Algèbre II

Catégories, Groupes, Corps et Théorie de Galois

David Cimasoni

2025–2026

Table des matières

Introduction

Avant de commencer à élaborer un cours, il ne semble pas inutile de se poser la question suivante : quel est son but ? Dans la brochure officielle, l'objectif affiché est le suivant :

Ce cours a pour but de poursuivre l'étude des structures algébriques fondamentales débutée en Algèbre I.

Ainsi, nous considérons comme acquis les notions étudiées en Algèbre I, à savoir le contenu du polycopié de Michelle Bucher.

Cet objectif officiel est peu détaillé, c'est le moins qu'on puisse dire. Fort heureusement, des buts plus précis peuvent être énumérés, au nombre de quatre.

1. Caractériser la résolubilité des équations polynomiales

Entre autres définitions possibles, on peut voir *l'algèbre classique* comme l'étude de la résolution d'équations de la forme

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0\,,$$

où x est l'inconnue : c'est ce qu'on appelle *l'équation polynomiale (générale)* de degré n. Explorons ce problème pour de petites valeurs de $n \geq 1$.

Muhammad al-Khwarizmi (780-847)

Une équation de degré 1 est aussi appelée une équation *linéaire*. Sa résolution est triviale : elle admet l'unique solution $x = -a_0$. Notons que l'étude de la résolution de systèmes d'équations linéaires n'est autre que *l'algèbre linéaire*, dont vous n'ignorez plus rien grâce au cours d'Algèbre I automne.

Une équation de degré 2 est appelée une équation *quadratique*. L'histoire de sa résolution est complexe, et remonte aux Babyloniens. On sait avec certitude que la solution figure dans le livre "Al-Jabr"[1] du mathématicien perse Muhammad al-Khwarizmi[2]. En notation moderne, on l'écrit :

$$x^2 + a_1 x + a_0 = 0 \quad \Leftrightarrow \quad x = -\frac{a_1}{2} \pm \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0}\,.$$

Scipione del Ferro (1465-1526)

Les choses se corsent en degré 3, avec l'équation *cubique* $x^3+a_2x^2+a_1x+a_0 = 0$. Une première remarque est que la substitution $u = x + \frac{a_2}{3}$ permet de se ramener

1. Ce nom est à l'origine du mot "algèbre".
2. Ce nom est à l'origine du mot "algorithme".

à une équation de la forme $u^3 + au = b$. Il est ensuite possible d'en extraire la solution suivante, due à Scipione del Ferro :

$$u = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}.$$

Lodovico Ferrari (1522-1565)

Finalement, Lodovico Ferrari a montré que l'équation générale de degré 4, ou équation *quartique*, admet aussi une solution "de ce type".

En conclusion : pour tout degré $n \leq 4$, il est possible d'exprimer les solutions de l'équation polynomiale générale de degré n en fonction des coefficients en un nombre fini d'étapes au moyen des quatre opérations fondamentales (addition, soustraction, mutliplication, division) et de "racines". On dit que cette équation est *résoluble par radicaux*.

Niels Abel (1802-1829)

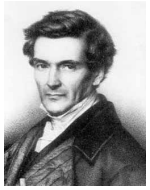
Mais qu'en est-il des degrés $n \geq 5$? L'histoire n'a pas retenu les noms des innombrables mathématiciens qui se sont cassés les dents sur cette question pendant les trois siècles qui suivirent, mais celui qui l'a résolue l'a marquée, l'histoire, au point de donner son nom à de nombreux objets mathématiques. En 1826, Niels Abel montre que l'équation polynomiale générale de degré $n \geq 5$ n'est *pas* résoluble par radicaux. En 1832, un autre jeune mathématicien au destin tragique, Evariste Galois, parvient à donner une caractérisation des équations polynomiales résolubles par radicaux (équations polynomiales pas forcément générales).

Evariste Galois (1811-1832)

Ces résultats reposent sur des considérations de théorie des groupes (Chapitre II), d'extensions de corps (Chapitre III) et de théorie de Galois (Chapitre IV), que nous verrons en détail dans ce cours.

2. Caractériser les points constructibles à la règle et au compas

Comme vous l'avez vu en Géométrie I, une longueur $x \in \mathbb{R}_+$ est constructible à la règle et au compas (à partir des points $(0,0)$ et $(1,0)$) si et seulement si x appartient à l'ensemble des réels positifs qui s'écrivent à partir des nombres entiers au moyen des quatre opérations élémentaires et de la racine carrée. Mais nous ne savons pas déterminer si un réel positif donné appartient à cet ensemble.



Pierre-Laurent Wantzel (1814-1848)

Nous verrons la réponse à cette question au Chapitre III, sous la forme d'un théorème traditionnellement attribué à Pierre-Laurent Wantzel. Nous développerons également les outils nécessaires pour déterminer quels polygones réguliers sont constructibles à la règle et au compas, un résultat dû à Carl Friedrich Gauss.

Ces deux premiers buts sont relativement "pratiques", dans la mesure où il s'agit d'apporter des réponses complètes à des problèmes très naturels et concrets. Les deux buts suivants sont de nature plus "théorique".

Carl Friedrich Gauss (1777-1855)

3. Illustrer le pouvoir unificateur de l'algèbre formel

Au Chapitre II, nous allons énoncer (et partiellement démontrer) le théorème de classification des *modules de génération finie* sur un anneau principal A. Derrière cette terminologie absconse se cachent des objets très naturels. Il est difficile

de créditer ce théorème à un mathématicien en particulier, mais il est incontestable que la mathématicienne Emmy Noether a joué un rôle prépondérant dans l'étude de ces objets.

Emmy Noether (1882-1935)

Cet énoncé très général implique simultanément :

(i) dans le cas de $A = K$ un corps, le théorème de classification des K-espaces vectoriels de dimension finie ;

(ii) dans le cas de $A = \mathbb{Z}$, le théorème de classification des groupes abéliens finis ;

(iii) pour $A = \mathbb{C}[X]$, le théorème de classification des endomorphismes d'espaces vectoriels complexes de dimension finie via la forme normale de Jordan.

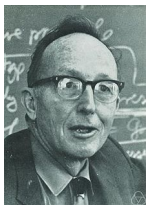
Il s'agit donc à n'en pas douter d'une des plus belles illustrations du pouvoir unificateur de l'algèbre formel.

4. Introduire le langage des catégories

Samuel Eilenberg (1913-1998)

Ce langage permet de jeter une lumière nouvelle et unificatrice sur nombre de notions que vous connaissez (et qu'on revisitera au passage), et d'en définir de nouvelles de manière très naturelle. Depuis son introduction dans les années 1940 par Samuel Eilenberg et Saunders MacLane, il a progressivement envahi de nombreux domaines des mathématiques, comme jadis la théorie des ensembles, et il y a fort à parier que sa connaissance vous sera utile dans la suite de vos études.

Nous avons décidé de présenter ce langage dès le début du cours (Chapitre I), puis de l'utiliser quand bon nous semble dans la suite.



Saunders MacLane (1909-2005)

Nous terminons cette brève introduction avec quelques remarques de nature générale.

Tout d'abord, il est à noter que l'enseignement de l'algèbre formel se fait dans un ordre essentiellement anti-chronologique. Historiquement, des problèmes concrets (tels ceux décrits ci-dessus) apparaissent, et leur résolution donne progressivement naissance, via de multiples essais et erreurs, à la formalisation d'une théorie rigoureuse.[3] Du point de vue didactique, on commence par énoncer les axiomes de la théorie formelle, et on obtient la résolution des problèmes comme corollaires via un processus rigoureux de déduction logique. De ce fait, la présentation de l'algèbre formel est la plupart du temps aride, mais elle permet également un entraînement au raisonnement rigoureux, à n'en pas douter une compétence utile à tout mathématicien[4]. Cela aurait d'ailleurs pu figurer comme 5ème but de ce cours.

Voici encore une remarque, qui bien qu'évidente, mérite d'être énoncée : *l'algèbre formel s'écrit et se communique dans le language de la théorie des ensembles, et se construit à l'aide des principes de base de la logique élémentaire*.

3. Voir à ce sujet l'ouvrage *Preuves et réfutations* d'Imre Lakatos.

4. voire même, à tout citoyen.

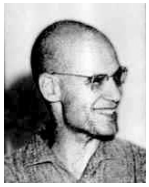
Pour cette raison, nous nous permettons le conseil suivant, qui se veut ferme mais bienveillant :

> Pour étudier l'algèbre formel, il est absolument impératif de maîtriser parfaitement les principes de base de la théorie des ensembles et de la logique élémentaire.

A contrario, étudier l'algèbre formel sans maîtriser la théorie des ensembles et la logique s'apparente à lire Shakespeare dans le texte sans parler l'anglais : c'est une activité absurde et vouée à l'échec.

Encore une remarque aussi importante qu'évidente : l'apprentissage des mathématiques en général et de l'algèbre formel en particulier est un *apprentissage profond*, au même titre que l'assimilation d'un sport ou d'un instrument de musique. Par conséquent, cette acquisition prend du temps, et requière un investissement personnel conséquent : c'est la raison d'être des nombreux exercices présents dans ce polycopié et dans les séries hebdomadaires. Espérer maîtriser l'algèbre formelle uniquement en venant aux cours et en lisant le polycopié, mais sans tenter de résoudre les exercices, est aussi réaliste que de vouloir apprendre à jouer au tennis en regardant des matchs et en lisant des livres sur ce sport, mais sans jamais prendre une raquette dans ses mains. [5]

Et bien entendu, non seulement cela prend du temps, mais cela requière de faire des erreurs, de se tromper. Les meilleurs joueurs de tennis ont fait un nombre incalculable de fautes directes dans leur carrière, les musiciens virtuoses de très nombreuses fausses notes. Il en va de même pour tous les mathématiciens, quel que soit leur niveau. Nous terminerons donc cette introduction par la célèbre phrase d'un des géants des mathématiques du siècle dernier, Alexander Grothendieck :



Alexander Grothendieck (1928-2014)

> "*Craindre l'erreur et craindre la vérité est une seule et même chose. Celui qui craint de se tromper est impuissant à découvrir.*"

5. Je vous laisse le soin de filer la métaphore avec votre instrument de musique favori.

Chapitre I: Catégories

Henri Poincaré (1854-1912)

Le but de ce premier chapitre est d'introduire les notions de base du *langage des catégories*. Ne vous attendez pas à de grands théorèmes [1] : il s'agit "seulement" d'un langage. Mais comme vous le verrez, ce langage permet d'exprimer de manière claire et unifiée une foule de théories mathématiques, dans l'esprit de la célèbre citation d'Henri Poincaré : *La mathématique est l'art de donner le même nom à des choses différentes.*

I.1 Catégories : définitions et exemples

Donnons sans plus attendre la définition d'une catégorie. Pour naviguer dans cette longue définition, il peut être utile d'avoir d'ores et déjà à l'esprit l'exemple fondamental de la catégorie des ensembles (voir le point 1 ci-dessous).

