \ldots, y_n) \neq 0$, sinon la seule possibilité serait que g_j ne dépend pas de X pour $j \geq 1$ et alors on aurait $f = g_0(X, Y_2, \ldots, Y_n) + \sum_{j \geq 1} g_j(Y_2, \ldots, Y_n) Y_1^j$. Donc X devrait apparaître dans g_0 et x serait algébrique sur $K(y_2, \ldots, y_n)$, ce qui n'est pas le cas. Ainsi y_1 est racine du polynôme non nul $\sum_j g_j(x, y_2, \ldots, y_n) X^j$ de degré au moins 1 et il est donc algébrique sur $K(x, y_2, \ldots, y_n)$. □

Lemme 4.42 *Soit A un ensemble algébriquement indépendant sur K et x un élément qui est transcendant sur $K(A)$. Alors $A \cup \{x\}$ est algébriquement indépendant sur K.*

Démonstration. On doit avoir $x \notin A$. Supposons que $A \cup \{x\}$ soit algébriquement dépendant sur K. Par le lemme 4.40 il existe $y \in A$ tel que y soit algébrique sur $K((A \setminus \{y\}) \cup \{x\})$. Puisque A est algébriquement indépendant sur K, y n'est pas algébrique sur $A \setminus \{y\}$ (lemme 4.40), et donc x serait algébrique sur $K((A \setminus \{y\}) \cup \{y\}) = K(A)$ (lemme 4.41), ce qui serait absurde. □

Définition 4.43 *Soit L/K une extension de corps. Un sous-ensemble B de L est appelé* base de transcendance de L sur K *si il possède les deux propriétés suivantes :*

1) *l'ensemble B est algébriquement indépendant sur K ;*
2) *tout élément de L est algébrique sur $K(B)$.*

Exemple 4.44

(1) *Si L/K est une extension algébrique alors, $B = \emptyset$ est une base de transcendance de L sur K.*
(2) *Soit $L = K(X_1, \ldots, X_n)$ le corps des fractions rationnnelles sur K en les indéterminées $X_1, \ldots, X_n$, alors $B = \{X_1, \ldots, X_n\}$ est une base de transcendance de L sur K.*

Les exemples précédents sont d'une certaine façon extrêmes.

Théorème 4.45 *Toute extension de corps possède une base de transcendance et deux bases de transcendance ont toujours la même cardinalité.*

Démonstration. Pour l'existence on utilise le lemme 4.42 et le lemme de Zorn, une base de transcendance étant un ensemble algébriquement indépendant maximal. Pour ce qui est de la cardinalité, on peut distinguer selon qu'il existe une base de transcendance finie ou non. Si il y a une base vide c'est que l'extension est algébrique et il ne peut y avoir que cette base. Soit L/K une extension et supposons qu'on ait une base de transcendance finie $B = \{x_1, \ldots, x_n\}$. Supposons que C est une autre base de transcendance.

Lemme 4.46 *Pour tout $1 \leq k \leq n+1$ il existe $y_1, \ldots, y_{k-1} \in C$ tels que $\{y_1, \ldots, y_{k-1}, x_k, \ldots, x_n\}$ soit une base de transcendance.*

Démonstration. On procède par récurrence sur k. Pour $k = 1$ il n'y a rien à voir. Supposons qu'on ait déjà $y_1, \ldots, y_{k-2}$, c'est-à-dire que $\{y_1, \ldots, y_{k-2}, x_{k-1}, x_k, \ldots, x_n\}$ soit une base de transcendance.. Il doit y avoir un $y \in C$ tel que y n'est pas algébrique sur $K(y_1, \ldots, y_{k-2}, x_k, \ldots, x_n)$, sinon tous les éléments de C le seraient, et puisque tous les éléments sont algébriques sur $K(C)$ on obtiendrait en particulier aussi que x_{k-1} serait algébrique sur $K(y_1, \ldots, y_{k-2}, x_k, \ldots, x_n)$. Mais ceci contredit l'hypothèse de récurrence selon laquelle $y_1, \ldots, y_{k-2}, x_{k-1}, x_k, \ldots, x_n$ sont algébriquement indépendants sur K (lemme 4.40). Soit donc $y_{k-1} \in C$ qui ne soit pas algébrique sur $K(y_1, \ldots, y_{k-2}, x_k, \ldots, x_n)$. Par le lemme 4.42, $y_1, \ldots, y_{k-2}, y_{k-1}, x_k, \ldots, x_n$ sont algébriquement indépendants sur K. Puisque y_{k-1} est algébrique sur $K(y_1, \ldots, y_{k-2}, x_{k-1}, x_k, \ldots, x_n)$, le lemme 4.41 assure que x_{k-1} est algébrique sur $K(y_1, \ldots, y_{k-2}, y_{k-1}, x_k, \ldots, x_n)$ et il s'ensuit que tous les éléments de L sont algébriques sur $K(y_1, \ldots, y_{k-2}, y_{k-1}, x_k, \ldots, x_n)$. Ainsi $y_1, \ldots, y_{k-2}, y_{k-1}, x_k, \ldots, x_n$ forment une base de transcendance, ce qui complète la récurrence. □

En appliquant le lemme avec $k = n + 1$, on obtient une base de transcendance $\{y_1, \ldots, y_n\} \subseteq C$, d'où $\{y_1, \ldots, y_n\} = C$ et on a fini. Le lemme assure en même temps qu'on a, ou bien seulement des bases de transcendance finie avec le même nombre d'éléments, ou bien seulement des bases de transcendance infinie. Dans le cas infini, on peut procéder comme avec les modules libres de rang infini (voir la proposition 3.26). Cela termine la démonstration du théorème.

Définition 4.47 *Soit L/K une extension de corps. On appelle* degré de transcendance de L sur K, *noté $degtr(L/K)$ ou $degtr_K L$, la cardinalité d'une base de transcendance de L sur K.*

Exemple 4.48

1) *Si L/K est une extension algébrique, $degtr(L/K) = 0$.*
2) *Soit $L = K(X_1, \ldots, X_n)$ le corps des fractions rationnnelles sur K en les indéterminées $X_1, \ldots, X_n$, alors $degtr(L/K) = n$.*

Exercice 4.49

1) *Montrer que deux corps algébriquement clos qui ont la même caractéristique et le même degré de transcendance fini sur leur corps premier sont isomorphes.*
2) *Montrer que deux corps algébriquement clos qui ont la même caractéristique et le même degré de transcendance sur leur corps premier sont isomorphes.*

L'exercice précédent indique en quelque sorte la structure des corps algébriquement clos et met en évidence l'analogie du degré de transcendance avec la dimension des espaces vectoriels.

Les arguments utilisés à partir des propriétés de la dépendance algébrique pour aboutir au degré de transcendance sont d'ordre tout à fait général. Steinitz en a dégagé les propriétés fondamentales, qui se trouvent être dans les lemmes 4.38, 4.39,4.40, 4.41, et il a décrit une théorie générale des relations de dépendance. Nous renvoyons à [4], chap. 3.

4.4 La dimension des variétés affines

Dans cette section nous utilisons le degré de transcendance pour définir une notion algébrique de dimension pour les variétés algébriques affines.

Nous fixons un corps de base algébriquement clos K . On notera parfois $K[\boldsymbol{X}]$ l'anneau de polynômes $K[X_1, \ldots, X_n]$.

Définition 4.50 *Soit F un ensemble de polynômes appartenant à l'anneau $K[X_1, \ldots, X_n]$, et soit E un sous-ensemble quelconque de K^n.*

(1) Un point $(x_1, \ldots, x_n) \in K^n$ est appelé un zéro *de F si $f(x_1, \ldots, x_n) = 0$ pour tout $f \in F$.*

(2) L'ensemble des zéros de F, noté $\mathcal{Z}(F)$ ou $\mathcal{Z}_K(F)$, est appelé un ensemble algébrique affine*, ou K-ensemble algébrique affine si on veut préciser le corps de base K.*

(3) On définit $\mathcal{I}(E) = \{f \in K[X_1, \ldots, X_n] : f(x) = 0$, pour tout $x \in E\}$. C'est l'ensemble des polynômes qui s'annulent en tout point de E.

On vérifie facilement que $\mathcal{I}(E)$ est un idéal de $K[X_1, \ldots, X_n]$.

Proposition 4.51 *Soit F, F_1, F_2 des ensembles de polynômes de $K[\boldsymbol{X}]$, et E, E_1, E_2 des sous-ensembles de K^n.*

(1) $F_1 \supseteq F_2$ entraîne $\mathcal{Z}(F_1) \subseteq \mathcal{Z}(F_2)$;

(2) $E_1 \supseteq E_2$ entraîne $\mathcal{I}(E_1) \subseteq \mathcal{I}(E_2)$;

(3) $\mathcal{Z}(\mathcal{I}(E)) \supseteq E$;

(4) $\mathcal{I}(\mathcal{Z}(F)) \supseteq F$;

(5) $\mathcal{I}(\mathcal{Z}(\mathcal{I}(E))) = \mathcal{I}(E)$;

(6) $\mathcal{Z}(\mathcal{I}(\mathcal{Z}(F))) = \mathcal{Z}(F)$.

La proposition précédente nous dit donc que pour tout ensemble algébrique A on a $\mathcal{Z}(\mathcal{I}(A)) = A$. Il s'ensuit que la correspondance qui associe à tout ensemble algébrique A son idéal $\mathcal{I}(A)$ est injective, et que la correspondance qui associe à tout idéal I son ensemble de zéros $\mathcal{Z}(I)$ est surjective sur l'ensemble des K-ensembles algébriques affines. On a $\mathcal{I}(\mathcal{Z}(I)) \supseteq I$, mais pas toujours l'égalité, par exemple pour $I = (X_1^2)$. Cela indique que les correspondances ci-dessus ne sont pas biunivoques. On verra plus loin pour quelle classe d'idéaux elles deviennent inverses l'une de l'autre.

Les ensembles algébriques A dont l'idéal $\mathcal{I}(A)$ est *premier* ont des propriétés particulières.

Définition 4.52 *Soit R un anneau commutatif et I un idéal de R. On dit que I est un* idéal premier*, si pour tous $x, y \in R$, $xy \in I$ entraîne $x \in I$ ou $y \in I$.*

Les ensembles algébriques A dont l'idéal $\mathcal{I}(A)$ est premier ont la propriété suivante : A ne peut être la réunion de deux ensembles K-algébriques plus petits, c'est-à-dire que $A = A_1 \cup A_2$ entraîne $A = A_1$ ou $A = A_2$, où les A_i sont K-algébriques. En effet, supposons $A = A_1 \cup A_2$,alors $\mathcal{I}(A) = \mathcal{I}(A_1) \cap \mathcal{I}(A_2)$ et comme $\mathcal{I}(A)$ est premier on obtient $\mathcal{I}(A) \supseteq \mathcal{I}(A_1)$ ou $\mathcal{I}(A) \supseteq \mathcal{I}(A_2)$. Si, par exemple, $\mathcal{I}(A) \supseteq \mathcal{I}(A_1)$ alors $A \subseteq A_1$, d'où l'égalité. En fait, cette propriété caractérise les ensembles algébriques dont l'idéal est premier.

Définition 4.53 *Un K-ensemble algébrique A est dit* irréductible *s'il ne peut être la réunion de deux K-ensembles algébriques affines plus petits, c'est-à-dire pour tous K-ensembles algébriques affines A_i la relation $A = A_1 \cup A_2$ entraîne $A = A_1$ ou $A = A_2$. Un tel ensemble algébrique est aussi appelé une* K-variété affine.

Proposition 4.54 *Un K-ensemble algébrique affine A est irréductible si et seulement si son idéal $\mathcal{I}(A)$ est un idéal premier.*

Démonstration. Il reste à voir que si $\mathcal{I}(A)$ n'est pas premier alors A n'est pas irréductible. Supposons donc que $\mathcal{I}(A)$ n'est pas premier, et soit $f_1, f_2 \notin \mathcal{I}(A)$ tels que $f_1 f_2 \in \mathcal{I}(A)$. Posons $A_i = \mathcal{Z}(\mathcal{I}(A), f_i)$, $i = 1, 2$. On a $A_i \subseteq A$, $i = 1, 2$. D'autre part, il existe un point $x_i \in A$ qui témoigne de $f_i \notin \mathcal{I}(A)$, donc tel que $f(x_i) \neq 0$, d'où $x_i \notin A_i$. Donc les A_i sont des sous-ensembles plus petits que A. Il reste à voir que $A \subseteq A_1 \cup A_2$, mais cela découle directement de ce que $f_1 f_2 \in \mathcal{I}(A)$: soit $x \in A$, alors $f_1(x) f_2(x) = 0$, d'où $f_1(x) = 0$ ou $f_2(x) = 0$, et $x \in A_1$ ou $x \in A_2$ selon le cas. □

Exemple 4.55

(1) On vérifie qu'un point $P \in K^n$ est une K-varété affine.