Définition I.1

Une **catégorie** $\mathscr{C}$ consiste en la donnée suivante :

- Une classe $\mathrm{Ob}(\mathscr{C})$ dont les éléments sont appelés les **objets** de $\mathscr{C}$;
- Pour toute paire d'objets (A, B) de $\mathscr{C}$, un ensemble $\mathrm{Hom}_{\mathscr{C}}(A, B)$ de **morphismes** de $\mathscr{C}$, tels que $\mathrm{Hom}_{\mathscr{C}}(A, B)$ et $\mathrm{Hom}_{\mathscr{C}}(C, D)$ sont disjoints pour $(A, B) \neq (C, D)$.
- Pour tous objets A, B, C de $\mathscr{C}$, une opération

$$\mathrm{Hom}_{\mathscr{C}}(A, B) \times \mathrm{Hom}_{\mathscr{C}}(B, C) \longrightarrow \mathrm{Hom}_{\mathscr{C}}(A, C), \quad (f, g) \longmapsto gf$$

  appelée la **composition** des morphismes dans $\mathscr{C}$.

Cette donnée doit satisfaire les deux axiomes suivants :

(i) Pour tout objet A de $\mathscr{C}$, il existe un morphisme 1_A dans $\mathrm{Hom}_{\mathscr{C}}(A, A)$ tel que pour tout $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$, on a $f1_A = f$ et $1_B f = f$; on parle du morphisme **identité** de A.

(ii) La composition est associative : pour tous morphismes $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$, $g \in \mathrm{Hom}_{\mathscr{C}}(B, C)$ et $h \in \mathrm{Hom}_{\mathscr{C}}(C, D)$, on a $(hg)f = h(gf)$.

1. À dire vrai, il n'y aura dans ce chapitre pas le moindre théorème ni la moindre proposition, mais une suite de définitions, de remarques et d'exemples.

Comme d'habitude en algèbre formel, la seule façon d'assimiler une définition aussi aride est de l'illustrer avec un maximum d'exemples. Nous allons commencer avec un exemple et quelques remarques, avant de présenter une liste d'exemples plus conséquente.

Exemple et remarques I.2. 1. La *catégorie des ensembles*, que l'on notera Set, est définie comme suit :

- Les objets de Set sont les ensembles.
- Pour deux ensembles $A, B \in \mathrm{Ob}(\mathsf{Set})$, les morphismes sont donnés par

$$\mathrm{Hom}_{\mathsf{Set}}(A, B) = B^A\,,$$

  l'ensemble des applications de A dans B.
- La composition dans Set est la composition des applications.

Cette donnée définit de manière évidente une catégorie, avec le morphisme identité 1_A sur l'ensemble A donné par l'application identité $\mathrm{id}_A\colon A \to A$.

2. Inspirés par cet exemple fondamental, nous aurons tendance à simplifier la notation d'un morphisme $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ en écrivant

$$f\colon A \longrightarrow B \quad \text{ou} \quad A \xrightarrow{f} B\,,$$

pour autant que la catégorie $\mathscr{C}$ dans laquelle se situe ce morphisme ne prête pas à confusion. Mais attention : l'entité mathématique notée ainsi n'est en général pas une application entre deux ensembles (voir Exemple I.3.7 ci-dessous).

3. Naturellement, la composition de deux morphismes est notée en juxtaposant les flèches correspondantes :

$$A \xrightarrow{f} B \xrightarrow{g} C\,. \qquad (\text{avec } A \xrightarrow{gf} C)$$

L'associativité de la composition (l'axiome (ii) ci-dessus) implique que le résultat d'une composition arbitraire de morphismes

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \xrightarrow{f_3} \quad \dots \quad \xrightarrow{f_n} A_{n+1}$$

est un morphisme bien défini, que l'on peut donc noter $f_n \cdots f_2 f_1$ sans besoin de parenthèses [2].

4. Cette notation permet également de tracer des *diagrammes* dont les sommets sont des objets et les flèches des morphismes de $\mathscr{C}$. En voici un exemple :

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow{i} & D\,. \end{array}$$

2. Exactement comme la composition de plus de deux éléments d'un groupe.

Un diagramme est dit *commutatif* si, lorsqu'on suit un chemin d'un objet à un autre dans le diagramme, le résultat de la composition des morphismes (bien définie par la remarque 3 ci-dessus) ne dépend que de l'objet de départ et de l'objet d'arrivée. Dans l'exemple ci-dessus, cela correspond à l'équation $gf = ih$ dans $\mathrm{Hom}_{\mathscr{C}}(A, D)$.

5. La condition sur les morphismes peut se reformuler de la façon suivante :

$$\mathrm{Hom}_{\mathscr{C}}(A, B) \cap \mathrm{Hom}_{\mathscr{C}}(C, D) \neq \varnothing \;\Rightarrow\; A = C \text{ et } B = D\,.$$

Exprimée pour l'exemple de Set, elle signifie que deux applications $f\colon A \to B$ et $g\colon C \to D$ ne peuvent être égales que si leurs ensembles de départ (ou sources) coïncident, de même que leurs ensembles d'arrivée (ou buts). En d'autres termes, ces ensembles font partie intégrante de la donnée d'une application.

On reprend donc ce principe, et cette terminologie, dans le cadre des catégories : un morphisme $f\colon A \to B$ admet la *source* A et le *but* B, qui font partie intégrante de la donnée de ce morphisme. On dit que f est un *morphisme de A dans B*.

6. Dans la Définition I.1, il est fait mention de "classe" d'objets et non d'ensemble d'objets. C'est une précaution due au célèbre *paradoxe de Russell* que vous avez vu en LOGIQUE ET THÉORIE DES ENSEMBLES : l'ensemble de tous les ensembles n'existe pas ! Cependant, nous nous placerons au niveau de la "théorie naïve des ensembles", et cette subtilité ne jouera aucun rôle dans ce cours. [3]

BERTRAND RUSSELL (1872-1970)

7. Pour tout objet A d'une catégorie $\mathscr{C}$, les éléments de

$$\mathrm{Hom}_{\mathscr{C}}(A, A) =: \mathrm{End}_{\mathscr{C}}(A)$$

sont appelés les *endomorphismes* de A. Notons que la composition des morphismes définit une loi de composition associative sur $\mathrm{End}_{\mathscr{C}}(A)$, avec le morphisme identité 1_A comme élément neutre. Ainsi, l'ensemble [4] $\mathrm{End}_{\mathscr{C}}(A)$ muni de cette loi est ce qu'on appelle un *monoïde*.

Voici enfin la liste d'exemples promise, qui ne manquera pas de vous convaincre que les catégories, comme les groupes, sont omniprésentes en mathématiques. [5]

Exemples I.3 (catégories)**.**

1. La *catégorie des groupes*, notée Grp, est définie comme suit :
   - Les objets de Grp sont les groupes.
   - Pour deux groupes G, H, les morphismes sont donnés par

$$\mathrm{Hom}_{\mathsf{Grp}}(G, H) = \{\varphi\colon G \to H \mid \varphi \text{ homomorphisme de groupes}\}\,.$$

3. Dans la définition la plus générale de catégorie, on parle d'ailleurs de classe de morphismes et non d'ensemble de morphismes ; la Définition I.1 correspond à ce qu'on appelle parfois une catégorie *localement petite*.

4. C'est un des (très rares) endroits où nous utilisons l'hypothèse que les morphismes forment un ensemble, voir note 3.

5. D'ailleurs, vous "faites" déjà des catégories comme Monsieur Jourdain faisait de la prose : sans le savoir.

- La composition dans Grp est la composition des homomorphismes de groupes.

Cette donnée définit bien une catégorie, puisque la composition de deux homomorphismes de groupes est encore un homomorphisme de groupes, cette composition est associative, et l'application identité $\mathrm{id}_G : G \to G$ est un homomorphisme de groupes.

2. La *catégorie des groupes abéliens*, notée Ab, est définie comme suit :
   - Les objets de Ab sont les groupes abéliens.
   - Pour $A, B \in \mathrm{Ob}(\mathsf{Ab})$, on pose
   $$\mathrm{Hom}_{\mathsf{Ab}}(A, B) = \{\varphi : A \to B \mid \varphi \text{ homomorphisme de groupes}\}.$$
   - La composition dans Ab est la composition des homomorphismes de groupes.

   Cette donnée définit bien une catégorie, pour les mêmes raisons que l'exemple précédent.

3. Soit K un corps quelconque. La donnée suivante définit clairement une catégorie, appelée la *catégorie des K-espaces vectoriels*, et notée K-Vect :
   - Les objets de K-Vect sont les K-espaces vectoriels.
   - Pour E, F deux tels objets, on considère
   $$\mathrm{Hom}_{K\text{-}\mathsf{Vect}}(E, F) = \{f : E \to F \mid f \text{ application } K\text{-linéaire}\}.$$
   - La composition dans K-Vect est la composition des applications linéaires.

4. La *catégorie des anneaux* Ann et la *catégorie des corps* Corps se définissent de manière analogue, via les homomorphismes d'anneaux.

Tous ces exemples sont similaires, car issus de l'algèbre. En voici issus d'autres domaines des mathématiques : la topologie et l'analyse.

5. Soit Top la catégorie définie comme suit :
   - Les objets de Top sont les espaces topologiques.
   - Pour X, Y deux espaces topologiques, posons
   $$\mathrm{Hom}_{\mathsf{Top}}(X, Y) = \{f : X \to Y \mid f \text{ application continue}\}.$$
   - La composition dans Top est la composition des applications continues.

   Comme vous le verrez en TOPOLOGIE, la composition de deux applications continues est encore continue, de même que l'application identité $\mathrm{id}_X : X \to X$. Il s'agit donc bien d'une catégorie.

6. Soit Diff la catégorie définie comme suit :
   - Les objets de Diff sont les ouverts de $\mathbb{R}^n$ (pour un entier $n \geq 1$ quelconque).
   - Pour $U \subset \mathbb{R}^n$ et $V \subset \mathbb{R}^m$ deux ouverts, on pose
   $$\mathrm{Hom}_{\mathsf{Diff}}(U, V) = \{f : U \to V \mid f \text{ fonction différentiable}\}.$$

- La composition dans Diff est la composition des fonctions différentiables.

  Comme vous l'avez vu en ANALYSE I, la composition de deux fonctions différentiables est aussi différentiable, de même que la fonction identité $\mathrm{id}_U : U \to U$. Il s'agit donc bien d'une catégorie.

Même si ces exemples sont issus de domaines variés des mathématiques, ils ont un point commun : les objets sont des ensembles (munis d'une certaine structure), les morphismes sont des applications entre ces ensembles (qui respectent la structure en question), et la composition des morphismes est la composition des applications sous-jacentes. [6]

Voici un exemple, issu de la combinatoire, de nature totalement différente.

7. Soit $(X, \sim)$ un *ensemble préordonné*, c'est-à-dire un ensemble quelconque X muni d'un *préordre*, i.e. une relation $\sim$ réflexive ($\forall x \in X : x \sim x$) et transitive ($\forall x, y, z \in X : x \sim y, y \sim z \Rightarrow x \sim z$). Par exemple, on peut prendre pour $\sim$ une relation d'ordre ou une relation d'équivalence.

   Soit $\overline{\mathsf{X}}$ la catégorie définie comme suit :

   - $\mathrm{Ob}(\overline{\mathsf{X}}) = X$.
   - Pour $x, y \in \mathrm{Ob}(\overline{\mathsf{X}}) = X$, on pose

   $$\mathrm{Hom}_{\overline{\mathsf{X}}}(x, y) = \begin{cases} \{(x, y)\} & \text{si } x \sim y\,; \\ \varnothing & \text{sinon.} \end{cases}$$

     Notons qu'on a bien $\mathrm{Hom}_{\overline{\mathsf{X}}}(x, y)$ et $\mathrm{Hom}_{\overline{\mathsf{X}}}(z, t)$ disjoints pour $(x, y) \neq (z, t)$.
   - Soient $x, y, z \in \mathrm{Ob}(\overline{\mathsf{X}}) = X$. L'existence de morphismes $f \in \mathrm{Hom}_{\overline{\mathsf{X}}}(x, y)$ et $g \in \mathrm{Hom}_{\overline{\mathsf{X}}}(y, z)$ implique $x \sim y$ et $y \sim z$ et les égalités $f = (x, y)$ et $g = (y, z)$. Comme $\sim$ est une relation transitive, on a $x \sim z$, ce qui implique $\mathrm{Hom}_{\overline{\mathsf{X}}}(x, z) = \{(x, z)\}$. On peut (et on doit) donc poser $gf := (x, z)$. En résumé, la composition est définie via

   $$(y, z)(x, y) = (x, z) \tag{I.1}$$

     pour tous $x, y, z \in X$ tels que $x \sim y$ et $y \sim z$.

   Vérifions que $\overline{\mathsf{X}}$ satisfait bien les deux axiomes d'une catégorie.

   (i) Comme $\sim$ est réflexive, on a $\mathrm{Hom}_{\overline{\mathsf{X}}}(x, x) = \{(x, x)\}$ pour tout $x \in X$. On peut (et doit) donc définir le morphisme identité via $1_x := (x, x)$. Par l'équation (I.1), on a bien

   $$f 1_x = (x, y)(x, x) = (x, y) = f \quad \text{et} \quad 1_y f = (y, y)(x, y) = (x, y) = f$$

     pour tout $f \in \mathrm{Hom}_{\overline{\mathsf{X}}}(x, y) = \{(x, y)\}$.

   (ii) L'associativité se démontre de manière analogue, ou en notant simplement qu'il y a au plus un morphisme dans $\overline{\mathsf{X}}$ entre deux objets fixés. [7]

6. Il s'agit de *catégories concrètes*.
7. De ce fait, tous les diagrammes dans $\overline{\mathsf{X}}$ sont commutatifs.

Notons que dans cet exemple, la classe des objets est bien un ensemble (voir Remarque 6). On parle de *petite catégorie*.

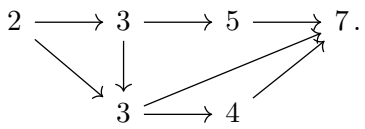
Voyons quelques sous-exemples de cette construction générale.

(a) Si $\sim$ est la relation d'égalité, on obtient

$$\mathrm{Hom}_{\overline{X}}(x,y) = \begin{cases} \{1_x\} & \text{si } x = y\,; \\ \varnothing & \text{sinon.} \end{cases}$$

Ici, les seuls morphismes sont les morphismes identité.

(b) Si $(X,\sim) = (\mathbb{Z},\leq)$ avec $\leq$ la relation d'ordre naturelle sur $\mathbb{Z}$, alors on obtient une catégorie avec des diagrammes (commutatifs) de la forme suivante :



Terminons avec quelques exemples de construction de nouvelles catégories à partir d'anciennes ; ces exemples serviront à illustrer diverses notions aux sections suivantes.

8. Soit $\mathscr{C}$ une catégorie. Considérons la structure $\mathscr{C}^{\mathrm{op}}$ avec
   - $\mathrm{Ob}(\mathscr{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathscr{C})$;
   - $\mathrm{Hom}_{\mathscr{C}^{\mathrm{op}}}(A,B) = \mathrm{Hom}_{\mathscr{C}}(B,A)$ pour tous A, B dans $\mathrm{Ob}(\mathscr{C}^{\mathrm{op}})$.

   On vérifie facilement que, pour la bonne notion de compositon, cela forme une catégorie. On parle de la catégorie *duale* ou *opposée* à $\mathscr{C}$.

9. Soient $\mathscr{C}$ une catégorie et $A \in \mathrm{Ob}(\mathscr{C})$ un objet fixés. On définit une nouvelle catégorie $\mathscr{C}_A$ comme suit.

   - Les objets sont $\mathrm{Ob}(\mathscr{C}_A) = \{f \in \mathrm{Hom}_{\mathscr{C}}(Z,A) \mid Z \in \mathrm{Ob}(\mathscr{C})\}$, notés $\begin{array}{c} Z \\ \downarrow f \\ A \end{array}$.
   - Pour $\begin{array}{c} Z_1 \\ \downarrow f_1 \\ A \end{array}$ et $\begin{array}{c} Z_2 \\ \downarrow f_2 \\ A \end{array}$ deux objets de $\mathscr{C}_A$, les morphismes $f_1 \to f_2$ dans $\mathscr{C}_A$ sont les diagrammes commutatifs de la forme

$$\begin{array}{ccc} Z_1 & \xrightarrow{\sigma} & Z_2 \\ & {\scriptstyle f_1}\searrow \quad \swarrow{\scriptstyle f_2} & \\ & A & \end{array} \tag{I.2}$$

   dans la catégorie $\mathscr{C}$. Ainsi, un tel morphisme correspond à un élément $\sigma \in \mathrm{Hom}_{\mathscr{C}}(Z_1,Z_2)$ tel que $f_2\sigma = f_1$.

- Pour des morphismes $f_1 \to f_2$ et $f_2 \to f_3$ donnés par les diagrammes commutatifs

$$\begin{array}{ccc} Z_1 & \xrightarrow{\sigma} & Z_2 \\ & {\scriptstyle f_1}\searrow \quad \swarrow{\scriptstyle f_2} & \\ & A & \end{array} \qquad \text{et} \qquad \begin{array}{ccc} Z_2 & \xrightarrow{\tau} & Z_3\,, \\ & {\scriptstyle f_2}\searrow \quad \swarrow{\scriptstyle f_3} & \\ & A & \end{array}$$

leur composition dans $\mathscr{C}_A$ est définie par le diagramme $\begin{array}{ccc} Z_1 & \xrightarrow{\tau\sigma} & Z_3 \\ & {\scriptstyle f_1}\searrow \quad \swarrow{\scriptstyle f_3} & \\ & A & \end{array}$. Il s'agit bien d'un élément de $\mathrm{Hom}_{\mathscr{C}_A}(f_1, f_3)$, puisque

$$f_3(\tau\sigma) = (f_3\tau)\sigma = f_2\sigma = f_1\,,$$

où l'on a utilisé l'associativité de la composition dans $\mathscr{C}$ et la commutativité des deux triangles ci-dessus.

Vérifions que $\mathscr{C}_A$ satisfait les deux axiomes d'une catégorie.

(i) Le morphisme identité 1_f dans $\mathscr{C}_A$ pour l'objet $\begin{array}{c} Z \\ \downarrow{\scriptstyle f} \\ A \end{array}$ est donné par le diagramme $\begin{array}{ccc} Z & \xrightarrow{1_Z} & Z \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle f} & \\ & A & \end{array}$ qui est bien commutatif car $f1_Z = f$ dans $\mathscr{C}$.

Pour tout morphisme $f_1 \to f_2$ comme en (I.2), la composition à droite (resp. à gauche) avec 1_{f_1} (resp. 1_{f_2}) redonne bien $f_1 \to f_2$, puisque les égalités $\sigma 1_{Z_1} = \sigma$ et $1_{Z_2}\sigma = \sigma$ sont valides dans $\mathscr{C}$.

(ii) Similairement, on vérifie que l'associativité de la composition dans $\mathscr{C}$ implique l'associativité de la composition dans $\mathscr{C}_A$.

Ainsi, on est donc bien en présence d'une catégorie $\mathscr{C}_A$.

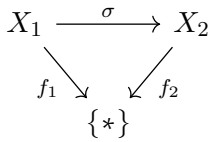
De manière en tous points analogue, étant donnés une catégorie $\mathscr{C}$ et un objet $A \in \mathrm{Ob}(\mathscr{C})$, on définit une nouvelle catégorie $\mathscr{C}^A$ dont les objets sont les morphismes de $\mathscr{C}$ de la forme $\begin{array}{c} A \\ \downarrow{\scriptstyle f} \\ Z \end{array}$. C'est un exercice.

Voyons quelques sous-exemples de ces constructions générales.

(a) Considérons la catégorie $\mathscr{C} = \mathsf{Set}$ des ensembles et l'objet A donné par un singleton $\{*\}$. La catégorie $\mathscr{C}_A = \mathsf{Set}_*$ ne donne rien de nouveau. En effet, on a

$$\begin{aligned} \mathrm{Ob}(\mathsf{Set}_*) &= \{f \in \mathrm{Hom}_{\mathsf{Set}}(X, \{*\}) \mid X \in \mathrm{Ob}(\mathsf{Set})\} \\ &= \{f\colon X \to \{*\} \mid X \text{ ensemble}\} = \mathrm{Ob}(\mathsf{Set})\,, \end{aligned}$$

puisque tout ensemble X admet une unique application $X \to \{*\}$. Comme de plus tout diagramme de la forme

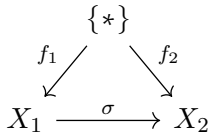


commute, on a $\mathrm{Hom}_{\mathsf{Set}_*}(f_1, f_2) = \mathrm{Hom}_{\mathsf{Set}}(X_1, X_2)$, et l'on peut identifier [8] la catégorie Set_* avec Set.

(b) La catégorie $\mathscr{C}^A = \mathsf{Set}^*$ est plus intéressante. En effet, on a

$$\begin{aligned}\mathrm{Ob}(\mathsf{Set}^*) &= \{f \in \mathrm{Hom}_{\mathsf{Set}}(\{*\}, X) \mid X \in \mathrm{Ob}(\mathsf{Set})\} \\ &= \{f : \{*\} \to X \mid X \text{ ensemble}\} = \{(X, x) \mid X \text{ ensemble}, x \in X\},\end{aligned}$$

puisque la donnée d'une application $f : \{*\} \to X$ est équivalente à celle d'un élément $f(*) = x \in X$. Une telle paire (X, x) est appelée un *ensemble pointé*. De plus, un diagramme



commute si et seulement si $\sigma : X_1 \to X_2$ satisfait $\sigma(x_1) = x_2$, où $x_1 = f_1(*)$ et $x_2 = f_1(*)$. Une telle application, notée $\sigma : (X_1, x_1) \to (X_2, x_2)$, est appelée une *application pointée*.

(c) Pour $\mathscr{C} = \mathsf{Set}$ et A un ensemble à deux éléments, les catégories $\mathscr{C}_A$ et $\mathscr{C}^A$ se comprennent aisément : c'est un exercice.

(d) Pour $\mathscr{C} = \overline{\mathsf{X}}$ la catégorie obtenue via $(X, \sim) = (\mathbb{Z}, \leq)$ comme en Exemple 7 ci-dessus, et pour tout $A = n \in \mathrm{Ob}(\mathscr{C}) = \mathbb{Z}$, il en va de même des catégories $\mathscr{C}_A$ et $\mathscr{C}^A$: c'est un autre exercice.

10. Soient $\mathscr{C}$ une catégorie et $A, B \in \mathrm{Ob}(\mathscr{C})$ deux objets fixés. On définit une nouvelle catégorie $\mathscr{C}_{A,B}$ comme suit.