(2) Soit $V = K^n$. On vérifie que V est une K-variété affine.

(3) Soit $V = \mathcal{Z}(XY)$, V n'est pas une varété affine puisque $V = \mathcal{Z}(X) \cup \mathcal{Z}(Y)$.

Définition 4.56 *Soit $V \subset K^n$ une K-variété affine. Son idéal $\mathcal{I}(V)$ est donc premier. On appelle* anneau de V*, noté $K[V]$, l'anneau quotient $K[X_1, \ldots, X_n]/\mathcal{I}(V)$. C'est un anneau intègre dont nous noterons $K(V)$ le corps des fractions. On définit la* dimension *de V, notée $dimV$, comme étant le degré de transcendance de $K(V)$ sur K.*

Exemple 4.57 *Soit $K = \mathbb{C}$, $V = \{(x, y) \in \mathbb{C} : y - x^2 = 0\}$. On vérifie que $\mathcal{I}(V) = (Y - X^2)$, que c'est un idéal premier de $\mathbb{C}[X, Y]$ et que $dimV = 1$.*

Proposition 4.58 *Soit V_1, V_2 des K-variétés affines.*

(1) Si V et un point de K^n alors $dimV = 0$;

(2) Soit $V = K^n$, alors $dimV = n$;

(3) Si $V_1 \subseteq V_2$ alors $dimV_1 \leq dimV_2$.

Nous complétons maintenant la discussion sur la correspondance entre les ensembles algébriques et les idéaux de polynômes. Le théorème des zéros permet d'identifier la classe d'idéaux de polynômes qui est en correspondance biunivoque avec les ensembles algébriques.

Définition 4.59 *Soit A un anneau unitaire commutatif. On définit la* racine d'un idéal *I, noté $\sqrt{I}$, comme suit*

$$\sqrt{I} = \{a \in A : \text{ il existe un entier } n \text{ tel que } a^n \in I\}$$

autrement dit c'est l'ensemble des éléments dont une puissance appartient à I.

Proposition 4.60 *La racine $\sqrt{I}$ d'un idéal I est aussi un idéal et $I \subseteq \sqrt{I}$.*

Définition 4.61 *Un idéal est dit* radical *si il est égal à sa racine, c'est-à-dire si $I = \sqrt{I}$.*

Exemple 4.62

(1) Tout idéal premier est radical.

(2) L'idéal (XY) est un idéal radical, qui n'est pas premier.

Proposition 4.63 *Pour tout idéal I de $K[X_1, \ldots, X_n]$, $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$.*

Démonstration. On vérifie directement que $\sqrt{I} \subseteq \mathcal{I}(\mathcal{Z}(I))$. Il reste donc à vérifier l'inclusion $\mathcal{I}(\mathcal{Z}(I)) \subseteq \sqrt{I}$. Soit $f \in \mathcal{I}(\mathcal{Z}(I))$. Soit $f_1, \ldots, f_m$ des générateurs de I. Considérons les polynômes $f_1, \ldots, f_m, 1 - Tf$ de l'anneau de polynômes à $n+1$ variables $K[X_1, \ldots, X_n, T]$. Ils ne possèdent dans K^n aucun zéro commun. En effet, un zéro commun z des f_i est un zéro de I, de sorte que $f(z) = 0$ et donc $1 - Tf(X_1, \ldots, X_n)$ prend la valeur 1 en z ; ainsi les f_i et $1 - Tf$ ne peuvent avoir de zéro commun. Par une conséqunece du théorème des zéros, $f_1, \ldots, f_m, 1 - Tf$ engendrent l'idéal trivial (1) et il existe donc des polynômes $g_i, g \in K[X_1, \ldots, X_n, T]$ tels que

$$g_1 f_1 + \ldots + g_n f_n + g(1 - Tf) = 1$$

En substituant $\frac{1}{f}$ à T dans cette relation, on obtient

$$\sum_{i=1}^{m} g_i(X_1, \ldots, X_n, \frac{1}{f(X_1, \ldots, X_n)}) f_i(X_1, \ldots, X_n) = 1$$

En chassant les dénominateurs, on en tire une relation de la forme

$$\sum_{i=1}^{m} h_i(X_1, \ldots, X_n,) f_i(X_1, \ldots, X_n) = f^s(X_1, \ldots, X_n)$$

où $h_i \in K[X_1, \ldots, X_n]$ et $s \geq 1$ est un entier positif. C'est donc dire que $f \in \sqrt{I}$. □

Corollaire 4.64 *Si P est un idéal premier alors $\mathcal{I}(\mathcal{Z}(P)) = P$.*

Il s'ensuit que les opérations I et Z établissent une correspondance biunivoque, l'une inverse de l'autre, entre les K-ensembles algébriques irréductibles et les idéaux premiers de $K[\boldsymbol{X}]$. On a plus.

Corollaire 4.65 *Un idéal de polynômes de $K[X_1, \ldots, X_n]$ est l'idéal d'un ensemble K-algébrique si et seulement si c'est un idéal radical.*

Démonstration. En effet, on vérifie directement que l'idéal d'un ensemble algébrique est radical. D'autre part, si un I est un idéal radical alors c'est l'idéal de son ensemble de zéros $Z(I)$ par la proposition. □

Il s'ensuit que les opérations I et Z établissent une correspondance bi-univoque, l'une inverse de l'autre, entre les ensembles algébriques de K^n et les idéaux radicaux de polynômes.

On généralise la notion de dimension à tous les ensembles algébriques à l'aide du théorème suivant, que nous nous contenterons d'énoncer.

Théorème 4.66 *Tout K-ensemble algébrique s'exprime d'une manière unique comme réunion finie non triviale de K-variétés, à savoir sans qu'aucune de ces K-variétés ne soit contenue dans la réunion des autres.*

Les K-variétés associées à un K-ensemble algébrique par ce théorème sont appelées ses *composantes irréductibles*. On définit alors la dimension d'un K-ensemble algébrique comme étant le maximum parmi les dimensions de ses composantes irréductibles.

4.5 La résolution par radicaux

On sait comment résoudre les équations quadratiques $X^2+aX+b=0$, disons rationnelles, $a, b \in \mathbb{Q}$. Les racines sont données par la formule

$$x = \frac{-a \pm \sqrt{a^2-4b}}{2}$$

ou plus précisément par *les* formules

$$x_1 = \frac{-a+\sqrt{a^2-4b}}{2}$$

$$x_2 = \frac{-a-\sqrt{a^2-4b}}{2}.$$

Il est bon de souligner le fait que ces formules sont valables dans *tous* les corps de caractéristique différente de 2. On pourrait dire qu'elles sont *universelles*. On sait qu'il existe des formules semblables pour les équations polynomiales de degré 3, $X^3+aX^2+bX+c=0$

$$\begin{aligned} x \;=\; & -\frac{a}{3} + \sqrt[3]{\frac{\frac{ab}{3}-c-\frac{2a^3}{27}}{2} + \sqrt{\left(\frac{\frac{ab}{3}-c-\frac{2a^3}{27}}{2}\right)^2 + \left(\frac{b-\frac{a^2}{3}}{3}\right)^3}} \\ & + \sqrt[3]{\frac{\frac{ab}{3}-c-\frac{2a^3}{27}}{2} - \sqrt{\left(\frac{\frac{ab}{3}-c-\frac{2a^3}{27}}{2}\right)^2 + \left(\frac{b-\frac{a^2}{3}}{3}\right)^3}} \end{aligned}$$

et les équation polynomiales de degré 4, $X^4 + aX^3 + bX^2 + cX + d = 0$

$$x = -\frac{a}{4} + \frac{1}{2}\left(\sqrt{\gamma - \left(b - \frac{3a^2}{8}\right)} + \sqrt{\beta - \left(b - \frac{3a^2}{8}\right)} + \sqrt{\alpha - \left(b - \frac{3a^2}{8}\right)}\right)$$

où α, β, γ sont les racines de $X^3 - a_0X^2 - 4c_0X + 4a_0c_0 - b_0^2 = 0$, et $a_0 = (b - \frac{3a^2}{8}), b_0 = \frac{11}{64}a^3 - \frac{1}{2}ab + c, c_0 = \frac{15}{64}a^4 + \frac{1}{16}a^2b - \frac{1}{4}ac + d$. Existe-t-il des formules de ce genre pour chaque degré $n = 5, 6, 7 \ldots$? La réponse à cette question célèbre est non, et c'est ce que nous allons voir. Cette question est éclaircie par « la théorie de Galois », dont les idées sont parmi les plus fécondes en mathématiques. Nous l'effleurerons à peine.

Pour fixer les idées et donner une formulation à la fois précise et commode des résultats, nous allons supposer que toute la discussion se passe dans le corps des nombres complexes $\mathbb{C}$. On fera donc comme si tous les corps dont nous allons parler s'y trouvaient, de même que toutes les racines de tous les polynômes. Il y aurait plusieurs façons de faire une discussion complètement générale, par exemple travailler dans une clôture algébrique du corps de base, mais là n'est pas notre propos. On peut dire que notre point de départ est la résolution des équations rationnelles, c'est-à-dire sur $\mathbb{Q}$, et que nous nous contenterons d'illustrer les idées dans ce contexte.

Si on revient à l'équation quadratique $X^2 + aX + b = 0$, disons avec a, b dans un corps K, et à ses racines x_1, x_2, on peut remarquer que

$$\begin{aligned} K(x_1, x_2) &= K(\sqrt{a^2 - 4b}) \\ &= K(\alpha) \qquad\qquad , \alpha^2 = a^2 - 4b \in K \end{aligned}$$

On remarque aussi que les formules pour les degré 3 et 4 ne font intervenir en plus des quatres opérations élémentaires $+, -, \times, \div$, que des extractions de racines.

Définition 4.67

(1) Soit K un corps. Un polynôme $f \in K[X]$ est dit résoluble sur K *si il existe une suite d'extensions K_{i+1}/K_i avec des éléments $\alpha_i \in K_i$, et des entiers $d_i > 0$, $i = 1, \ldots, n$ tels que*

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n = K_f$$

où K_f est le corps de rupture de f, et où $K_{i+1} = K_i(\alpha_{i+1})$, $\alpha_{i+1}^{d_{i+1}} \in K_i$, autrement dit $K_{i+1} = K_i(\sqrt[d_{i+1}]{a_i}), a_i = \alpha_{i+1}^{d_{i+1}} \in K_i$.

(2) On dira qu'un polynôme f est résoluble*, si il est résoluble sur le corps engendré par ses coefficients.*

Avec la notation de la définition, considérons un élément

$$x \in K_2$$

Il peut s'exprimer

$$x = g(\alpha_1, \alpha_2)$$

où g est un polynôme à deux variables sur K. Utilisons la notation $\alpha_i = \sqrt[d_{i+1}]{a_i}$:

$$x \;=\; g(\sqrt[d_1]{a_0},\ \sqrt[d_2]{a_1})$$

Puisque $a_1 \in K_1 = K(\alpha_0)$, on a $a_1 = h(\alpha_0)$, où h est un polynôme à une variable sur K, disons $h = \sum_{j=1}^{m} b_j X^j$, $b_j \in K$. On obtient

$$\begin{aligned} x &= g\left(\sqrt[d_1]{a_1},\ \sqrt[d_2]{h(\sqrt[d_1]{a_1})}\right) \\ x &= g\left(\sqrt[d_1]{a_1},\ \sqrt[d_2]{b_0 + b_1\sqrt[d_1]{a_1} + \ldots + b_m\sqrt[d_1]{a_1}^m}\right) \end{aligned}$$

De la même façon, un élément $x \in K_n$ peut s'exprimer en termes d'éléments de K à l'aide des quatre opérations élémentaires et d'extractions de racines. Ce sera donc le cas des racines de f, d'où des « formules par radicaux » pour obtenir les racines de f en termes d'éléments du corps K.

Exercice 4.68

(1) Tout polynôme sur $\mathbb{C}$ est résoluble sur $\mathbb{C}$.