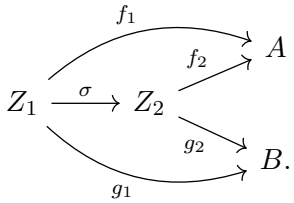
- Les objets sont

$$\mathrm{Ob}(\mathscr{C}_{A,B}) = \{(f, g) \in \mathrm{Hom}_{\mathscr{C}}(Z, A) \times \mathrm{Hom}_{\mathscr{C}}(Z, B) \mid Z \in \mathrm{Ob}(\mathscr{C})\},$$

notés $Z \overset{f}{\underset{g}{\rightrightarrows}} \begin{matrix} A \\ B \end{matrix}$.

8. La signification précise des mots "on peut identifier" et de l'égalité (légèrement abusive) $\mathrm{Ob}(\mathsf{Set}_*) = \mathrm{Ob}(\mathsf{Set})$ est à chercher du côté des *équivalences de catégories*, dont nous ne parlerons pas ici.

- Les morphismes dans $\mathscr{C}_{A,B}$ de $Z_1 \overset{f_1}{\underset{g_1}{\rightrightarrows}} \begin{matrix} A \\ B \end{matrix}$ dans $Z_2 \overset{f_2}{\underset{g_2}{\rightrightarrows}} \begin{matrix} A \\ B \end{matrix}$ sont les diagrammes commutatifs de la forme suivante dans $\mathscr{C}$:



Il n'est pas difficile de définir la composition dans $\mathscr{C}_{A,B}$ (dans l'esprit de l'Exemple 9 ci-dessus), ni de vérifier les axiomes d'une catégorie.

En renversant les flèches, on définit de manière analogue la catégorie $\mathscr{C}^{A,B}$ dont les objets sont les diagrammes dans $\mathscr{C}$ de la forme $\begin{matrix} A \\ B \end{matrix} \overset{f}{\underset{g}{\rightrightarrows}} Z\,.$

I.2 Isomorphismes

Dans la catégorie des ensembles, certains morphismes jouent un rôle important : il s'agit des applications bijectives. Le but de cette section est d'étudier la généralisation de cette notion à des catégories arbitraires.

Notons tout d'abord que la définition usuelle d'injectivité ($f\colon X \to Y$ injective si $\forall x, x' \in X : f(x) = f(x') \Rightarrow x = x'$) ne fait pas de sens dans une catégorie quelconque, où les objets ne sont pas nécessairement des ensembles. Il en va de même pour la définition usuelle de surjectivité ($f\colon X \to Y$ surjective si $\forall y \in Y : \exists x \in X,\ f(x) = y$), et donc a fortiori pour la définition de bijectivité.

Rappelons néanmoins que, comme vous l'avez vu en LOGIQUE ET THÉORIE DES ENSEMBLES, une application $f\colon X \to Y$ est injective (resp. surjective) si et seulement s'il existe $g\colon Y \to X$ telle que $g \circ f = \mathrm{id}_X$ (resp. $f \circ g = \mathrm{id}_Y$). En particulier, elle est bijective si et seulement si elle admet un inverse à gauche et à droite. Cela justifie la définition suivante.

Définition I.4

Soit $\mathscr{C}$ une catégorie quelconque. Un morphisme $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ est appelé un **isomorphisme** s'il existe $g \in \mathrm{Hom}_{\mathscr{C}}(B, A)$ tel que $gf = 1_A$ et $fg = 1_B$. Les objets A et B sont alors dits **isomorphes**, ce qui est noté $A \simeq B$.

La vérification des assertions suivantes est laissée en exercice : les preuves sont identiques à celles donnés en théorie des groupes pour les énoncés correspondants. Ensemble, elles montrent que $\simeq$ est une relation d'équivalence (sur la classe $\mathrm{Ob}(\mathscr{C})$).

Remarques I.5.

1. Si $f \in \mathrm{Hom}_{\mathscr{C}}(A,B)$ est un isomorphisme, alors le morphisme g tel que $gf = 1_A$ et $fg = 1_B$ est unique. Il est habituellement noté $f^{-1} \in \mathrm{Hom}_{\mathscr{C}}(B,A)$ et appelé *l'inverse* de f.
2. Le morphisme identité 1_A est un isomorphisme, d'inverse $1_A^{-1} = 1_A$.
3. Si f est un isomorphisme, alors f^{-1} est un isomorphisme, avec $(f^{-1})^{-1} = f$.
4. Si $f \in \mathrm{Hom}_{\mathscr{C}}(A,B)$ et $g \in \mathrm{Hom}_{\mathscr{C}}(B,C)$ sont des isomorphismes, alors la composition $gf \in \mathrm{Hom}_{\mathscr{C}}(A,C)$ est un isomorphisme, d'inverse $(gf)^{-1} = f^{-1}g^{-1}$.

Reprenons à présent la liste des catégories vues en Section I.1, et tentons d'identifier les isomorphismes.

Exemples I.6 (isomorphismes)**.**

1. Par la discussion ci-dessus, les isomorphismes dans Set coïncident avec les applications bijectives.
2. Par définition, les isomorphismes dans Grp sont les isomorphismes de groupes. Comme vous l'avez vu en ALGÈBRE I, ils coïncident avec les homomorphismes de groupes bijectifs.
3. Par définition, les isomorphismes dans Ab sont les isomorphismes de groupes abéliens, qui coïncident avec les homomorphismes de groupes abéliens bijectifs.
4. Les isomorphismes dans K-Vect sont les isomorphismes linéaires, qui coïncident avec les applications linéaires bijectives.
5. Les isomorphismes dans Ann et Corps sont les isomorphismes d'anneaux et de corps, respectivement, qui ne sont autres que les homomorphismes bijectifs.
6. Les isomorphismes dans Top portent le nom d'*homéomorphismes*. Attention, pour la première fois dans cette liste, un morphisme bijectif dans Top n'est pas nécessairement un isomorphisme : comme vous le verrez en TOPOLOGIE, une application continue bijective n'est pas toujours un homéomorphisme.
7. Les isomorphismes dans Diff sont appelés *difféomorphismes*.
8. Dans la catégorie $\overline{\mathsf{X}}$ associée à $(X,\sim) = (\mathbb{Z},\leq)$, deux objets $m,n \in \mathbb{Z}$ sont isomorphes si et seulement s'ils sont égaux (et de même dès que $\sim$ est une relation d'ordre). Ainsi, les seuls isomorphismes dans cette catégorie sont les identités.
9. Les isomorphismes dans $\mathscr{C}_A$ entre $\begin{array}{c} Z_1 \\ \downarrow{\scriptstyle f_1} \\ A \end{array}$ et $\begin{array}{c} Z_2 \\ \downarrow{\scriptstyle f_2} \\ A \end{array}$ sont les diagrammes commutatifs de la forme

$$\begin{array}{ccc} Z_1 & \xrightarrow{\sigma} & Z_2 \\ & {\scriptstyle f_1}\searrow \quad \swarrow{\scriptstyle f_2} & \\ & A & \end{array}$$

avec σ un isomorphisme de $\mathscr{C}$. Le cas des catégories $\mathscr{C}^A$, $\mathscr{C}_{A,B}$ et $\mathscr{C}^{A,B}$ est similaire.

Terminologie I.7. Soit A un objet d'une catégorie $\mathscr{C}$. Un *automorphisme* de A est un isomorphisme dans $\mathrm{End}_{\mathscr{C}}(A)$.

Remarque I.8. Par le second axiome d'une catégorie et les Remarques I.5.2–4 ci-dessus, l'ensemble[9] $\mathrm{Aut}_{\mathscr{C}}(A)$ des automorphismes de A est un groupe pour la composition.

Exemples I.9 (groupes d'automorphismes)**.**

1. Le groupe des automorphismes dans Set d'un ensemble X n'est autre que le groupe symétrique :

$$\mathrm{Aut}_{\mathsf{Set}}(X) = \{f\colon X \to X \mid \exists g\colon X \to X,\ f \circ g = g \circ f = \mathrm{id}_X\} = S(X)\,.$$

   Rappelons qu'une *action* $\rho\colon G \times X \to X$ d'un groupe G sur un ensemble X est équivalente à la donnée d'un homomorphisme de groupes $\varphi\colon G \to S(X)$, via $\rho(g,x) = \varphi(g)(x)$ pour $g \in G$ et $x \in X$. Ainsi, on peut définir plus généralement une *action* d'un groupe G sur un objet $A \in \mathrm{Ob}(\mathscr{C})$ comme la donnée d'un homomorphisme de groupes $\varphi\colon G \to \mathrm{Aut}_{\mathscr{C}}(A)$. On y reviendra.

2. Pour G un groupe, le groupe $\mathrm{Aut}(G)$ des automorphismes de G est souvent difficile à calculer. Comme on le verra en exercices, dans le cas d'un groupe cyclique $G = \mathbb{Z}/n\mathbb{Z}$, on obtient

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^* = \{[k] \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{pgcd}(n,k) = 1\}\,, \tag{I.3}$$

   où l'élément $[k] \in (\mathbb{Z}/n\mathbb{Z})^*$ correspond à l'automorphisme de $\mathbb{Z}/n\mathbb{Z}$ induit par la multiplication par $k \in \mathbb{Z}$. Notons que cette analyse inclut le cas $n = 0$, qui donne $\mathrm{Aut}(\mathbb{Z}) \simeq \mathbb{Z}^* = \{\pm 1\}$.

3. Pour E un K-espace vectoriel de dimension finie, tout choix d'une base de E fournit un isomorphisme de groupes

$$\mathrm{Aut}_{K-\mathsf{Vect}}(E) \simeq \mathrm{GL}(n,K)$$

   avec le groupe général linéaire de degré $n = \dim(E)$.

4. Dans la catégorie $\overline{\mathsf{X}}$ définie via $(X, \sim)$, on a $\mathrm{End}_{\overline{\mathsf{X}}}(x) = \{(x,x)\} = \{1_x\}$ pour tout $x \in X$. En particulier, le groupe $\mathrm{Aut}_{\overline{\mathsf{X}}}(x)$ est trivial pour tout $x \in X$.

I.3 Propriétés universelles

Le but de cette section est d'introduire une façon extrêmement commode de présenter certains objets dans des catégories. Comme vous le verrez, ici encore, vous avez déjà utilisé de telles *propriétés universelles* plus d'une fois sans le savoir.

9. C'est un autre des (très rares) endroits où nous utilisons l'hypothèse que les morphismes forment un ensemble, voir notes 3 et 4.

L'exposition parfaitement formelle de cette notion est inutilement technique pour notre cours ; nous allons donc nous contenter dans cette section d'une version basée sur les *objets initiaux et finaux*, qui constituent le sujet de la première sous-section. On donnera ensuite les exemples des propriétés universelles du *quotient*, du *produit*, et du *coproduit*.

D'autres exemples de propriétés universelles apparaîtront naturellement au fil du cours, en particulier en Sections II.2.3 et II.3.1 où l'on traitera des propriétés universelles de l'abélianisé et du groupe libre.

I.3.1 Objets initiaux et finaux

Définition I.10

Soit $\mathscr{C}$ une catégorie. Un objet $I \in \mathrm{Ob}(\mathscr{C})$ est dit **initial** dans $\mathscr{C}$ si pour tout $A \in \mathrm{Ob}(\mathscr{C})$, l'ensemble $\mathrm{Hom}_{\mathscr{C}}(I, A)$ a un unique élément. Similairement, un objet $F \in \mathrm{Ob}(\mathscr{C})$ est dit **final** (ou **terminal**) dans $\mathscr{C}$ si pour tout $A \in \mathrm{Ob}(\mathscr{C})$, l'ensemble $\mathrm{Hom}_{\mathscr{C}}(A, F)$ a un unique élément.

Que peut-on dire de l'existence et de l'unicité de ces objets ?

Remarques I.11.

1. Notons tout de suite que certaines catégories n'admettent pas de tels objets. Par exemple, dans la catégorie $\overline{\mathsf{X}}$ donnée par $(X, \sim) = (\mathbb{Z}, \leq)$, un objet initial serait un entier $i \in \mathbb{Z}$ avec $i \leq a$ pour tout $a \in \mathbb{Z}$. De même, un objet final serait un entier $f \in \mathbb{Z}$ avec $a \leq f$ pour tout $a \in \mathbb{Z}$. De tels entiers n'existent pas.
2. Notons également que même quand ils existent, de tels objets ne sont pas nécessairement uniques. Par exemple, si l'ensemble vide $\varnothing$ est clairement le seul objet initial dans la catégorie Set des ensembles, tout singleton en est un objet final.
3. En revanche, si I_1 et I_2 sont deux objets initiaux dans une catégorie $\mathscr{C}$, alors $I_1 \simeq I_2$ et cet isomorphisme est unique.

   ⌜ Soient donc I_1, I_2 deux objets initiaux dans $\mathscr{C}$. Comme I_1 est initial, il existe un unique morphisme $f : I_1 \to I_2$; comme I_2 est initial, il existe un unique morphisme $g : I_2 \to I_1$. La composition gf appartient à l'ensemble $\mathrm{Hom}_{\mathscr{C}}(I_1, I_1)$, qui est réduit au seul élément $\{1_{I_1}\}$ puisque I_1 est initial, d'où l'égalité $gf = 1_{I_1}$; pour la même raison, on a $fg = 1_{I_2}$. Ainsi, on a $I_1 \simeq I_2$ via cet unique isomorphisme f d'inverse g. ⌟

   De même, on montre que si F_1 et F_2 sont deux objets finaux dans une catégorie, alors $F_1 \simeq F_2$ et cet isomorphisme est unique. La preuve est essentiellement identique.

   On aura donc tendance à dire "l'objet initial" et "l'objet final" dans $\mathscr{C}$, même s'il s'agit là d'un léger abus de langage.

Exemples I.12 (objets initiaux et finaux)**.**

1. Comme on l'a vu, la catégorie Set admet l'objet initial $I = \varnothing$ et l'objet final $F \simeq \{*\}$. (Deux singletons sont en unique bijection l'un avec l'autre, ce qui est cohérent avec la Remarque 3.)
2. La catégorie Grp admet l'objet initial et l'objet final donnés par "le" groupe trivial, un groupe unique à unique isomorphisme près.
3. La situation est identique dans Ab (le groupe abélien trivial) et dans K-Vect (le K-espace vectoriel trivial).
4. Dans Ann, on a l'objet final donné par l'anneau trivial (le seul anneau A où $0_A = 1_A$). Mais l'objet initial est donné par l'anneau $\mathbb{Z}$. En effet, on vérifie facilement que pour tout anneau A, il existe un unique homomorphisme[10] d'anneaux $\varepsilon\colon \mathbb{Z} \to A$: il est donné par $\varepsilon(n) = n \cdot 1_A$ pour $n \in \mathbb{Z}$.
5. Il n'y a ni objet initial ni objet final dans la catégorie des corps.

   ⌜ Rappelons que s'il existe un homomophisme d'anneaux $\varphi\colon A_1 \to A_2$, alors $\mathrm{car}(A_2)$ divise $\mathrm{car}(A_1)$. Ainsi, un objet final dans Corps serait un corps K tel que $\mathrm{car}(K)$ divise tous les premiers ; on aurait donc $\mathrm{car}(K) = 1$ ce qui implique $K = \{0\}$, qui n'est pas un corps.[11] Rappelons également qu'un homomorphisme de corps est toujours injectif. Ainsi, un objet initial dans Corps serait un corps qui s'injecte dans tous les corps, en particulier dans $\mathbb{F}_2$ et dans $\mathbb{F}_3$: on vérifie que cela n'existe pas. ⌟
6. Si I est initial dans une catégorie $\mathscr{C}$, alors l'unique $\begin{array}{c} I \\ \downarrow f \\ A \end{array}$ est initial dans la catégorie $\mathscr{C}_A$: c'est un exercice.
7. On vérifie facilement que I est initial dans une catégorie $\mathscr{C}$ si et seulement si I est final dans la catégorie opposée $\mathscr{C}^{\mathrm{op}}$.

Il est temps d'introduire la notion de propriété universelle, de façon semi-formelle.

Terminologie I.13. On dit qu'une construction *satisfait une propriété universelle* si elle peut être vue comme l'objet initial ou final d'une catégorie.

Remarques I.14.

1. Comme mentionné au début de cette section, il existe une définition plus formelle, mais elle dépasse largement le cadre de ce cours sans pour autant apporter de grande clarification. Nous nous contenterons donc de cette terminologie.
2. Rappelons que, par la Remarque I.11.3, une telle construction est unique à unique isomorphisme près (dans la catégorie en question).

Comme toujours avec des définitions aussi abstraites, la seule manière (que je connaisse) pour les assimiler est de les illustrer avec un maximum d'exemples. Dans un premier temps, nous allons nous contenter de trois familles d'exemples : les quotients, les produits, et les coproduits.

10. C'est d'ailleurs à l'aide cet unique homomorphisme qu'on définit habituellement la caractéristique de A, via $\mathrm{Ker}(\varepsilon) = \mathrm{car}(A)\mathbb{Z}$.
11. Ce calcul est cohérent avec le fait que $A = \{0\}$ est final dans Ann.

I.3.2 Quotients

Le but de cette première sous-section est de présenter la *propriété universelle du quotient*, tout d'abord dans la catégorie des ensembles, puis dans diverses autres catégories.

Fixons un ensemble X muni d'une relation d'équivalence $\sim$. Comme d'habitude, on notera $\pi : X \to X/\sim$ la projection canonique qui envoie $x \in X$ sur sa classe d'équivalence $\pi(x) = [x]$ dans l'ensemble quotient $X/\sim$.

La propriété universelle du quotient de X par $\sim$ est l'énoncé suivant :

> Soit $f : X \to Y$ une application telle que pour tous $x, x' \in X$ avec $x \sim x'$, on a $f(x) = f(x')$; une telle application induit une application $\overline{f} : X/\sim \to Y$ via $\overline{f}([x]) = f(x)$.

On dit que l'application f *passe au quotient*. De manière plus formelle, cette propriété universelle peut s'énoncer comme suit :

$$\forall f : X \to Y \text{ telle que } x \sim x' \Rightarrow f(x) = f(x'), \exists!\, \overline{f} : X/\sim \to Y \text{ telle que } \overline{f} \circ \pi = f\,.$$

Elle s'illustre à l'aide du diagramme

$$\begin{array}{ccc} X & \xrightarrow{\forall f} & Y\,, \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists!\overline{f}} & \\ X/\sim & & \end{array} \tag{I.4}$$

où l'on adopte la convention de couleurs suivante : les éléments en noir sont fixés dans la propriété universelle ; le bleu est la donnée ($\forall$...) ; le violet est l'unique résultat qui fait commuter le diagramme ($\exists!$...).

De manière encore plus formelle, considérons la catégorie $\mathscr{C} = \mathscr{C}(X, \sim)$ avec

- $\mathrm{Ob}(\mathscr{C}) = \{f : X \to Y \mid Y \text{ ensemble}, \forall x \in X, \forall x' \in X,\ x \sim x' \Rightarrow f(x) = f(x')\}$;
- les morphismes entre $\begin{array}{c} X \\ \downarrow{\scriptstyle f} \\ Y \end{array}$ et $\begin{array}{c} X \\ \downarrow{\scriptstyle g} \\ Z \end{array}$ sont les diagrammes commutatifs de la forme

$$\begin{array}{ccc} & X & \\ {\scriptstyle f}\swarrow & & \searrow{\scriptstyle g} \\ Y & \xrightarrow{\sigma} & Z \end{array}$$

, donc sont donnés via les applications $\sigma : Y \to Z$ avec $\sigma \circ f = g$.

L'énoncé ci-dessus dit précisément que $\pi : X \to X/\sim$ est un objet initial dans $\mathscr{C}$: il s'agit donc bien d'une propriété universelle.

Remarque I.15. [12] Étant donnée une application $F : X \to Z$ quelconque, considérons la relation d'équivalence $\sim_F$ sur X définie par $x \sim_F x' :\Leftrightarrow F(x) = F(x')$. Alors, l'application $F : X \to \mathsf{Im}(F)$ satisfait la propriété universelle du quotient de X par $\sim_F$.

12. Cette remarque n'a pas été discutée en détail en cours, et n'est pas exigible aux examens.

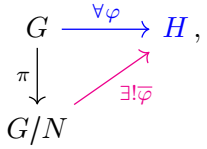
⌜ En effet, soit $f\colon X \to Y$ une application telle que $f(x) = f(x')$ pour tous $x, x' \in X$ avec $x \sim_F x'$. Cela signifie que $F(x) = F(x') \Rightarrow f(x) = f(x')$. Ainsi, il existe une unique application $\overline{f}\colon \mathsf{Im}(F) \to Y$ telle que $\overline{f} \circ F = f$: elle est donnée par $\overline{f}(F(x)) = f(x)$ pour tout $x \in X$, et est bien défini par hypothèse. ⌟

Par la Remarque I.11.3, les objets $\pi\colon X \to X/\sim_F$ et $F\colon X \to \mathsf{Im}(F)$ sont canoniquement isomorphes dans la catégorie $\mathscr{C}(X, \sim_F)$. En particulier, l'application arbitraire $F\colon X \to Z$ dont on était parti induit une bijection $X/\sim_F \simeq \mathsf{Im}(F)$. C'est un énoncé classique de théorie des ensembles, qui porte parfois le nom de *théorème de la bijection*, et dont nous avons maintenant obtenu une preuve plus abstraite.

Vous avez également vu cette propriété universelle du quotient dans la catégorie Grp, en ALGÈBRE I. Cette fois, on fixe un groupe G et un sous-groupe normal $N \lhd G$, et l'on note $\pi\colon G \to G/N$ la projection canonique sur le groupe quotient. La propriété universelle du quotient de G par N est l'énoncé suivant :

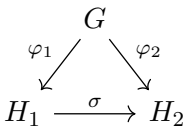
> Si $\varphi\colon G \to H$ est un homomorphisme de groupes tel que $N \subset \mathrm{Ker}(\varphi)$, alors il existe un unique homomorphisme de groupes $\overline{\varphi}\colon G/N \to H$ tel que $\overline{\varphi} \circ \pi = \varphi$.

Elle s'illustre à l'aide du diagramme



où l'on utilise la même convention de couleurs qu'en (I.4).

De manière plus formelle, cet énoncé signifie que la projection $\pi\colon G \to G/N$ est un objet initial de la catégorie $\mathscr{C}(G, N)$ dont les objets sont les homomorphismes de groupes $\varphi\colon G \to H$ avec $N \subset \mathrm{Ker}(\varphi)$, et dont les morphismes sont donnés par les diagrammes commutatifs de la forme



.