(2) Tout polynôme sur $\mathbb{R}$ est résoluble sur $\mathbb{R}$.

(3) Tout polynôme quadratique est résoluble.

(4) Tout polynôme de degré trois est résoluble.

(5) Tout polynôme de degré quatre est résoluble.

(6) Si un polynôme est résoluble sur K, il est résoluble sur toute extension de K.

S'il existait des formules générales par radicaux pour les racines de tout polynôme de degré $n \geq 5$, en particulier tout polynôme de degré n sur $\mathbb{Q}$ serait résoluble par radicaux. Nous allons montrer qu'il existe des polynômes rationnels de chaque degré $n \geq 5$ qui ne sont pas résolubles. Cela indiquera qu'à partir du degré 5, il ne peut y avoir de formules générales par radicaux pour les racines d'un polynôme.

Définition 4.69 *Soit E/F une extension de corps. Le* groupe de Galois de E/F, *noté $Gal(E/F)$, est le groupe des automorphismes de E qui coïncident avec l'identité sur les éléments de F, autrement dit les automorphismes σ tels que $\sigma(x) = x$, pour tout $x \in F$.*

Exemple 4.70 *Le groupe de Galois $Gal(\mathbb{C}/\mathbb{R}) = \{id, \bar{}\}$, où $\bar{}$ est la conjugaison complexe.*

Soit K un corps et $f \in K[X]$, nous allons noter K_f le corps de rupture de f sur K et nous allons noter $G_{f/K}$ le groupe de Galois de K_f/K, qu'on appellera groupe de Galois de f sur K. Soit f un polynôme, on appellera *groupe de Galois de f* son groupe de Galois sur le corps engendré par ses coefficients et on le notera G_f. Comme un élément de $G_{f/K}$ doit permuter entre elles les racines de f et que K_f/K est engendré par ces racines, il y a un plongement de $G_{f/K}$ dans le groupe des permutations des racines de f, identifiable à un groupe symétrique S_n. En particulier $G_{f/K}$ est un groupe fini. Il est en général difficile deÊ calculer à la main le groupe de Galois d'un polynôme. Quelques logiciels permettent certains calculs.

Rappelons qu'un groupe fini G est dit résoluble si il possède une suite de composition

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = 1$$

dont les quotients G_i/G_{i+1} sont abéliens. Nous utiliserons le fait que tout sous-groupe et tout quotient d'un groupe résoluble est aussi résoluble. Voici le théorème principal de cette section.

Théorème 4.71 [3] *Si un polynôme f est résoluble sur K, alors le groupe de Galois $G_{f/K}$ est résoluble.*

Pour trouver des polynômes rationnels non résolubles, il suffira donc d'en trouver dont le groupe de Galois n'est pas résoluble. Or, à partir de $n = 5$ le groupe symétrique S_n n'est pas résoluble puisqu'il possède un sous-groupe qui n'est pas résoluble, à savoir le groupe alterné A_n, qui est simple mais non abélien. On donnera un moyen de fabriquer des polynômes de chaque degré premier $p \geq 5$ dont le groupe de Galois est S_p, et cela suffira pour obtenir des polynômes non résolubles de chaque degré $n \geq 5$.

Démonstration du théorème 4.71. Supposons que f est résoluble sur K et soit une suite d'extensions K_{i+1}/K_i

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n = K_f$$

[3] Les deux conditions sont en fait équivalentes.

où $K_{i+1} = K_i(\alpha_{i+1})$, $\alpha_{i+1}^{d_{i+1}} = a_i \in K_i$. Soit $m = d_1 d_2 \dots d_n$ et ζ une racine primitive m-ième de 1. Posons $K_i' = K_i(\zeta)$. On obtient la nouvelle suite d'extensions successives

$$K \subseteq K(\zeta) = K_0' \subseteq K_1' \subseteq K_2' \subseteq \dots \subseteq K_n' = K_f(\zeta)$$

Considérons $Gal(K_f/K)$ et $Gal(K_n'/K)$. Un élément $\sigma \in Gal(K_n'/K)$ doit permuter entre elles les racines de f et puisque K_f/K est engendré par elles on doit avoir $\sigma(K_f) = K_f$. On a donc un homomorphisme de restriction

$$Gal(K_n'/K) \xrightarrow{\rho} Gal(K_f/K)$$

De plus, K_n' est aussi le corps de rupture de $f(X)(X^m - 1)$ sur K_f de sorte que par la proposition 4.25 l'application de restriction ci-dessus est surjective. Ainsi $Gal(K_f/K)$ est un quotient de $Gal(K_n'/K)$ et on se ramène à montrer que $Gal(K_n'/K)$ est résoluble. Avant de continuer, on peut remarquer que $ker(\rho) = Gal(K_n'/K_f)$ de sorte que

$$Gal(K_n'/K_f) \lhd Gal(K_n'/K)$$

et

$$Gal(K_n'/K)/Gal(K_n'/K_f) \simeq Gal(K_f/K)$$

À partir de la suite des K_i' on obtient la suite de groupes suivante

$$Gal(K_n'/K) \geq Gal(K_n'/K_0') \geq Gal(K_n'/K_1') \geq \dots \geq Gal(K_n'/K_n') = 1$$

Notons d'abord que K_0' est le corps de rupture de $X^m - 1$ sur K, de sorte qu'on a un homomorphisme de restriction $Gal(K_n'/K) \to Gal(K_0'/K)$ surjectif comme ci-dessus et dont le noyau est précisément $Gal(K_n'/K_0')$. On obtient

$$Gal(K_n'/K_0') \lhd Gal(K_n'/K)$$

et

$$Gal(K_n'/K)/Gal(K_n'/K_0') \simeq Gal(K_0'/K)$$

C'est le début de notre suite de composition pour $Gal(K_n'/K)$. Pour continuer, on remarque qu'une fois ajouté ζ au début on a aussi toutes les racines d_i-ièmes de 1, de sorte que K_{i+1}' contient toutes les racines d_{i+1}-ièmes de a_i et est le corps de rupture de $X^{d_{i+1}} - a_i$ sur K_i'. On a donc la même configuration que ci-dessus avec un homomorphisme de restriction surjectif

$$Gal(K_n'/K_i) \to Gal(K_{i+1}'/K_i)$$

dont le noyau est $Gal(K'_n/K'_{i+1})$, d'où

$$Gal(K'_n/K'_{i+1}) \lhd Gal(K'_n/K_i)$$

et

$$Gal(K'_n/K'_i)/Gal(K'_n/K'_{i+1}) \simeq Gal(K'_{i+1}/K_i)$$

On a donc bien une suite de composition

$$Gal(K'_n/K) \rhd Gal(K'_n/K'_0) \rhd Gal(K'_n/K'_1) \rhd \ldots \rhd Gal(K'_n/K'_n) = 1$$

dont les quotients sont

$$Gal(K'_0/K) = Gal(K(\zeta)/K)$$

et

$$Gal(K'_{i+1}/K'_i) = Gal(K'_i(\alpha_i)/K'_i)$$

Il s'agit maintenant de voir que ces quotients sont abéliens. Pour $Gal(K(\zeta)/K)$, on remarque qu'on a un homomorphisme de restriction injectif

$$Gal(K(\zeta)/K) \hookrightarrow Aut(\mu_m)$$

de $Gal(K(\zeta)/K)$ dans le groupe des automorphismes du groupe μ_m des racines m-ièmes de 1. On laisse en exercice de vérifier que $Aut(\mu_m)$ est abélien ; d'où $Gal(K(\zeta)/K)$ est aussi abélien. Pour $Gal(K'_i(\alpha_i)/K'_i)$, soit $\zeta_i \in K'_i$ une racine primitive d_{i+1}-ième de 1. On remarque qu'on a un homomorphisme injectif

$$Gal(K'_i(\alpha_i)/K'_i) \hookrightarrow \mu_{d_{i+1}}$$

de $Gal(K'_i(\alpha_i)/K'_i)$ dans le groupe $\mu_{d_{i+1}}$ des racines d_{i+1}-ièmes de 1. En effet, un élément $\sigma \in Gal(K'_i(\alpha_i)/K'_i)$ est déterminé par $\sigma(\alpha_i)$ et permute entre elles les racines de $X^{d_{i+1}} - a_i$, qui sont $\alpha_i, \alpha_i\zeta_i, \ldots, \alpha_i{\zeta_i}^{d_{i+1}-1}$. Si $\sigma(\alpha_i) = \alpha_i{\zeta_i}^k$, σ est envoyé sur ${\zeta_i}^k$. On laisse en exercice de vérifier que cela définit bien un homomorphisme injectif. Il s'ensuit aussitôt que $Gal(K'_i(\alpha_i)/K'_i)$ est abélien. Cela termine la démonstration.

La théorie de Galois établit une correspondance biunivoque entre les corps intermédiaires de K_f/K, f séparable, et les sous-groupes de $G_{f/K}$, en associant à un corps intermédiaire $K \subseteq E \subseteq K_f$ le sous-groupe $Gal(K_f/E)$. Les sous-groupes normaux correspondent alors aux corps intermédiaires qui sont eux-mêmes des corps de rupture de polynôme séparable. Cette correspondance permet de traduire des questions sur les corps en des questions sur les groupes. Nous renvoyons à [8].

Nous allons maintenant construire des polynômes rationnels de chaque degré premier $p \geq 5$ et dont le groupe de Galois est le groupe symétrique S_p. Ces polynômes ne sont donc pas résolubles par radicaux.

Lemme 4.72 *Soit $f \in K[X]$ un polynôme irréductible de degré d . Alors $G_{f/K}$ opère transitivement sur les racines de f et d divise l'ordre de $G_{f/K}$.*

Démonstration. Rappelons que nous sommes implicitement en caractéristique zéro de sorte que f possède d racines distinctes $x_1, \ldots, x_d$. On sait qu'il y a un K-isomorphisme $K(x_i) \xrightarrow{\varphi} K(x_j)$ tel que $\varphi(x_i) = x_j$ (corollaire 4.7). Or K_f est aussi le corps de rupture de f à la fois sur $K(x_i)$ et sur $K(x_j)$. Le K-isomorphisme φ se prolonge donc en un K-automorphisme de K_f (proposition 4.25) qui enverra x_i sur x_j. Cela montre que $G_{f/K}$ opère transitivement sur $x_1, \ldots, x_d$, qui constituent donc l'unique orbite de cette action. D'où $d = [G_f : Stab(x_1)]$ et $d \mid |G_{f/K}|$. □

Lemme 4.73 *Soit p un nombre premier et G un sous-groupe du groupe symétrique S_p tel que G contienne un élément d'ordre p et une transposition, alors $G = S_p$.*

Théorème 4.74 *Soit $f \in \mathbb{Q}[X]$ un polynôme rationnel irréductible de degré premier p et qui ait exactement deux racines complexes non réelles, alors son groupe de Galois est le groupe symétrique S_p.*

Démonstration. Par le lemme 4.72 on a $p \mid |G_f|$, et puisque p est premier G_f possède un élément d'ordre p. D'autre part, la restriction de la conjugaison complexe donne un élément de G_f. Puisque f n'a que deux racines non réelles, la conjugaison laisse invariantes les racines réelles et permute les deux racines non réelles. La conjugaison est donc une transposition de G_f vu comme sous-groupe de S_p et on conclut par le lemme précédent. □

Nous indiquons maintenant comment fabriquer des polynômes rationnels qui vérifient les hypothèses du théorème précédent. Cette construction est due à R. Brauer[4]. Nous suivons de près l'exposé de [3]. On prend un nombre entier *positif pair* m, un nombre *impair* $k > 3$, et des entiers *pairs* $n_1 < n_2 < \ldots < n_{k-2}$. Considérons le polynôme

$$g(X) = (X^2 + m)(X - n_1)(X - n_2)\ldots(X - n_{k-2}).$$

Les racines réelles de g sont $n_1, \ldots, n_{k-2}$. Notons que pour tout entier impair h, $\mid g(h) \mid > 2$. Par ailleurs, le graphe de g possède $\frac{k-3}{2}$ maximums relatifs dont la valeur doit toujours être strictement plus grande que 2 par la remarque précédente. Ceci entraîne que le polynôme

$$f(x) = g(X) - 2$$

[4]Richard Brauer, 1901-1977.