Remarque I.16. [13] Étant donné un homomorphisme de groupes $\Phi\colon G \to G'$ quelconque, posons $N := \mathrm{Ker}(\Phi) \lhd G$. Alors, l'homomorphisme $\Phi\colon G \to \mathsf{Im}(\Phi)$ satisfait la propriété universelle du quotient de G par N.

⌜ En effet, soit $\varphi\colon G \to H$ un homomorphisme de groupes tel que $N = \mathrm{Ker}(\Phi) \subset \mathrm{Ker}(\varphi)$. Il existe un unique homomorphisme de groupes $\overline{\varphi}\colon \mathsf{Im}(\Phi) \to H$ tel que $\overline{\varphi} \circ \Phi = \varphi$: il est donné par $\overline{\varphi}(\Phi(g)) = \varphi(g)$ pour tout $g \in G$, et est bien défini car $\mathrm{Ker}(\Phi) \subset \mathrm{Ker}(\varphi)$. ⌟

Par la Remarque I.11.3, les objets $\pi\colon G \to G/N$ et $\Phi\colon G \to \mathsf{Im}(\Phi)$ sont canoniquement isomorphes dans la catégorie $\mathscr{C}(G, N)$. En particulier, l'homomorphisme

13. Cette remarque non plus n'a pas été discutée en détail en cours et n'est pas exigible aux examens.

de groupes $\Phi : G \to G'$ induit un isomorphisme de groupes $G/\mathrm{Ker}(\Phi) \simeq \mathsf{Im}(\Phi)$. Ce n'est autre que le *(premier) théorème d'isomorphisme*, vu en ALGÈBRE I, et dont nous avons maintenant obtenu une preuve de nature catégorielle.

Il existe également des propriétés universelles du quotient analogues dans les catégories Ab, Ann, et K-Vect, où l'on quotiente les groupes abéliens par des sous-groupes, les anneaux par des idéaux, et les espaces vectoriels par des sous-espaces vectoriels : cela sera discuté en exercices.

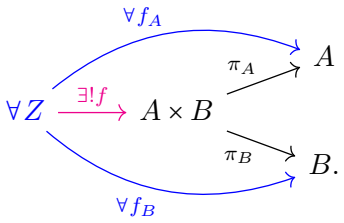
Notons pour finir que pour tout espace topologique X muni d'une relation d'équivalence $\sim$, il existe une *topologie quotient* sur $X/\sim$ telle que la projection $\pi : X \to X/\sim$ satisfait la propriété universelle du quotient dans la catégorie Top. Vous le verrez en cours de TOPOLOGIE.

I.3.3 Produits

Dans cette sous-section, nous allons commencer par identifier la propriété universelle satisfaite par la produit cartésien de deux ensembles dans la catégorie Set. Il sera ensuite aisé de formuler cette propriété universelle dans une catégorie quelconque, avant de l'illustrer par les exemples de catégories vues en Section I.1.

Soient donc A et B deux ensembles, et considérons leur produit cartésien $A \times B$ muni des projections $A \times B \overset{\pi_A}{\to} A$, $A \times B \overset{\pi_B}{\to} B$ définies par $\pi_A(a,b) = a$, $\pi_B(a,b) = b$ pour tout $(a,b) \in A \times B$. Nous allons maintenant montrer que cette donnée satisfait la propriété universelle suivante :

Pour tout ensemble Z et applications $Z \overset{f_A}{\to} A$, $Z \overset{f_B}{\to} B$, il existe une unique application $f : Z \to A \times B$ telle que $\pi_A \circ f = f_A$ et $\pi_B \circ f = f_B$. Cette propriété est illustrée dans le diagramme ci-dessous, avec la convention de couleurs de (I.4) :



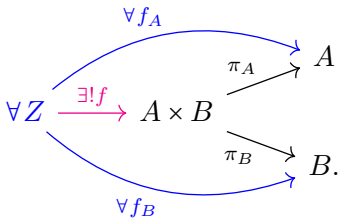
La vérification de cet énoncé est triviale : il suffit de poser $f(z) = (f_A(z), f_B(z))$ pour tout $z \in Z$. Ce que cette propriété universelle dit en des termes abstraits, c'est tout simplement que la donnée d'une application $Z \to A \times B$ est équivalente à la donnée de deux applications $Z \to A$ et $Z \to B$: ses deux coordonnées.

L'avantage de cette reformulation, c'est qu'il est maintenant possible de définir des produits dans n'importe quelle catégorie, ce que nous n'allons pas nous priver de faire immédiatement.

Définition I.17

Soient $\mathscr{C}$ une catégorie, et A, B deux objets de $\mathscr{C}$. Le **produit** de A et B dans $\mathscr{C}$ consiste en la donnée d'un objet $A \times B$ de $\mathscr{C}$ et de deux morphismes $\pi_A \in \mathrm{Hom}_{\mathscr{C}}(A \times B, A)$ et $\pi_B \in \mathrm{Hom}_{\mathscr{C}}(A \times B, B)$ tels que : $\forall Z \in \mathrm{Ob}(\mathscr{C})$, $\forall f_A \in \mathrm{Hom}_{\mathscr{C}}(Z, A)$, $\forall f_B \in \mathrm{Hom}_{\mathscr{C}}(Z, B)$, $\exists! f \in \mathrm{Hom}_{\mathscr{C}}(Z, A \times B)$ avec $\pi_A f = f_A$ et $\pi_B f = f_B$.

Cette propriété est illustrée dans le diagramme ci-dessous, maintenant à interpréter comme un diagramme commutatif dans $\mathscr{C}$:



Remarques I.18.

1. Ainsi, un produit de A et B dans $\mathscr{C}$ n'est autre qu'un objet final dans la catégorie $\mathscr{C}_{A,B}$ définie en Section I.1. Cela valide donc l'énoncé ci-dessus comme une propriété universelle : on parle de la *propriété universelle du produit*.
2. Comme on le verra plus bas, un produit de A et B dans $\mathscr{C}$ n'existe pas toujours.
3. S'il existe, alors il est unique à unique isomorphisme près dans $\mathscr{C}_{A,B}$ (par la Remarque I.11.3). En particulier, deux produits de A et B dans $\mathscr{C}$ sont isomorphes dans $\mathscr{C}$, ce qui justifie de dire *le* produit de A et B dans $\mathscr{C}$ (plutôt qu'*un* produit).

Voyons à présent comment cette définition très abstraite s'incarne concrètement dans les différentes catégories vues en en Section I.1. La plupart des vérifications sont triviales et laissées en exercice.

Exemples I.19 (produits)**.**

1. Comme on l'a vu ci-dessus, le produit de deux ensembles A, B dans Set est leur produit cartésien $A \times B$ (muni des projections naturelles), ce qui justifie bien évidemment la terminologie.
2. Dans la catégorie Grp, on vérifie très facilement que le produit direct $G \times H$ des groupes G et H (muni des projections naturelles) satisfait cette propriété universelle. C'est un exercice.
3. Dans Ab, cette propriété universelle est satisfaite par le produit direct des groupes abéliens, habituellement noté $A \oplus B$.
4. Dans K-Vect, c'est la somme directe $E \oplus F$ d'espaces vectoriels qui satisfait cette propriété universelle.
5. Dans Ann, l'anneau produit $A \times B$ fonctionne.

6. Dans la catégorie Corps, la situation se corse. Notons d'abord que si K_1 et K_2 sont deux corps, alors l'anneau produit $K_1 \times K_2$ n'est jamais un corps : en effet, il n'est jamais intègre puisque $(1_{K_1}, 0_{K_2})(0_{K_1}, 1_{K_2}) = 0_{K_1 \times K_2}$. En fait, les produits n'existent en général pas dans cette catégorie.

   ⌜ Considérons par exemple les deux corps $K_1 = \mathbb{F}_2$ et $K_2 = \mathbb{F}_3$. Un produit de $\mathbb{F}_2$ et $\mathbb{F}_3$ dans Corps serait un corps K muni de deux morphismes de corps $K \to \mathbb{F}_2$ et $K \to \mathbb{F}_3$. Comme ces morphismes sont injectifs, le corps K serait un sous-corps de $\mathbb{F}_2$ et de $\mathbb{F}_3$, et serait donc à la fois de caractéristique 2 et de caractéristique 3. ⌟

7. Vous verrez en TOPOLOGIE que le produit cartésien $X \times Y$ de deux espaces topologiques admet une topologie naturelle appelée la *topologie produit*. Cela définit le produit dans la catégorie Top.
8. Soit $\overline{\mathsf{X}}$ la catégorie associée à l'ensemble ordonné $(\mathbb{Z}, \leq)$. Pour $m, n \in \mathrm{Ob}(\overline{\mathsf{X}}) = \mathbb{Z}$, leur produit est un entier $m \times n \in \mathbb{Z}$ avec $m \times n \leq m$ et $m \times n \leq n$, et tel que pour tout $z \in \mathbb{Z}$ avec $z \leq m$ et $z \leq n$, on a $z \leq m \times n$. Il s'agit de l'infimum de l'ensemble $\{m, n\}$. On a donc $m \times n = \inf(m, n)$ dans $\overline{\mathsf{X}}$.
   Il en va de même pour tout ensemble ordonné $(X, \leq)$.

N'est-il pas tout à fait remarquable de rassembler en une seule et même notion des constructions a priori aussi disparates que le produit cartésien de deux ensembles et le minimum de deux entiers ? C'est une excellente illustration du pouvoir unificateur du langage des catégories.

I.3.4 Coproduits

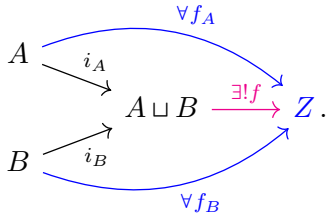
En langage des catégories, le suffixe *co-* signifie qu'on "renverse toutes les flèches". Ainsi, si le produit de A et B dans $\mathscr{C}$ est l'objet final dans la catégorie $\mathscr{C}_{A,B}$, leur *coproduit* est l'objet initial dans la catégorie $\mathscr{C}^{A,B}$.

Cela mène à la définition suivante.

Définition I.20

Soient $\mathscr{C}$ une catégorie, et A, B deux objets de $\mathscr{C}$. Un **coproduit** de A et B dans $\mathscr{C}$ consiste en la donnée d'un objet $A \sqcup B$ de $\mathscr{C}$ et de deux morphismes $i_A \in \mathrm{Hom}_{\mathscr{C}}(A, A \sqcup B)$ et $i_B \in \mathrm{Hom}_{\mathscr{C}}(B, A \sqcup B)$ tels que : $\forall Z \in \mathrm{Ob}(\mathscr{C})$, $\forall f_A \in \mathrm{Hom}_{\mathscr{C}}(A, Z)$ et $\forall f_B \in \mathrm{Hom}_{\mathscr{C}}(B, Z)$, $\exists! f \in \mathrm{Hom}_{\mathscr{C}}(A \sqcup B, Z)$ avec $f i_A = f_A$ et $f i_B = f_B$.

En d'autres termes, un coproduit de A et B dans $\mathscr{C}$ est un objet initial dans la catégorie $\mathscr{C}^{A,B}$. Cette propriété universelle est appelée la *propriété universelle du coproduit*. Elle est illustrée dans le diagramme commutatif suivant dans $\mathscr{C}$:



Les remarques faites pour le produit restent valides pour le coproduit : un coproduit de A et B dans $\mathscr{C}$ n'existe pas toujours, mais s'il existe, il est unique à unique isomorphisme de $\mathscr{C}^{A,B}$ près. En particulier, deux tels coproduits sont isomorphes dans $\mathscr{C}$, et l'on dit donc *le* coproduit de A et B dans $\mathscr{C}$.

Nous terminons cette section avec une liste d'exemples de coproduits, suivant une nouvelle fois la liste de catégories vues en Section I.1.

Exemples I.21 (coproduits)**.**

1. Dans la catégorie Set, le coproduit de deux ensembles A, B est leur union disjointe, ce qui justifie la notation.

   ⌜ Construisons l'union disjointe de A et B par $A \sqcup B := (\{0\} \times A) \cup (\{1\} \times B)$, et définissons $i_A : A \to A \sqcup B$ et $i_B : B \to A \sqcup B$ via $i_A(a) = (0, a)$ et $i_B(b) = (1, b)$ pour tous $a \in A$ et $b \in B$. Pour tout ensemble Z et toutes applications $f_A : A \to Z$ et $f_B : B \to Z$, il existe une unique application $f : A \sqcup B \to Z$ telle que $f \circ i_A = f_A$ et $f \circ i_B = f_B$: elle est donnée par $f(0, a) = f_A(a)$ et $f(1, b) = f_B(b)$. ⌟

   Ce que cette propriété universelle dit dans le cas de Set, c'est simplement que la donnée d'une application $A \sqcup B \to Z$ est équivalente à la donnée de deux applications $A \to Z$ et $B \to Z$: ses restrictions.

   Notons que cette construction de $A \sqcup B$ n'est pas unique, et c'est normal : en tant qu'objet initial, le coproduit n'est pas unique, mais seulement unique à unique bijection près (dans $\mathsf{Set}^{\mathsf{A},\mathsf{B}}$).
2. Le coproduit existe dans la catégorie Grp, mais il est difficile à contruire : il est appelé *produit libre* et sera l'objet de la Sous-section II.3.5.
3. Le coproduit existe dans Ab, et coïncide avec le produit : c'est un exercice.
4. Il en va de même dans K-Vect (et plus généralement dans la catégorie A-Mod des A-modules, comme on le verra en Sous-section II.5.3).
5. Le coproduit existe dans Ann, et porte le nom de *produit tensoriel*, mais sa construction dépasse le cadre de ce cours.
6. Les coproduits n'existent en général pas dans la catégorie des corps : c'est un exercice.
7. Vous verrez (sans doute) en TOPOLOGIE que l'union disjointe $X \sqcup Y$ de deux espaces topologiques admet une topologie naturelle appelée la *topologie de l'union disjointe*. C'est le coproduit dans Top.
8. Si $\overline{\mathsf{X}}$ est la catégorie obtenue à partir d'un ensemble ordonné $(X, \leq)$, par exemple $(\mathbb{Z}, \leq)$, alors on montre facilement que le coproduit de deux éléments de X est donné par leur supremum.

Cette liste d'exemples conclut cette sous-section sur le coproduit, et cette section sur les propriétés universelles.

I.4 Foncteurs

Bien entendu, il est souvent naturel et intéressant de relier deux catégories entre elles ; la manière naturelle de le faire est via un *foncteur*, qu'il s'agit maintenant de définir.

Définition I.22

Soient $\mathscr{C}$ et $\mathscr{D}$ deux catégories. Un **foncteur** (ou **foncteur covariant**)

$$\mathscr{F}\colon\mathscr{C}\longrightarrow\mathscr{D}$$

associe :

- à chaque objet $A\in\mathrm{Ob}(\mathscr{C})$ un objet $\mathscr{F}(A)\in\mathrm{Ob}(\mathscr{D})$;
- à chaque $f\in\mathrm{Hom}_{\mathscr{C}}(A,B)$ un morphisme $\mathscr{F}(f)\in\mathrm{Hom}_{\mathscr{D}}(\mathscr{F}(A),\mathscr{F}(B))$;

de telle manière que :

(i) pour tout objet $A\in\mathrm{Ob}(\mathscr{C})$, on a $\mathscr{F}(1_A)=1_{\mathscr{F}(A)}$;

(ii) pour tous $f\in\mathrm{Hom}_{\mathscr{C}}(A,B), g\in\mathrm{Hom}_{\mathscr{C}}(B,C)$, on a $\mathscr{F}(gf)=\mathscr{F}(g)\mathscr{F}(f)$.

Un **foncteur contravariant** $\mathscr{G}\colon\mathscr{C}\to\mathscr{D}$ est défini comme un foncteur covariant $\mathscr{G}\colon\mathscr{C}^{\mathrm{op}}\to\mathscr{D}$.

Remarques I.23.

1. Ainsi, un foncteur covariant $\mathscr{F}\colon\mathscr{C}\to\mathscr{D}$ envoie le diagramme

$$A\xrightarrow{f}B\xrightarrow{g}C\,. \qquad \text{(I.5)}$$
$$\qquad\qquad\searrow^{gf}$$

dans la catégorie $\mathscr{C}$ sur le diagramme

$$\mathscr{F}(A)\xrightarrow{\mathscr{F}(f)}\mathscr{F}(B)\xrightarrow{\mathscr{F}(g)}\mathscr{F}(C)\,.$$
$$\qquad\qquad\searrow^{\mathscr{F}(gf)=\mathscr{F}(g)\mathscr{F}(f)}$$

dans $\mathscr{D}$. On en déduit que $\mathscr{F}$ envoie tout diagramme commutatif dans $\mathscr{C}$ sur un diagramme commutatif dans $\mathscr{D}$.

2. En revanche, un foncteur contravariant $\mathscr{G}\colon\mathscr{C}\to\mathscr{D}$ envoie un morphisme

$$f\in\mathrm{Hom}_{\mathscr{C}}(A,B)=\mathrm{Hom}_{\mathscr{C}^{\mathrm{op}}}(B,A)$$

sur un morphisme $\mathscr{G}(f)\in\mathrm{Hom}_{\mathscr{D}}(\mathscr{G}(B),\mathscr{G}(A))$, et le diagramme commutatif (I.5) dans $\mathscr{C}$ sur le diagramme commutatif

$$\mathscr{G}(A)\xleftarrow{\mathscr{G}(f)}\mathscr{G}(B)\xleftarrow{\mathscr{G}(g)}\mathscr{G}(C)\,.$$
$$\qquad\qquad\nwarrow_{\mathscr{G}(gf)=\mathscr{G}(f)\mathscr{G}(g)}$$

dans $\mathscr{D}$. L'axiome (ii) se traduit donc par l'égalité $\mathscr{G}(gf) = \mathscr{G}(f)\mathscr{G}(g)$ dans le cas contravariant. Par conséquent, un foncteur contravariant $\mathscr{G}$ envoie tout diagramme commutatif dans $\mathscr{C}$ sur un diagramme commutatif dans $\mathscr{D}$, mais il "renverse les flèches".

3. Un foncteur (covariant ou contravariant) $\mathscr{F}\colon\mathscr{C} \to \mathscr{D}$ envoie les isomorphismes de $\mathscr{C}$ sur des isomorphismes de $\mathscr{D}$.

   ⌜ Supposons $\mathscr{F}$ covariant, et soit $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ un isomorphisme. Par définition, il existe $g \in \mathrm{Hom}_{\mathscr{C}}(B, A)$ tel que $gf = 1_A$ et $fg = 1_B$. On a donc des morphismes $\mathscr{F}(f) \in \mathrm{Hom}_{\mathscr{D}}(\mathscr{F}(A), \mathscr{F}(B))$ et $\mathscr{F}(g) \in \mathrm{Hom}_{\mathscr{D}}(\mathscr{F}(B), \mathscr{F}(A))$ tels que

   $$\mathscr{F}(g)\mathscr{F}(f) = \mathscr{F}(gf) = \mathscr{F}(1_A) = 1_{\mathscr{F}(A)} \quad \text{et} \quad \mathscr{F}(f)\mathscr{F}(g) = \mathscr{F}(fg) = \mathscr{F}(1_B) = 1_{\mathscr{F}(B)}\,.$$

   Ainsi $\mathscr{F}(f)$ est bien un isomorphisme de $\mathscr{D}$, d'inverse $\mathscr{F}(g)$. La preuve dans le cas contravariant est essentiellement identique. ⌟

   En particulier, si A, B sont deux objets isomorphes dans $\mathscr{C}$, alors $\mathscr{F}(A), \mathscr{F}(B)$ sont isomorphes dans $\mathscr{D}$.

   Ainsi, un foncteur est un outil pour obtenir des "invariants" : afin de montrer que deux objets A, B de $\mathscr{C}$ ne sont pas isomorphes (ce qui peut être difficile), il suffit de construire un foncteur $\mathscr{F}\colon\mathscr{C} \to \mathscr{D}$ tel que $\mathscr{F}(A)$ et $\mathscr{F}(B)$ ne sont pas isomorphes dans $\mathscr{D}$ (ce qui peut être plus facile).

   Vous en verrez des exemples plus loin, et tout au long de vos études.

4. Par la Remarque 3 ci-dessus et la Définition I.22, un foncteur $\mathscr{F}\colon\mathscr{C} \to \mathscr{D}$ définit pour tout objet A de $\mathscr{C}$ un homomorphisme de groupes

   $$\mathrm{Aut}_{\mathscr{C}}(A) \longrightarrow \mathrm{Aut}_{\mathscr{D}}(\mathscr{F}(A))\,,\, f \longmapsto \mathscr{F}(f)\,.$$

5. L'identité $1_{\mathscr{C}}\colon\mathscr{C} \to \mathscr{C}$ est trivialement un foncteur, et la composition de deux foncteurs $\mathscr{F}\colon\mathscr{C} \to \mathscr{D}$ et $\mathscr{G}\colon\mathscr{D} \to \mathscr{E}$ est également un foncteur... Vous l'avez deviné : il existe une catégorie des catégories [14], dont les objets sont les catégories et les morphismes les foncteurs !

Après toutes ces remarques, il est grand temps d'en venir aux exemples, en commençant par les plus triviaux et en terminant par certains que vous ne verrez en détail qu'en troisième année. Une fois de plus, vous allez vite vous apercevoir que des foncteurs, vous en connaissez déjà des quantités.

Exemples I.24 (foncteurs)**.**

1. Étant donné un groupe G, on peut "oublier" la structure de groupe et ne plus considérer que l'ensemble sous-jacent $\mathscr{F}(G)$. De même, un homomorphisme de groupes $\varphi\colon G \to H$ définit une application $\mathscr{F}(\varphi)\colon\mathscr{F}(G) \to \mathscr{F}(H)$. On obtient ainsi ce qu'on appelle un *foncteur oubli*

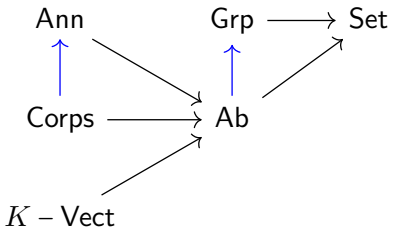
   $$\mathscr{F}\colon \mathsf{Grp} \longrightarrow \mathsf{Set}\,,$$

   qui est clairement un foncteur covariant.