possède $\frac{k-3}{2}$ maximums relatifs dans l'intervalle (n_1, n_{k-2}) et ayant tous des valeurs positives. Il s'ensuit que f possède $k-3$ racines réelles dans l'intervalle (n_1, n_{k-2}). Comme $f(n_{k-2}) = -2$ et que f est éventuellement toujours positif à droite de n_{k-2}, f possède aussi une racine réelle plus grande que n_{k-2}. Le polynôme f, qui est de degré k, possède donc au moins $k-2$ racines réelles. Vérifions qu'on peut choisir m de sorte que les deux racines qui restent ne soient pas réelles. Soit $r_i \in \mathbb{C}$ tels que

$$f(x) = (X - r_1) \dots (x - r_k).$$

En comparant nos deux expressions pour f on obtient les relations

$$\sum_{i=1}^{k} r_i = \sum_{s=1}^{k-2} n_s \qquad \sum_{i<j} r_i r_j = \sum_{s<t} n_s n_t + m$$

d'où on tire

$$\sum r_i^2 = (\sum r_i)^2 - 2 \sum_{i<j} r_i r_j = \sum n_s^2 - 2m.$$

Si on prend m assez grand, on obtient $\sum r_i^2 < 0$ ce qui entraîne que les r_i ne sont pas tous réels. Puisque f est un polynôme rationnel ses racines non réelles viennent par paires de racines conjuguées. On se retrouve donc maintenant avec un polynôme rationnel f, et même entier, qui a exactement deux racines non réelles. Posons

$$f(x) = X^k + a_1 X^{k-1} + \dots + a_k.$$

On voit que les a_i doivent être des entiers pairs. Par ailleurs, le terme constant de $f = g - 2$ n'est pas divisible par 4 puisque celui de g l'est. Le critère d'Einsenstein [5] entraîne donc que f est irréductible sur $\mathbb{Q}$. On a donc indiqué comment construire pour chaque entier impair $k \geq 5$ un polynôme rationnel de degré k qui est irréductible et qui ne possède que deux racines non réelles. On peut donc le faire pour chaque nombre premier $p \geq 5$ et obtenir un polynôme rationnel qui n'est pas résoluble. Pour obtenir un polynôme rationnel non résoluble de degré quelconque $d \geq 5$, il suffit de prendre un polynôme rationnel qui n'est pas résoluble f de degré disons 5 et alors $g = X^{d-5} f$ est de degré d et n'est pas résoluble puisqu'il a le même corps de rupture que f.

[5] Ferdinand Eisenstein, 1823-1852.

4.6 Le dix-septième problème de Hilbert

Dans la liste de problèmes que Hilbert présenta au Congrès international des mathématiciens de 1900 à Paris, le dix-septième pose la question suivante : si une fonction rationnelle $f(x_1, \ldots, x_n)$ de n variables à coefficients rationnels ne prends que des valeurs positives ou nulles partout où elle est définie dans $\mathbb{R}^n$, cette fonction doit-elle pouvoir s'exprimer comme une somme de carrés de fonctions rationnelles à coefficients rationnels ? C'est Artin[6] qui apporta une réponse positive en 1927, grâce à la théorie des corps ordonnables développée par lui et Schreier. Il démontre en fait le résultat pour $\mathbb{Q}$ et pour tout autre sous-corps de $\mathbb{R}$ qui possède un seul ordre qui en fasse un corps ordonné, ce qui inclut $\mathbb{R}$ lui-même. On peut mentionner le résultat remarquable de Pfister sur le nombre de carrés nécessaires sur $\mathbb{R}$: il est majoré par 2^n, résultat conjecturé par Ax après avoir montré le cas $n = 3$ (pour $n = 2$, c'est Hilbert, pour $n = 1$, c'est un exercice). Notre exposé de la solution du problème de Hilbert s'inspire du traitement de A. Robinson[7] via la théorie des modèles.

Définition 4.75 *Un* corps ordonné *est un corps muni d'une relation d'ordre total qui est compatible avec les opérations algébriques, c'est-à-dire telle qu'on ait $x > y$ entraîne $x + a > y + a$ et $xb > yb$ si $b > 0$.*

Exemple 4.76

(1) Les nombres rationnels avec l'ordre habituel.

(2) Les nombres réels avec l'ordre habituel.

(3) Tout sous-corps des nombres réels avec l'ordre des nombres réels. Par exemple $\mathbb{Q}(\sqrt{2})$ ou encore $\mathbb{Q}(e)$.

(4) Il ne peut y avoir d'ordre qui ferait des nombres complexes un corps ordonné. En effet, on voit que dans un corps ordonné tout carré d'un élément non nul est strictement positif et on a toujours $1 > 0$ et $-1 < 0$. Or pour le nombre complexe non nul i on a $i^2 = -1$!

On peut remarquer que l'ordre d'un corps ordonné est complètement déterminé dès que les éléments positifs sont déterminés. En effet, si P est un sous-ensemble d'un corps K tel que $0 \notin P$, P est clos par rapport à l'addition et au produit, $P \cap -P = \emptyset$, et $K = P \cup \{0\} \cup -P$, alors la relation $x < y$ définie par $y - x \in P$ est un ordre sur K qui en fait un corps ordonné.

[6] Emil Artin, 1898-1962.

[7] Abraham Robinson, 1918 -1974.

Pour un corps K nous utiliserons la notation $K^\times$ pour désigner $K \setminus \{0\}$, qui est aussi le groupe multiplicatif de$K$.

Définition 4.77 *Un corps est dit* ordonnable *si il peut être muni d'au moins une relation d'ordre qui en fait un corps ordonné.*

Exemple 4.78

(1) Le corps des fractions rationnelles $\mathbb{Q}(T)$ est ordonnable. En effet, puisque e est transcendant sur $\mathbb{Q}$ il existe un $\mathbb{Q}$-isomorphisme de $\mathbb{Q}(T)$ sur $\mathbb{Q}(e)$ qui envoie T sur e. Cet isomorphisme induit un ordre sur $\mathbb{Q}(T)$ qui en fait un corps ordonné. On peut remarquer qu'il y a aussi un $\mathbb{Q}$-isomorphisme qui envoie T sur $-e$ et ce nouvel isomorphisme induit un ordre sur $\mathbb{Q}(T)$ où cette fois on a $T < 0$.

(2) Le corps des nombres complexes n'est pas ordonnable.

Comme on l'a fait remarquer dans l'exemple précédent, il peut y avoir plusieurs ordres possibles qui fassent d'un même corps ordonnable un corps ordonné.

Exemple 4.79 *Un ordre sur le corps des fractions rationnelles réelles $\mathbb{R}(X)$ est complètement déterminé par la coupure de X dans $\mathbb{R}$, c'est-à-dire par les inégalités $a < X < b$, $a, b \in \mathbb{R}$ qui sont vraies pour cet ordre. En effet, il suffit de voir qu'alors le signe de chaque polynôme est déterminé. Or tout polynôme $f \in \mathbb{R}[X]$ se décompose en un produit*

$$f(X) = c(X - a_1)^{r_1} \dots (X - a_m)^{r_m}((X + b_1)^2 + c_1^2)^{s_1} \dots ((X + b_n)^2 + c_n^2)^{s_n}$$

d'une constante réelle c, de facteurs linéaires unitaires et de facteurs quadratiques irréductibles unitaires. On voit que pour déterminer le signe de f il ne reste qu'à déterminer le signe des facteurs linéaires unitaires $X - a_i$, qui sont déterminés par les inégalités données.

L'obstruction qui empêche les nombres complexes d'être ordonnable n'est pas la seule de son espèce.

Proposition 4.80 *Un corps est ordonnable si et seulement si -1 n'est pas une somme de carrés.*

Exemple 4.81 *Tout corps de fractions rationnelles $K(T_1, \dots, T_n)$ sur un corps ordonnable est ordonnable.*

Nous utiliserons un raffinement de la proposition 4.80. On obtient celle-ci en posant $A = \{1\}$ dans la proposition suivante.

Proposition 4.82 *Soit K un corps et A un sous-groupe multiplicatif de $K^\times$. Alors K est ordonnable et il existe au moins un ordre sur K tel que $A > 0$, si et seulement si -1 ne peut s'exprimer sous la forme $\sum a_i x_i^2$, où $a_i \in A, x_i \in K$.*

Démonstration. Une direction est claire. Supposons donc que -1 ne puisse s'exprimer sous la forme $\sum a_i x_i^2$, où $a_i \in A, x_i \in K$. Alors toute somme $\sum a_i x_i^2$, où $a_i \in A, x_i \neq 0$ doit être non nulle. Nous allons obtenir un ordre sur K à partir d'une partie appropriée de $K^\times$ qui en formera les éléments positifs (cf. remarque ci-dessus). Posons

$$P_0 = \{\frac{\sum a_i x_i^2}{\sum a'_j y_j^2} : a_i, a'_j \in A, x_i, y_j \in K, x_i, y_j \neq 0\}$$

Ce sous-ensemble de K possède les propriétés suivantes :

1) P_0 contient toutes les sommes de carrés non nuls de K ;
2) $A \subseteq P_0$;
3) P_0 est un sous-groupe multiplicatif de $K^\times$;
4) $P_0 + P_0 \subseteq P_0$, ou autrement dit P_0 est clos par rapport à l'addition.

On utilise le lemme de Zorn pour obtenir l'ordre voulu. Soit $\mathcal{F}$ la famille des sous-ensembles de K qui possède les propriétés 1),2),3),4) ci-dessus. Alors $(\mathcal{F}, \subseteq)$ est un ensemble inductif. Par le lemme de Zorn, soit P un élément maximal de $\mathcal{F}$.

Lemme 4.83 *Pour tout $x \in K$, non nul, si $-x \notin P$, alors $P_1 = P + Px = \{b + cx : b, c \in P\}$ est un sous-groupe multiplicatif de K qui est clos par rapport à l'addition et qui contient x.*

Démonstration. Notons d'abord que $P_1 \neq \emptyset$, puisque par exemple $1 + x = 1 + 1 \cdot x \in P_1$. On voit directement que P_1 est clos par rapport à l'addition. Par ailleurs, pour $b_1, b_2, c_1, c_2 \in P$, on a

$$(b_1 + c_1 x)(b_2 + c_2 x) = (b_1 b_2 + c_1 c_2 x^2) + (b_1 c_2 + b_2 c_1)x$$

et puisque $b_1 b_2 + c_1 c_2 x^2, b_1 c_2 + b_2 c_1 \in P$, ce produit appartient à P. Aussi, P_1 ne contient pas 0 car $b + cx = 0$ avec $b, c \in P$ entraîne $-x = bc^{-1}$. Il faut voir que P_1 est clos par rapport à l'inverse multiplicatif. Or on a

$$(b + cx)^{-1} = (b + cx)(b + cx)^{-2} = b(b + cx)^{-2} + c(b + cx)^{-2}x$$

qui appartient à P_1 puisque P est un sous-groupe multiplicatif qui contient les carrés non nuls. Ainsi P_1 est bien un sous-groupe multiplicatif et en particulier $1 \in P_1$, disons $1 = b+cx, c, b \in P$. Alors $x = 1 \cdot x = bx+cx^2 \in P_1$. □

On note que $P \subseteq P_1$ puisque $PP_1 \subseteq P_1$ (si $a, b, c \in P$, alors $a(b + cx) = ab + (ac)x \in P_1$). Par le lemme et la maximalité de P, on obtient que pour tout $x \in K$, non nul, $x \in P$ ou $-x \in P$. Ainsi $K = P \cup \{0\} \cup -P$. Comme $0 \notin P$ et que P est clos par rapport à l'addition, on a aussi $P \cap -P = \emptyset$. Il s'ensuit que P fournit l'ordre sur K voulu. □

Les sommes de carrés sont des éléments très particuliers des corps ordonnables.

Théorème 4.84 *Soit K un corps ordonnable. Un élément non nul de K est une somme de carrés si et seulement si cet élément est positif pour tous les ordres de K qui en font un corps ordonné.*

Démonstration. Il est clair qu'une somme de carrés non nuls est positive pour tous les ordres sur K. Il s'agit donc de voir qu'un élément non nul qui n'est pas une somme de carrés peut devenir négatif pour au moins un ordre sur K. Soit donc un élément non nul $a \in K$ qui ne soit pas une somme de carrés, et soit A le sous-groupe multiplicatif de K engendré par $-a$. Je dis que A vérifie les hypothèses de la proposition 4.82. En effet, une relation de la forme

$$-1 = \sum a_i x_i^2 \qquad a_i \in A$$

se ramène, en regroupant les carrés, à une de la forme

$$-1 = -a(\sum y_j^2) + \sum z_i^2$$

où $-a$ doit apparaître car K est ordonnable. Mais alors on aurait

$$a = \frac{(1 + \sum z_i^2)}{(\sum y_j^2)} = \frac{(1 + \sum z_i^2)}{(\sum y_j^2)^2}(\sum y_j^2)$$

et a serait une somme de carrés, ce qui est absurde. D'où, par la proposition 4.82, l'existence d'un ordre qui fasse de K un corps ordonné et pour lequel $-a > 0$, et donc pour lequel $a < 0$. □

Pour exploiter cette caractérisation des sommes de carrés en rapport avec le dix-septième problème de Hilbert, on introduit les notions de corps réel clos et de clôture réelle d'un corps ordonné. Pour mettre en évidence les ordres on désignera un corps ordonné par un couple $(K, <)$ constitué du corps lui-même et de l'ordre $<$.

Définition 4.85 *Un corps est dit* réel clos *si il est ordonnable et possède un seul et unique ordre défini par* $x \geq 0 \leftrightarrow \exists y(y^2 = x)$ *, et cet ordre est tel que tout polynôme qui change de signe aux extrémités d'un intervalle possède une racine dans cet intervalle.*

Exemple 4.86

(1) Les nombres réels forment un corps réel clos.

(2) Les nombres réels algébriques forment un corps réel clos. En effet,les propriétés découlent de celles de $\mathbb{R}$ *et du fait que les nombres réels algébriques sont relativement algébriquement clos dans* $\mathbb{R}$*.*

Voici la propriété fondamentale des corps réels clos que nous allons utiliser.

Théorème 4.87 (Théorème de Sturm) *Soit* R *un corps réel clos,* $f \in R[X]$ *et* $a, b \in R$*, tels que* $a < b$ *et* $f(a)f(b) \neq 0$*. Soit la suite de polynômes suivants associés à* f *:* $f_0 = f$*,* $f_1 = f'$ *le polynôme dérivé de* f*,* $f_{i-1} = g_i f_i - f_{i+1}$ *où* $deg(f_{i+1}) < deg(f_i)$ *;* f_{i+1} *est l'inverse additif du reste de la division euclidienne de* f_{i-1} *par* f_i *de sorte qu'il y a un* s *tel que* $f_{s+1} = 0$*. Alors le nombre de racines (distinctes) de* f *dans l'intervalle* (a, b) *de* R *est donné par* $V_a - V_b$*, où* V_c *est le nombre de variations de signes dans la suite* $f_0(c), f_1(c), \ldots, f_s(c)$*.*

Le théorème de Sturm[8] se démontre comme dans les nombres réels et la démonstration n'utilise que la propriété d'existence des racines pour les polynômes qui changent de signe (voir, par exemple, [8] ou [6] ou [3]).

Définition 4.88 *Soit* $(K, <)$ *un corps ordonné et* R/K *une extension algébrique de* K *telle que* R *soit réel clos et que l'ordre de* R *prolonge l'ordre* $<$ *de* K*. On dit alors que* R *est une* clôture réelle *de* $(K, <)$*.*

Exemple 4.89

(1) Le corps des nombres algébriques réels est une clôture réelle de $\mathbb{Q}$*.*

(2) Soit R *un corps réel clos,* K *un sous-corps de* R *et* K^r *la clôture algébrique relative de* K *dans* R*. Soit* $<$ *l'ordre induit par* R *sur* K*. Alors* K^r *est une clôture réelle de* $(K, <)$*.*

Le lemme suivant assurera l'existence d'une clôture réelle pour chaque corps ordonné.

[8] Charles François Sturm, 1803-1855.

Lemme 4.90 *Soit $(K,<)$ un corps ordonné, $f \in K[X]$ un polynôme irréductible, et $L = K[X]/(f)$. S'il existe $a < b \in K$ tel que $f(a)f(b) < 0$, alors il existe un ordre sur L qui prolonge l'ordre sur K et tel que $a < X + (f) < b$.*

Démonstration. On procède par récurrence sur le degré de f. Soit n le degré de f. On vérifie directement le cas $n = 1$. Pour $n > 1$, supposons qu'il n'y ait pas de tel ordre. Alors par la proposition 4.82, il existe une relation de la forme

$$1 + \sum c_i f_i^2 \in (f)$$

où $f_i \in K[X]$, et $c_i = X - a$ ou $c_i = b - X$ ou $c_i \in K, c_i > 0$. On peut remplacer les f_i par des polynômes r_i de degré strictement plus petit que n. Soit alors $h \in K[X]$ tel que

$$1 + \sum c_i r_i^2 = fh.$$

Il s'ensuit que $n + deg(h) \leq 2n - 1$ et $deg(h) \leq n - 1$. D'autre part en évaluant en a et b on obtient dans $(K,<)$

$$0 < 1 + \sum c_i' a_i^2 = f(a)h(a)$$

$$0 < 1 + \sum d_i' b_i^2 = f(b)h(b).$$

D'où $0 < f(a)f(b)h(a)h(b)$ et ainsi $h(a)h(b) < 0$. Il existe alors un facteur irréductible $g \in K[X]$ de h tel que $g(a)g(b) < 0$. Par récurrence, il existe un ordre sur $L' = K[X]/(g)$ qui prolonge l'ordre sur K et tel que $a < X + (g) < b$. Mais cela contredit alors la relation $1 + \sum c_i r_i^2 = fgh_1 = 0$ dans L'. Ceci complète la récurrence. □

Théorème 4.91 *(1) Tout corps ordonné possède une clôture réelle.*
(2) Soit R_1 et R_2 deux clôtures réelles d'un corps ordonné $(K,<)$, alors R_1 et R_2 sont K-isomorphes par un unique isomorphisme qui respecte l'ordre sur K.

Démonstration. Soit $(K,<)$ un corps ordonné.
(1) Dans une clôture algébrique fixée de K, on vérifie à l'aide du lemme de Zorn qu'il existe une extension algébrique maximale de K qui soit ordonné avec un ordre qui prolonge l'ordre donné sur K, disons $(R,<)$. Par le lemme précédent, tout polynôme qui change de signe aux extrémités d'un intervalle possède une racine dans cet intervalle. En considérant les polynômes $X^2 - a$, $a > 0$, on voit que l'ordre est défini par les carrés. Ainsi, R est une clôture

réelle de $(K, <)$.
(2) Soit R_1,R_2 deux clôtures réelles de $(K, <)$. On peut remarquer d'abord que tout K-isomorphisme de R_1 dans R_2 respectera l'ordre ambiant puisque dans chacun des R_i l'ordre est défini par les carrés. Quant à l'unicité d'un tel K-isomorphisme, on peut remarquer qu'un élément $x \in R_1$ est racine de son polynôme minimal sur K, disons f. Or un K-isomorphisme devra envoyer x sur une racine de f dans R_2 et fera aussi en sorte que f a le même nombre de racines dans R_1 que dans R_2 ; il induira donc une bijection entre les racines de f de chaque côté et comme cette bijection doit préserver l'ordre il ne peut y en avoir qu'une possible. Ceci montre alors que l'image de x est complètement déterminée, d'où l'unicité de l'isomorphisme cherché. Pour le trouver, par le lemme de Ax, il suffit de montrer que tout polynôme $f \in K[X]$ possède une racine dans R_1 si et seulement si il en a une dans R_2. Soit donc $f \in K[X]$, qu'on peut supposer unitaire, disons $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$. On vérifie que dans toute extension ordonnée de K qui prolonge l'ordre sur K, les racines de f sont comprises dans l'intervalle $(-M, M)$, où $M = 1 + |a_{n-1}| + \ldots + |a_0| \in K$. Mais alors, par le théorème de Sturm, le nombre de racine de f dans R_1 et dans R_2 est le même et égal à $V_{-M} - V_M$. □

Soit R un corps réel clos . En utilisant la formule quadratique et le fait que tout élément positif de R possède une racine carrée, on obtient que $R(i)$ ne possède aucune extension quadratique, ou encore que tout élément de $R(i)$ est un carré. En fait, $R(i)$ est carrément algébriquement clos. Ceci se démontre comme pour les nombres réels, en n'utilisant que la propriété d'existence des racines pour les polynômes qui changent de signe (voir, par exemple, [8], chap. IX, p.155). Ce résultat entraîne qu'un corps ordonnable qui est réel clos ne possède aucune extension algébrique propre ordonnable ; et vice versa, par le lemme 4.90.

Théorème 4.92 *Soit R un corps réel clos et $R(i)/R$ l'extension algébrique où $i^2 + 1 = 0$. Alors $R(i)$ est un corps algébriquement clos. En particulier, les seuls polynômes unitaires irréductibles de $R[X]$ sont les polynômes de degré un et les polynômes quadratiques de la forme $(X + b)^2 + c^2$.*

Corollaire 4.93 *Soit R un corps réel clos. Un ordre sur le corps des fractions rationnelles $R(X)$ est complètement déterminé par la coupure de X dans R, c'est-à-dire par les inégalités $a < X < b$, $a, b \in R$ qui sont vraies pour cet ordre.*

Proposition 4.94 *Soit R'/R une extension de corps réels clos et $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$. Si l'inéquation $f(X_1, \ldots, X_n) < 0$ possède une solution dans R', alors elle en possède déjà une dans R.*

Démonstration. Supposons donc que $f(X_1, \ldots, X_n) < 0$ possède une solution $x_1, \ldots, x_n$ dans R'. Considérons la suite

$$R \subseteq R(x_1)^r \subseteq R(x_1, x_2)^r \subseteq \ldots \subseteq R(x_1, \ldots, x_n)^r \subseteq R'$$

où ^{r} désigne le passage à la clôture réelle comme dans l'exemple 4.89. Cela nous donne une suite croissante de corps réel clos R_j telle que $f(X_1, \ldots, X_n) < 0$ a une solution dans le dernier corps de la suite, et le degré de transcendance de R_{j+1} sur R_j est 1. On peut donc supposer que le degré de transcendance de R' sur R est 1 puisque si on établit le résultat dans ce cas, alors, de proche en proche, $f(X_1, \ldots, X_n) < 0$ aura une solution dans tous les R_j et donc dans R. Dans ce cas, fixons $t \in R' \setminus R$. Ce t est alors transcendant sur R et l'ordre induit sur $R(t)$ est déterminé par les inégalités $a < t < b$, $a, b \in R$, vraies dans R' (cf. l'exemple 4.79). Notons que R' est une clôture réelle de $R(t)$. Par le théorème 4.91, le type d'isomorphisme de corps ordonné de R' sur $(R(t), <)$ est aussi déterminé par ces inégalités. Ceci fait en sorte que $f(X_1, \ldots, X_n) < 0$ aura une solution dans toute extension réelle close R'' de R qui possède un élément u satisfaisant aux mêmes inégalités ci-dessus que t, puisque R'' contient alors un sous-corps réel clos qui est R-isomorphe à R', à savoir la clôture algébrique relative de $R(u)$ dans R''.

Lemme 4.95 *Il existe un sous-ensemble fini des inégalités $a < t < b$ qui possède la même propriété, c'est-à-dire tel que $f(X_1, \ldots, X_n) < 0$ aura une solution dans toute extension réelle close R'' de R qui possède un élément satisfaisant ces inégalités.*

Ce lemme permet alors de conclure puisque, étant donné un nombre fini d'inégalités

$$a_1 < t < b_1, \quad a_2 < t < b_2, \quad \ldots \quad a_n < t < b_n$$

on se ramène à une seule

$$a < t < b$$

où $a = \max a_i$ et $b = \min b_j$, et alors par exmple $t_0 = \frac{a+b}{2} \in R$ est tel que $a < t_0 < b$. Par le lemme, $f(X_1, \ldots, X_n) < 0$ a aussi une solution dans R.

Démonstration du lemme. Soit T une nouvelle variable et posons

$$I = \mathcal{P}_f(\{a < T < b : a, b \in K \text{ et } a < t < b \text{ est vrai dans } R'\})$$

$$F_0 = \{X \in \mathcal{P}(I) : \exists i_0 \in I, x \in X \leftrightarrow i_0 \subseteq x\}$$

$$J = \{Y \in \mathcal{P}(I) : \exists X \in F_0, X \cap Y = \emptyset\}$$

On procède par l'absurde. Supposons donc que pour chaque $i \in I$ il y ait une extension réelle close R_i de R et un $u_i \in R_i$ qui satisfait les inégalités qui se trouvent dans i, mais que $f(X_1, \ldots, X_n) < 0$ n'ait pas de solution dans R_i. On vérifie que J est un idéal propre de l'anneau de Boole $\mathcal{P}(I)$ (voir chapitre 2). Soit $\mathcal{M}$ un idéal propre maximal de $\mathcal{P}(I)$ contenant J. Considérons l'anneau produit

$$\prod_{i \in i} R_i$$

et posons

$$M = \{(x_i)_{i \in I} \in \prod_{i \in I} R_i : \{i \in I : x_i = 0\}^c \in \mathcal{M}\}$$

On vérifie que M est un idéal propre maximal de $\prod_{i \in i} R_i$. Posons $R^* = \prod_{i \in i} R_i/M$. C'est un corps, qui est une extension de R par le plongement diagonal $a \mapsto (a)_{i \in I} + M$.

Lemme 4.96 *Le corps R^* est réel clos.*

Démonstration. 1) *Les carrés définissent un ordre.* Posons P égal à l'ensemble des carrés non nuls de R^*.
1.1) P est clos par rapport au produit : clair.
1.2) $P \cap -P = \emptyset$. En effet, si $x = y^2 = -z^2$, disons $x = (x_i) + M$ etc., alors $\{i \in I : x_i \neq 0\} \subseteq \{i \in I : x_i = y_i^2 = -z_i^2\}^c \in \mathcal{M}$, d'où $\{i \in I : x_i \neq 0\} \in \mathcal{M}$ et $x = 0$. Ceci assure que $P \cap -P = \emptyset$.
1.3) $R^* = P \cup \{0\} \cup -P$: soit $x = (x_i) + M$, et posons $y_i = \sqrt{x_i}$, si $x_i > 0$ dans R_i, $y_i = 0$, si $x_i = 0$, et $y_i = \sqrt{-x_i}$, si $x_i < 0$ dans R_i. Alors on a

$$I^c = (\{i \in I : x_i > 0\} \cup \{i \in I : x_i = 0\} \cup \{i \in I : x_i < 0\})^c$$

$$\emptyset = \{i \in I : x_i > 0\}^c \cap \{i \in I : x_i = 0\}^c \cap \{i \in I : x_i < 0\}^c \in \mathcal{M}$$

d'où

$$\{i \in I : x_i > 0\}^c \in \mathcal{M} \text{ ou } \quad \{i \in I : x_i = 0\}^c \in \mathcal{M} \text{ ou } \quad \{i \in I : x_i < 0\}^c \in \mathcal{M}.$$

Par exemple, si $\{i \in I : x_i > 0\}^c \in \mathcal{M}$, alors $\{i \in I : x_i = y_i^2\}^c \in \mathcal{M}$ et $x = y^2$, où $y = (y_i) + M$.
1.4) P est clos par rapport à l'addition : considérons une somme de deux carrés $x^2 + y^2$. Si elle est nulle, l'argument fait en (1.2) entraîne $x = y = 0$.

Si elle est égale à moins un carré, c'est- à-dire $x^2 + y^2 = -z^2$, alors comme en (1.2) ceci entraîne $x = y = z = 0$. D'où le résultat.

Ces quatre propriétés assurent que les carrés définissent bien un ordre sur R^* qui en fait un corps ordonné.

2) *Un polynôme qui change de signe aux extrémités d'un intervalle y a une racine.* Soit un polynôme $g \in R^*[X]$ et $a, b \in R^*$, $a < b$ tels que $g(a)g(b) < 0$. Disons $a = (a_i) + M$, $b = (b_i) + M$, $g = (g_i) + M$ au sens naturel, où $g_i \in R_i[X]$. On peut remarquer que $g(a)g(b) = (g_i(a_i)g_i(b_i)) + M$. Ceci entraîne que $\{i \in I : g_i(a_i)g_i(b_i) < 0\}^c \in \mathcal{M}$. Pour chaque i tel que $g_i(a_i)g_i(b_i) < 0$ soit $x_i \in R_i$ tel que $a_i < x_i < b_i$ et $g_i(x_i) = 0$, et pour les autres i posons $x_i = 1$. Alors on a

$$\{i \in I : a_i < x_i < b_i \text{ et } g_i(x_i) = 0\} \supseteq \{i \in I : g_i(a_i)g_i(b_i) < 0\}$$

$$\{i \in I : a_i < x_i < b_i \text{ et } g_i(x_i) = 0\}^c \subseteq \{i \in I : g_i(a_i)g_i(b_i) < 0\}^c \in \mathcal{M}$$

d'où

$$\{i \in I : a_i < x_i < b_i \text{ et } g_i(x_i) = 0\}^c \in \mathcal{M}$$

ce qui entraîne que $a < x < b$ et $g(x) = 0$ dans K^*. □

Posons $u = (u_i) + M$. Soit une inégalité $a < T < b$ de I. On peut remarquer que

$$\{i \in I : a < u_i < b\} \supseteq \{i \in I : \{a < T < b\} \subseteq i\} \in F_0$$

d'où

$$\{i \in I : a < u_i < b\}^c \subseteq \{i \in I : \{a < T < b\} \subseteq i\}^c \in \mathcal{M}$$

ce qui entraîne que $a < u < b$ dans R^*. Ainsi u satisfait *toutes* les inégalités $a < T < b$ satisfaites par t dans R'. D'autre part, soit $x_1, \ldots, x_n \in R^*$, disons $x_j = (x_{ji}) + M$. On a $\{i \in I : f(x_{1i}, \ldots, x_{ni}) \geq 0\} = I$, et donc $\{i \in I : f(x_{1i}, \ldots, x_{ni}) \geq 0\}^c = \emptyset \in \mathcal{M}$, ce qui entraîne que $f(x_1, \ldots, x_n) \geq 0$ dans R^*. Il s'ensuit que $f(X_1, \ldots, X_n) < 0$ n'a aucune solution dans R^*. Mais ceci contredit la propriété de l'ensemble des inégalités $a < t < b$ puisque u est un élément de R^* qui les satisfait toutes. Ceci conclut la démonstration du lemme et de la proposition.

Nous pouvons maintenant donné la solution du problème de Hilbert. Soit $f(X_1, \ldots, X_n)$ une fonction rationnelle à coefficients dans $\mathbb{Q}$ et telle que $\forall x \in \mathbb{R}^n, f(x) \geq 0$, partout où elle est définie. Considérons le corps ordonnable $\mathbb{Q}(X_1, \ldots, X_n)$, il suffit de montrer que f est positif pour tout ordre sur $\mathbb{Q}(X_1, \ldots, X_n)$ qui en fasse un corps ordonné. Supposons que ce ne soit pas le cas et soit un ordre $<$ sur $\mathbb{Q}(X_1, \ldots, X_n)$ tel que $f < 0$. Soit

R' la clôture réelle de $\mathbb{Q}(X_1, \ldots, X_n)$ pour cet ordre. Alors $X_1, \ldots, X_n \in R'$ forment une solution de l'inéquation $f(x_1, \ldots, x_n) < 0$. Or R' est aussi une extension des nombres réels algébriques, qui forment la clôture réelle de $\mathbb{Q}$. Par la proposition 4.94, $f(x_1, \ldots, x_n) < 0$ a aussi une solution dans les nombres réels algébriques, ce qui est absurde.

Chapitre 5

Exercices

5.1 Lemme de Zorn

5.1.1

(**Axiome du choix $\Rightarrow$ lemme de Zorn**) Soit $(E, \leq)$ un ensemble partiellement ordonné non vide, τ une fonction de choix sur E, c'est-à-dire une fonction $\tau : P^*(E) \to E$ telle que $\tau(Y) \in Y$ pour tout Y.

Définition. Une chaîne A de E est appelée une τ-*chaîne*, si pour tout segment initial [1] S de $A, S \neq A$, on a que $min(A \backslash S)$ existe et est égal à $\tau(M_S)$, où $M_S = \{x \in E : x > y, \forall y \in S\}$, l'ensemble des majorants stricts de S dans E.

Par exemple, $\{\tau(E)\}$ est une $\tau-$chaîne qui est un segment initial de toutes les autres (à cause du segment initial $S = \emptyset$). Montrez les lemmes suivants.

(a) *Lemme 1.* Toute $\tau-$ chaîne est bien ordonnée par $\leq$. (Aide : soit A une $\tau-$chaîne et $X \subseteq A, X \neq \emptyset$; vérifiez que $S = \{a \in A : a < x, \forall x \in X\}$ est un segment initial de A et $S \neq A$.)

(b) *Lemme 2.* Soit A, A' deux τ-chaînes. Alors A est un segment initial de A' ou A' est un segment initial de A. (Aide : soit

$$S_0 = \bigcup \{S : S \text{ est un segment initial de } A \text{ et } A'\}$$

vérifiez que S_0 est un segment initial de A et A' et qu'on doit avoir $S_0 = A$ ou $S_0 = A'$.)

[1] C'est-à-dire, pour tout $x \in S$ et $y \in A, y \leq x$ entraîne $y \in S$. L'ensemble vide est, par défaut, un segment initial.

(c) *Lemme 3.* Soit $A_\infty = \bigcup\{A : A \text{ est une } \tau\text{-chaîne}\}$. Alors (1) A_∞ est une τ-chaîne et (2) A_∞ n'a pas de majorant strict. (Aide : (1) soit S un segment initial de $A_\infty, S \neq A_\infty, x \in A_\infty \backslash S, A$ une τ-chaîne telle que $x \in A$. Utilisez le lemme 2 pour vérifiez que $S \subset A$; (2) considérer $M = \{x \in E : x > y, \forall y \in A_\infty\}$.

(d) *Lemme 4.* Si $(E, \leq)$ est inductif, alors il possède au moins un élément maximal. (Aide : considérer A_∞.)

5.1.2

Soit I un ensemble non vide. On dit que $\mathcal{F} \subseteq \mathcal{P}(I)$ est un *filtre propre* sur I si

(1) $\emptyset \notin \mathcal{F}, I \in \mathcal{F}$

(2) $F_1, F_2 \in \mathcal{F} \Rightarrow F_1 \cap F_2 \in F$

(3) $F_1 \subseteq F_2$ et $F_1 \in \mathcal{F} \Rightarrow F_2 \in \mathcal{F}$

On dit que $\mathcal{F}$ est un *ultrafiltre* si $\mathcal{F}$ est un filtre propre tel que pour tout $F \in \mathcal{P}(I), F \in \mathcal{F}$ ou $I \backslash F \in \mathcal{F}$. Montrez qu'un filtre propre est un ultrafiltre si et seulement si il est maximal par rapport à l'inclusion. Montrez que tout filtre propre sur I est inclus dans au moins un ultrafiltre.

5.1.3

Soient D, G, H des groupes abéliens tels que $H \subset G$ et D est *divisible*, c'est-à-dire que pour tout entier $n \geq 2$ et tout $y \in D$ il existe au moins un $z \in D$ tel que $n.z = y$. Montrez que tout homomorphisme $f : H \to D$ se prolonge en un homomorphisme $\bar{f} : G \to D$.

5.2 Catégories et foncteurs

5.2.1

Dans les catégories de structures mathématiques vérifiez qu'une flèche qui est une section est toujours une application injective, et qu'une flèche qui est une rétraction est toujours une application surjective. N.B. On n'a pas en général les réciproques.

5.2.2

Soit I un ensemble infini et $\mathcal{F}r = \{X \in \mathcal{P}(I) : I \backslash X \text{ est fini}\}$.

(a) Vérifiez que $\mathcal{F}r$ est un filtre propre sur I (voir l'exercice 5.1.2).

(b) Soit $\mathcal{F}$ un ultrafiltre fixé tel que $\mathcal{F}r \subseteq \mathcal{F}$, A un anneau unitaire commutatif, A^I l'anneau des fonctions de I dans A, et

$$J_{\mathcal{F}} = \{f \in A^I : \{i \in I : f(i) = 0\} \in \mathcal{F}\}$$

Vérifiez que $J_{\mathcal{F}}$ est un idéal de A^I.

(c) Soit $\mathcal{F}$ comme en (b). Vérifiez que la correspondance $A \mapsto A^I/J_{\mathcal{F}}$ induit de façon naturelle un foncteur $F : \mathcal{ANN} \to \mathcal{ANN}$. On l'appelle *le foncteur ultrapuissance* associé à $\mathcal{F}$.

(d) Même notation qu'en (c). Montrez que si A est un corps, alors $F(A)$ aussi.

(e) Même notation qu'en (c). Soit K un corps et posons $K^* = F(K)$. L'application *diagonale* qui associe à chaque $x \in K$ la fonction constante correspondante de K^I est un homomorphisme. On obtient donc un homomorphisme injectif $K \hookrightarrow K^*$ et on peut identifier K à un sous-corps de K^* par ce plongement. Soit un système polynomial $f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0, g(x_1, \ldots, x_n) \neq 0$, où $f_i, g \in K[X_1, \ldots, X_n]$. Montrez que ce système polynomial possède une solution à valeurs dans K si et seulement si il possède une solution à valeurs dans K^* (en considérant $K \subseteq K^*$ comme ci-dessus).

5.2.3

Soit $\mathcal{C}$ une catégorie ayant la propriété que pour toute flèche f il existe des flèches g, h telles que $f = hg$, g est une rétraction et h est une section. Démontrez que toute catégorie $\mathcal{D}$ équivalente à $\mathcal{C}$ possède la même propriété.

5.2.4

(1) Vérifiez que $\mathcal{P} : \mathcal{ENS} \to \mathcal{ENS}$ tel que défini à l'exemple 2.30 est bien un foncteur contravariant.

(2) Soit $\mathcal{C}$ une catégorie tel que pour tous objets A, B , $Hom_{\mathcal{C}}(A, B)$ est un ensemble (par exemple $\mathcal{GR}$). Fixons un objet A de $\mathcal{C}$. Vérifiez que $\mathrm{h}_A : \mathcal{C} \to \mathcal{ENS}$ tel que défini à l'exemple 2.30 est bien un foncteur contravariant.

5.2.5

Soit $F, G : \mathcal{C} \to \mathcal{D}$ deux foncteurs et $\eta : F \to G$ une transformation naturelle telle que pour tout objet A de $\mathcal{C}$, η_A est un isomorphisme. Montrez que η est un isomorphisme de foncteurs.

5.2.6

Soit $\mathcal{P} : \mathcal{ENS} \to \mathcal{ENS}$ le foncteur contravariant *ensemble des parties* déjà vu. Vérifiez que le foncteur contravariant $\mathcal{P}$ est isomorphe au foncteur contravariant $h_{\mathbf{2}}$, où $\mathbf{2} = \{0, 1\}$, c'est-à-dire trouvez des transformations naturelles $\eta : \mathcal{P} \to h_{\mathbf{2}}$ et $\xi : h_{\mathbf{2}} \to \mathcal{P}$ telles que $\eta\xi = 1_{h_{\mathbf{2}}}$ et $\xi\eta = 1_{\mathcal{P}}$. (On dit que $\mathcal{P}$ est *représentable*, et qu'il est *représenté* par $\mathbf{2}$.)

5.2.7

Pour un groupe fixé G on définit la catégorie des G-ensembles, notée $G - \mathcal{ENS}$: un objet est un couple $(X, \circ)$ formé d'un ensemble X et d'une action à gauche $G \times X \xrightarrow{\circ} X$ de G sur X ; une flèche $(X_1, \circ) \xrightarrow{f} (X_2, \circ)$ est donnée par une fonction $f : X_1 \to X_2$ qui préservent l'action de G, c'est-à-dire telles que $f(g \circ x) = g \circ f(x), \forall g \in G, \forall x \in X_1$. Soient G, H des groupes et $\varphi : G \to H$ un homomorphisme. Soit $\varphi^* : H - \mathcal{ENS} \to G - \mathcal{ENS}$ définie par $\varphi^*(X, \circ) = (X, \circ_\varphi)$, où $\circ_\varphi$ désigne l'action de G définie par $g \circ_\varphi (x) = \varphi(g) \circ x$ et $\varphi^*(f) = f, f$ vue comme application.

(a) Vérifiez que φ^* est un foncteur.

(b) Vérifiez que si φ est un isomorphisme, alors φ^* est une équivalence.

(c) Montrez que si φ^* est essentiellement surjectif, alors φ est injectif (N.B. $g_0 \in G$ est l'élément neutre si $\forall g \in G, g_0 g = g$).

(d) Montrez que si φ^* est plein et fidèle, alors φ est surjectif. (Aide : considérez $Hom_{H-\mathcal{ENS}}(\{1\}, Y)$, où Y est l'ensemble des translatés à gauche de $\varphi(G)$ sur lequel H opère par translation à gauche.)

Ainsi, par (a),(b),(c),(d), φ est un isomorphisme si et seulement si φ^* est une équivalence.

5.2.8

(a) Soit A une algèbre de Boole et $\mathcal{C}(S(A), \mathbf{2})$ l'anneau des fonctions continues de $S(A)$ dans $\mathbf{2}$. Vérifiez que l'application

$$\acute{e}v : A \to \mathcal{C}(S(A), \mathbf{2})$$

qui associe à chaque élément $a \in A$ la fonction d'évaluation en a, est un isomorphisme d'anneaux.
(b) Vérifiez que l'homomorphisme diagonal

$$\delta : A \longrightarrow \prod_{M \in S(A)} A/M$$

défini par $\delta(a) = (a + M)_{M \in S(A)}$, est injectif.

5.3 Modules

5.3.1

Il y a correspondance biunivoque entre les A-modules à gauche et les homomorphismes d'anneaux de A dans les anneaux d'endomorphismes de groupes abéliens. À un A-module à gauche M on associe l'homomorphisme $\rho_M : A \to End(M, +)$, qui associe à chaque $a \in A$ son action sur M. À chaque homomorphisme d'anneaux unitaires $\rho : A \to End(M, +)$, où M est un groupe abélien, on associe la structure de A-module à gauche $A \times M \to M$ donnée par $am = (\rho(a))(m)$. Vérifiez d'abord ces procédés et ensuite qu'ils sont inverses l'un de l'autre.

5.3.2

Définition. Soit A un anneau commutatif et M un A-module. On dit que $x \in M$ est un *élément de torsion* si il existe $a \in A, a \neq 0$ tel que $ax = 0$. On dit que M est *sans torsion* s'il ne possède aucun élément de torsion non nul et on dit que M est un module de torsion si tous ses éléments non nuls sont de torsion. On définit

$$ann(M) = \{a \in A : \forall x \in M, ax = 0\}$$

On peut vérifier que c'est un idéal de A.

(a) Vérifiez que si A est un anneau intègre[2], alors les éléments de torsion d'un A-module M forment un sous-module, disons T (appelé le module de torsion de M), et que M/T est un module sans torsion.

(b) Vérifiez que tout module libre sur un anneau intègre est sans torsion.

[2]C'est-à-dire commutatif et où le produit de deux éléments non nuls est non nul.

5.3.3

Soit A un anneau principal[3] et N un A-module de torsion de type fini tel que $ann(N) = (p^n)$, où $p \in A$ est irréductible. Posons $N = \langle x, y_1, \ldots, y_k \rangle$, où on peut supposer que $ann(\langle x \rangle) = (p^n)$.

(a) Vérifiez que pour tout sous-module $N' \subset N, ann(N')$ est de la forme (p^i), où $0 \leq i \leq n$.

(b) Montrez que N est une somme directe finie de modules cycliques : par induction sur le nombre de générateurs (1) considérez $N/\langle x \rangle$ et l'hypothèse d'induction pour obtenir une somme $N = \langle x \rangle + \langle x_1 \rangle + \ldots + \langle x_s \rangle$, telle que $p^{n_i}.x_i \in \langle x \rangle$, où $0 \leq n_i \leq n$; (2) disons $p^{n_i}.x_i = a_i x$, vérifiez que $p^{n-n_i} a_i \in ann(\langle x \rangle)$; (3) disons $p^{n-n_i} a_i = t_i p^n$ et posons $z_i = x_i - t_i.x$, vérifiez que $N = \langle x \rangle \oplus \langle z_1 \rangle \oplus \ldots \oplus \langle z_s \rangle$.

5.3.4

Soit A un anneau principal et N un A-module de torsion de type fini.

(a) Montrez que si N est cyclique et $ann(N) = (p^n)$, pour un élément irréductible $p \in A$, alors N est indécomposable.

(b) Montrez que si N est indécomposable, alors N est cyclique et $ann(N) = (p^n)$, pour un élément irréductible $p \in A$. (Aide : (1) vérifiez que $ann(N)$ est non nul ; (2) disons $ann(N) = (a)$, et supposons $a = b_1 b_2$, avec $b_1 b_2$, non inversibles et relativement premiers, vérifiez qu'on aurait alors $N = N_1 \oplus N_2$, où $N_i = \{b_1.x : x \in N\}$; (3) concluez en utilisant l'exercice précédent.)

5.3.5

Soit A un anneau principal.

(a) Montrez que si M est un A-module libre de rang r, alors tout sous-module de M est libre de rang au plus r. Procédez par induction sur le rang :

(1) Vérifiez pour $r = 1$.

(2) Soit N un sous-module et $x_1, \ldots, x_r$ une base de M, considérez $N' = N \cap \langle x_2, \ldots, x_r \rangle$ et la suite exacte

$$0 \to N' \to N \to N/N' \to 0$$

[3] Anneau principal : intègre et où tout idéal est principal, c'est-à-dire de la forme (x).

(b) Vous allez montrer que si M est un A-module sans torsion de type fini, alors M est libre de rang fini. (1) Utilisez le fait que M est noethérien pour montrer qu'il existe un sous-ensemble fini linéairement indépendant maximal ; soit L le sous-module engendré par cet ensemble ; (2) montrez que $ann(M/L)$ est un idéal non nul ; (3) disons $ann(M/L) = (t)$, montrez que l'application $f(x) = tx$ est un homomorphisme injectif de M dans L et utilisez (a) pour conclure.

(c) Vérifiez que pour $a \in A$, non nul, le A-module $A/(a)$ est artinien. (Aide : A est un anneau factoriel.)

(d) Soit M un A-module de type fini et T son module de torsion. Montrez que T est artinien : (1) vérifiez que T est de type fini ; (2) considérez $ann(T)$ et utilisez (c) pour montrer que T est l'image d'un A-module artinien.

(e) Soit M un A-module de type fini. Montrez que M est isomorphe à une somme directe d'un A-module libre de rang fini et d'un nombre fini de A-modules de torsion de type fini indécomposables et que cette représentation est essentiellement unique au sens suivant : soit T son module de torsion, montrez que M est isomorphe à $M/T \oplus T$ et utilisez le théorème de Krull-Schmidt.

N.B. On peut montrer directement (exercice précédent) que les A-modules de torsion de type fini indécomposables sont les modules cycliques N tels que $ann(N) = (p^n)$, où p est un élément irréductible de A. Ainsi, on obtient le théorème classique de structure des modules de type fini sur un anneau principal. En particulier, pour les groupes abéliens de type fini ($A = \mathbb{Z}$).

5.3.6

Montrez que la propriété universelle du théorème 3.14 caractérise la donnée du produit et de ses projections $(\prod_{i\in I} M_i, (p_i)_{i\in I})$ à isomorphisme près. De même, pour la somme avec ses injections $(\bigoplus_{i\in I} M_i, (\iota_i)_{i\in I})$.

5.3.7

Montrez que si A est un anneau unitaire noethérien, alors il ne peut exister d'entiers distincts m, n tels que les A-modules libres $A^{(m)}$ et $A^{(n)}$ soient isomorphes. Déduisez alors qu'il ne peut y avoir de A-module libre ayant des bases finies de cardinalité différentes.

5.3.8

Soit R un anneau unitaire, M le R-module $R^{(\mathbb{N})}$, et A l'anneau des endomorphismes de R-module de M. La fonction identité forme une base du A-module ${}_AA$. D'autre part, soit $(e_n)_{n\in\mathbb{N}}$ la base canonique du R-module M et soient f, g les éléments de A définis par les conditions suivantes : $f(e_{2n}) = e_n, f(e_{2n+1}) = 0, g(e_{2n}) = 0, g(e_{2n+1}) = e_n, n \geq 0$. Vérifiez que f, g forment une base du A-module ${}_AA$ (!).

5.3.9

Soit p un nombre premier fixé et

$$\mathbb{Z}(p^\infty) = \{z \in \mathbb{C} : \exists n \geq 1, z^{p^n} = 1\}$$

C'est un sous-groupe multiplicatif de $\mathbb{C}$. Vérifiez que les seuls sous-groupes propres de $\mathbb{Z}(p^\infty)$ sont les sous-groupes finis de la forme $\{z \in \mathbb{C} : z^{p^n} = 1\}$, où $n \geq 1$, et déduisez alors que $\mathbb{Z}(p^\infty)$ est un $\mathbb{Z}$-module indécomposable.

5.3.10

Soit M et f comme dans le lemme de Fitting et supposons $M = M_0 \oplus M_1$ tel que M_i est envoyé dans lui-même par f, $f|M_0$ est nilpotent, et $f|M_1$ est un automorphisme de M_1. Montrez que $M_0 = f^{-\infty}(0)$ et $M_1 = f^\infty(M)$.

5.3.11

Soit K un corps et A l'ensemble des matrices carrées triangulaires d'ordre n sur K du type

$$\begin{bmatrix} c & 0 & \dots & 0 \\ * & c & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots \\ * & * & * & c \end{bmatrix}$$

Montrez que A est un anneau local.

5.3.12

Soit A un anneau principal et M un A-module libre. Soit B une base de M et N un sous-module de M. Pour $x \in M$, disons $x = \lambda_1 w_1 + \ldots + \lambda_n w_n, \lambda_i \in A, \lambda_i \neq 0, w_i \in B$, posons $supp(x) = \{w_1, \ldots, w_n\}$ et appelons cet ensemble le *support* de x.

(a) Supposons $X \subseteq N, X \neq \emptyset$, tel que X est linéairement indépendant et $\langle B_X \rangle \cap N = \langle X \rangle$, où $B_X = \{w \in B : \exists x \in X, w \in supp(x)\}$, et supposons aussi $\langle X \rangle \neq N$.

(a.1) Montrez que si $z \in N \backslash \langle X \rangle$, alors $X \cup \{z\}$ est linéairement indépendant.

(a.2) Soit

$$Z_N = \{z \in N \backslash \langle X \rangle : supp(z) \backslash B_X \text{ a cardinalité minimale}\}$$

$$C_N = \{\lambda \in A : \exists z \in Z_N, \lambda \text{ est coefficient d'un } w \in supp(z) \backslash B_X\}$$

Prenons $\lambda \in C_N$ avec un nombre minimum de facteurs irréductibles et un $z = \lambda w_1 + \ldots + \lambda_n w_n$ correspondant. Montrez que $\langle B_{X \cup \{z\}} \rangle \cap N = \langle X \cup \{z\} \rangle$. (Aide : soit $v \in \langle B_{X \cup \{z\}} \rangle \cap N$, disons $v = \lambda'_1 w_1 + \ldots + \lambda'_k w'_k, \lambda'_i \in A, w'_i \in B$; montrez que λ doit diviser λ'_1, disons $\lambda'_1 = a\lambda$, et alors $v - az \in \langle X \rangle$)

(b) Utilisez (a) pour montrer que N est un A-module libre.

Ainsi tout sous-module d'un module libre sur un anneau principal est lui-même libre.

5.3.13

Soit M le $\mathbb{Z}$-module $\mathbb{Z}^{\mathbb{N}}$. Pour $k \in \mathbb{Z}$, $k \neq 0$, disons $k = 3^n k_0$, où 3 ne divise pas k_0, on définit $v_3(k) = n$. Soit S le sous-module suivant, $S = \{(x_n)_{n \geq 0} \in M : \lim_{n \to \infty} v_3(x_n) = +\infty\} \cup \{(0)_{n \geq 0}\}$.

(a) Vérifiez que la fonction $\varphi((x_n)_{n \geq 0}) = (3^{n+1} x_n)_{n \geq 0}$ définit un homomorphisme injectif de $\mathbb{Z}$-modules de M dans S.

(b) Vérifiez que S ne peut avoir de base dénombrable comme $\mathbb{Z}$-module.

(c) Soit le sous-module $3S = \{3x : x \in S\}$, alors le $\mathbb{Z}$-module quotient $S/3S$ a une structure naturelle d'espace vectoriel sur $\mathbb{F}_3$ (le corps à trois éléments). Montrez que $S/3S$ possède une base dénombrable comme espace vectoriel sur $\mathbb{F}_3$.

(d) Déduisez de (b) et (c) que S ne peut être un $\mathbb{Z}$-module libre.

N.B. Ainsi par le numéro précédent, le $\mathbb{Z}$-module $\mathbb{Z}^{\mathbb{N}}$ n'est pas libre.

5.3.14

Soit A un anneau fixé. Tous les modules seront des A-modules à gauche. Soit M un module fixé. On obtient un foncteur $h^M :_A \mathcal{M} \to \mathcal{AB}$, défini sur les objets par $h^M(N) = Hom(M, N)$, avec sa structure naturelle de groupe

abélien, et sur les flèches $N_1 \xrightarrow{f} N_2$ par l'application de $Hom(M, N_1)$ dans $Hom(M, N_2)$ donnée par $h^M(f) = fg$. Montrez que si M est un module libre, alors le foncteur h^M transforme une suite exacte

$$0 \to N_1 \to N_2 \to N_3 \to 0$$

en une suite exacte

$$0 \to h^M(N_1) \to h^M(N_2) \to h^M(N_3) \to 0$$

5.3.15

(a) Montrez que si un module M est noethérien, alors tout endomorphisme de M qui est surjectif est un isomorphisme.

(b) Montrez que si M est un module artinien, alors tout endomorphisme de M qui est injectif est un isomorphisme.

5.4 Polynômes et corps

5.4.1

Soit K un corps et $(K_i)_{i\in I}$ une famille de sous-corps de K. Alors $\cap_{i\in I} K_i$ est un sous-corps de K.

5.4.2

Soit K_1 un corps et K un sous-corps de K_1.

(1) Soit S une partie de K. Vérifiez que $K(S)$ coïncide avec le corps des fractions de $K[S]$, c'est-à-dire que

$$K(S) = \{\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} : n \geq 1, x_i \in S, f, g \in K[X_1, \ldots, X_n], g(x_1, \ldots, x_n) \neq 0\}$$

(2) Soit S, S' des parties de K_1. Vérifiez que $K(S \cup S') = (K(S))(S') = (K(S'))(S)$.

(3) Soient S, S' des parties de K_1. Vérifiez que $K(S \cup S') = (K(S))(S') = (K(S'))(S)$.

5.4.3

Vérifiez que chacune des propriétés suivantes est équivalente à ce que le corps K soit algébriquement clos.

(1) Tout polynôme non constant $f \in K[X]$ se décompose en facteurs linéaires.

(2) Les seuls polynômes irréductibles de $K[X]$ sont les polynômes linéaires.

(3) Il n'y a pas d'extension algébrique propre de K, ou autrement dit la seule extension algébrique de K est K lui-même.

5.4.4

Vérifiez qu'en caractéristique zéro toute extension est séparable.

5.4.5

Montrez que le théorème des zéros entraîne à son tour le corollaire 4.35.

5.4.6

Soit E, K, F des corps tels que $F \subset K \subset E$. Montrez que $degtr(E/F)$ est fini si et seulement si $degtr(E/K)$ et $degtr(K/F)$ sont finis et qu'alors on a $degtr(E/F) = degtr(E/K) + degtr(K/F)$.

5.4.7

Une extension de corps E/K est dite de *type fini* si il existe $u_1, \ldots, u_n$ tels que $E = K(u_1, \ldots, u_n)$. Montrez que si E/K est une extension de type fini, alors pour tout corps intermédiaire $K \subset F \subset E$ l'extension F/K est de type fini.

5.4.8

(a) Montrez que $degtr(\mathbb{C}/\mathbb{Q}) = |\mathbb{C}|$ (le cardinal de $\mathbb{C}$).

(b) Soit B une base de transcendance de $\mathbb{C}$ sur $\mathbb{Q}$. Montrez que toute bijection de B peut être prolongée en un automorphisme de $\mathbb{C}$.

(c) Déduisez de (b) que le groupe des automorphismes du corps $\mathbb{C}$ a même cardinalité que le groupe des bijections de $\mathbb{C}$.

5.4.9

Soit une extension de corps E/K telle qu'il y a des $a_1, \ldots, a_n \in E$ de sorte que $E = K[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) : f \in K[X_1, \ldots, X_n]\}$. On a ainsi un K-homomorphisme $\varphi : K[X_1, \ldots, X_n] \to E$ tel que $\varphi(X_i) = a_i$. Soit $P = ker(\varphi)$ et $\tilde{K}$ la clôture algébrique de K.

(a) Utilisez le théorème des zéros de Hilbert pour montrer qu'il existe $\alpha_1, \ldots, \alpha_n \in \tilde{K}$ tels que pour tout $f \in P, f(\alpha_1, \ldots, \alpha_n) = 0$.

(b) Déduisez de (a) que E est K-isomorphe à $K[\alpha_1, \ldots, \alpha_n]$ et que E/K est une extension algébrique.

5.4.10

Considérons l'homomorphisme canonique

$$(\mathbb{R}[Y])[X]/(X^2 - Y) \xrightarrow{\nu} (\mathbb{R}(Y))[X]/(X^2 - Y)$$

qui est injectif. Vérifiez que tout élément du corps $(\mathbb{R}(Y))[X]/(X^2 - Y)$ peut s'écrire comme quotient de deux éléments de l'image de ν. (Ainsi le corps des fractions de $\mathbb{R}[X, Y]/X^2 - Y)$ est $\mathbb{R}$-isomorphe à $\mathbb{R}(Y)[X]/(X^2 - Y)$).

5.4.11

Soit $\tilde{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$. Pour $f \in \mathbb{Q}[X]$, on a le corps de rupture $\mathbb{Q}_f, \mathbb{Q} \subseteq \mathbb{Q}_f \subseteq \tilde{\mathbb{Q}}$. On dira qu'une extension $K/\mathbb{Q}, K \subseteq \tilde{\mathbb{Q}}$, est *résoluble* si tout élément de K est racine d'au moins un polynôme résoluble $f \in \mathbb{Q}[X]$.

(a) Soient $f, g \in \mathbb{Q}[X]$ tels que g est irréductible et possède au moins une racine dans $\mathbb{Q}_f$. Montrez que *toutes* les racines de g sont déjà dans $\mathbb{Q}_f$. (Aide : considérez $Gal(\mathbb{Q}_{fg}/\mathbb{Q})$)

(b) Montrez que si $f \in \mathbb{Q}[X]$ est résoluble, alors $\mathbb{Q}_f/\mathbb{Q}$ est une extension résoluble.

(c) Montrez que si $x, y \in \tilde{\mathbb{Q}}$ appartiennent à des extensions résolubles, disons $x \in K, y \in L$, alors $x + y, xy$ appartiennent à une extension résoluble. Déduisez alors que

$$\mathbb{Q}_r = \bigcup \{K : K/\mathbb{Q} \text{ est une extension résoluble}\}$$

est un sous corps de $\tilde{\mathbb{Q}}$ (c'est *l'extension résoluble maximale de* $\mathbb{Q}$).

5.4.12

Montrer qu'il existe un polynôme rationnel non nul

$$h(X_1, X_2, X_3, X_4, X_5)$$

tel que les coefficients a_i de tout polynôme unitaire de degré 5 non résoluble donné par la construction de Brauer sont tels que $h(a_1, a_2, a_3, a_4, a_5) = 0$.

Bibliographie

[1] R. Cori et D. Lascar. 1993. *Logique mathématique, tome 1*, Masson. (QA9C67)

[2] Giraud, Jean. 197?. *Géométrie algébrique élémentaire. Cours de troisième cycle 1975-76*, Publications mathématiques d'Orsay, no.77-75, Université Paris-sud.

[3] N. Jacobson. 1985. *Basic Algebra I*, Freeman. (QA154.2J33v1)

[4] N. Jacobson. 1989. *Basic Algebra II*, Freeman. (QA154.2J33v2)

[5] P. Jaffard et G. Poitou. 1971. *Introduction aux catégories et aux problèmes universels*, Ediscience. (QA169J54)

[6] S. Lang, 2004. *Algèbre*, Dunod. (QA184.L34414.2004)

[7] S. Maclane, *Categories for the working mathematician*, Springer, 1971. (QA169M33)

[8] P. Ribenboim. 1972. *L'arithmétique des corps*, Hermann. (QA247R5)

Les expressions entre parenthèses indiquent la cote des livres disponibles à la Bibliothèque des sciences de l'UQAM.