14. À cela près que cette catégorie n'est pas localement petite, voir la note 3.

Sur cet exemple, la Remarque 3 ci-dessus se traduit en l'énoncé suivant : tout isomorphisme de groupes est une bijection. Et effectivement, c'est une bonne première manière de tenter de distinguer deux groupes non-isomorphes : si deux groupes n'ont pas même ordre, alors ils ne sont pas isomorphes.

2. Il existe bien évidemment une foule de foncteurs oublis similaires : certains sont des oublis de structures (comme $\mathsf{Grp} \to \mathsf{Set}$ ci-dessus), d'autres des oublis de propriété (comme $\mathsf{Ab} \to \mathsf{Grp}$, où l'on oublie qu'un groupe abélien est abélien). En voici quelques-uns dans un diagramme de catégories, avec les oublis de structure en noir et les oublis de propriété en bleu :



Sur tous ces exemples, la Remarque 3 s'illustre de manière un peu triviale, mais pas totalement inutile. Par exemple, si deux anneaux sont isomorphes, alors ils doivent être isomorphes comme groupes abéliens.

3. Un *foncteur constant* $\mathscr{F}\colon \mathscr{C} \to \mathscr{D}$ associe à tout objet A de $\mathscr{C}$ le même objet $\mathscr{F}(A) = X$ de $\mathscr{D}$, et à tout morphisme $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ l'identité

$$\mathscr{F}(f) = 1_X \in \mathrm{Hom}_{\mathscr{D}}(X, X) = \mathrm{Hom}_{\mathscr{D}}(\mathscr{F}(A), \mathscr{F}(B)) .$$

4. Étant donné un anneau A, on note $U(A)$ son groupe des unités (ou A^*). Cela définit un foncteur $\mathscr{U}\colon \mathsf{Ann} \to \mathsf{Grp}$ (exercice).

   Ici, la Remarque 3 est un peu moins triviale : si A et B sont deux anneaux isomorphes, alors leurs groupes d'unités $U(A)$ et $U(B)$ sont isomorphes.

5. Soit $\mathscr{G}\colon K\text{-}\mathsf{Vect} \to \mathsf{K\text{-}Vect}$ qui associe :
   - à tout K-espace vectoriel E son *dual* $\mathscr{G}(E) = E^* := \mathrm{Hom}_{K-\mathsf{Vect}}(E, K)$;
   - à toute application K-linéaire $f\colon E \to F$ l'application $\mathscr{G}(f) = f^*\colon F^* \to E^*$ définie par $f^*(\varphi) = \varphi \circ f$ pour $\varphi \in F^*$.

   On vérifie qu'il s'agit d'un foncteur contravariant, puisqu'il satisfait les égalités $(\mathrm{id}_E)^* = \mathrm{id}_{E^*}$ pour tout K-espace vectoriel E et $(g \circ f)^* = f^* \circ g^*$ pour toutes applications linéaires $f\colon E \to F$ et $g\colon F \to V$.

   ⌜ En effet, pour tout $\varphi \in E^*$, on a

$$(\mathrm{id}_E)^*(\varphi) = \varphi \circ \mathrm{id}_E = \varphi = \mathrm{id}_{E^*}(\varphi) ,$$

   tandis que

$$(g \circ f)^*(\psi) = \psi \circ (g \circ f) = (\psi \circ g) \circ f = f^*(\psi \circ g) = f^*(g^*(\psi) = (f^* \circ g^*)(\psi)$$

   pour tout $\psi \in V^*$.

   ⌟

6. Soient $(X, \sim)$ et $(Y, \sim)$ deux ensembles préordonnés, et soit $f : X \to Y$ une application telle que $x \sim x' \in X$ implique $f(x) \sim f(x') \in Y$. Alors, f définit un foncteur $\overline{f} : \overline{X} \to \overline{Y}$: c'est un exercice.

7. Voici un magnifique exemple issu de l'analyse.
   Soit Diff^* la catégorie des *applications différentiables pointées*, définie comme suit.
   - Les objets de Diff^* sont les paires (U, a) avec $a \in U$ et U un ouvert de $\mathbb{R}^n$ pour un certain $n \geq 0$.
   - Pour (U, a) et (V, b) de tels objets, les morphismes $(U, a) \to (V, b)$ dans Diff^* sont les applications différentiables $f : U \to V$ avec $f(a) = b$.

   Notons qu'il s'agit de la catégorie $\mathscr{C}^A$ avec $\mathscr{C} = \mathsf{Diff}$ et $A = \{*\}$, ce qui justifie la notation. [15]

   Soit $D : \mathsf{Diff}^* \to \mathbb{R}\text{-}\mathsf{Vect}$ défini comme suit.
   - Pour un objet (U, a) de Diff^* avec $U \subset \mathbb{R}^n$, on pose $D(U, a) = \mathbb{R}^n$, qui est bien un espace vectoriel réel, donc un objet de $\mathbb{R}\text{-}\mathsf{Vect}$.
   - Pour $f : U \to V$ avec $a \in U \subset \mathbb{R}^n$ et $b \in V \subset \mathbb{R}^m$ satisfaisant $f(a) = b$, on pose $D(f) = D_a f$ la dérivée de f en $a \in U \subset \mathbb{R}^n$, qui est bien une application $\mathbb{R}$-linéaire de $D(U, a) = \mathbb{R}^n$ dans $D(V, b) = \mathbb{R}^m$.

   Il s'agit bel et bien d'un foncteur :

   (i) Pour tout objet (U, a) de Diff^* avec U ouvert de $\mathbb{R}^n$, on a
   $$D(1_{(U,a)}) = D(\mathrm{id}_U) = D_a(\mathrm{id}_U) = \mathrm{id}_{\mathbb{R}^n} = 1_{D(U,a)}$$
   puisque la dérivée de l'application identité est l'identitié.

   (ii) Étant donné deux applications différentiables pointées $f : (U, a) \to (V, b)$ et $g : (V, b) \to (W, c)$, on a
   $$D(g \circ f) = D_a(g \circ f) = D_{f(a)}(g) \circ D_a(f) = D_b(g) \circ D_a(f) = D(g) \circ D(f)$$
   par la règle de dérivation en chaîne.

   Inutile de préciser que ce foncteur est extrêmement utile. Via la Remarque 3 ci-dessus, on obtient immédiatement le résultat suivant : si $U \subset \mathbb{R}^n$ et $V \subset \mathbb{R}^m$ sont difféomorphes, alors $\mathbb{R}^n$ et $\mathbb{R}^m$ sont des $\mathbb{R}$-espaces vectoriels isomorphes, et donc $n = m$. En particulier, les espaces $\mathbb{R}^n$ et $\mathbb{R}^m$ ne sont jamais difféomorphes pour $n \neq m$. Cet énoncé est déjà bien moins trivial que les précédents. [16]

8. Voici pour terminer un exemple issu de la *topologie algébrique*, que vous verrez en détail dans un cours dédié en troisième année.

15. Cette notation qui n'a en revanche rien à voir avec le dual d'un espace vectoriel défini en Exemple 5.

16. Il est très naturel à ce stade de se poser la même question dans la catégorie topologique : si $U \subset \mathbb{R}^n$ et $V \subset \mathbb{R}^m$ sont deux ouverts homéomorphes, a-t-on nécessairement $n = m$? La réponse est affirmative, un résultat qui porte le nom d'*invariance de la dimension.* Les preuves modernes de cet énoncé reposent sur la construction de foncteurs $\mathsf{Top} \to \mathsf{Ab}$ adéquats, qu'on étudie en *théorie de l'homologie*.

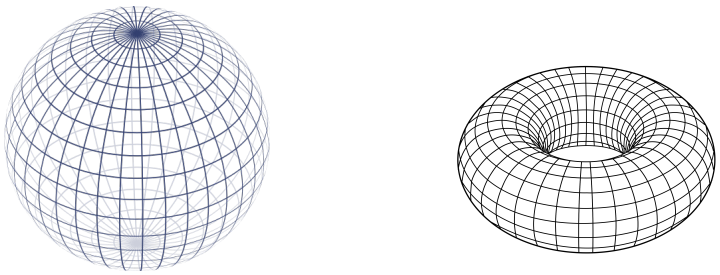


FIGURE 1 – La sphère et le tore.

Le *groupe fondamental* est un foncteur $\pi_1 \colon \mathsf{Top}^* \to \mathsf{Grp}$, qui associe donc à tout espace topologique pointé (X, x_0) un groupe $\pi_1(X, x_0)$. Par la Remarque 3, si deux espaces pointés (X, x_0) et (Y, y_0) sont tels que les groupes $\pi_1(X, x_0)$ et $\pi_1(Y, y_0)$ ne sont pas isomorphes (ce qui est souvent facile à vérifier), alors les espaces (pointés) ne sont pas homéomorphes (ce qui est parfois difficile à montrer sans ce genre d'outil).
Par exemple, la sphère $\mathbb{S}^2$ et le tore $\mathbb{T}^2$ illustrés en Figure 1 satisfont $\pi_1(\mathbb{S}^2) = 0$ et $\pi_1(\mathbb{T}^2) \simeq \mathbb{Z}^2$ (indépendamment du point base), ce qui montre que ces deux espaces ne sont pas homéomorphes. Ce résultat est impossible à obtenir avec les outils développés en topologie générale (connexité, compacité, etc.)

Exercices

1. Soit Ord la structure définie via
   - $\mathrm{Ob}(\mathsf{Ord})$ la classe des ensembles ordonnés ;
   - $\mathrm{Hom}_{\mathsf{Ord}}(X, Y)$ l'ensemble des applications $X \to Y$ croissantes, pour tous X, Y dans $\mathrm{Ob}(\mathsf{Ord})$.

   Montrer qu'il s'agit d'une catégorie.
   Les ensembles ordonnés et les applications décroissantes forment-ils une catégorie ?

2. Rappelons qu'un *monoïde* est un ensemble E muni d'une loi de composition $*$ interne associative et d'un élément neutre e pour cette loi. Un *morphisme* de $(E, *, e)$ vers $(E', *', e')$ est une application $\varphi \colon E \to E'$ telle que $\varphi(x * y) = \varphi(x) *' \varphi(y)$ pour tous $x, y \in E$ et telle que $\varphi(e) = e'$.
   (i) Montrer que la première condition n'implique pas forcément la seconde.
   (ii) Vérifier que cela forme une catégorie, qu'on notera Mon.

3. Étant donné un ensemble X, soit $\hat{\mathsf{X}}$ la structure définie via
   - $\mathrm{Ob}(\hat{\mathsf{X}}) = \mathscr{P}(X)$, l'ensemble des sous-ensembles de X ;
   - pour $A, B \in \mathrm{Ob}(\hat{\mathsf{X}})$ (i.e. $A \subset X$ et $B \subset X$), on pose $\mathrm{Hom}_{\hat{\mathsf{X}}}(A, B) = \{(A, B)\}$ si $A \subset B$ et $\mathrm{Hom}_{\hat{\mathsf{X}}}(A, B) = \varnothing$ sinon.

   Montrer qu'il s'agit bien d'une catégorie.
   Est-ce un cas particulier d'un exemple vu en cours ?

4. Pour K un corps, soit $\mathsf{Mat_K}$ la structure définie via
   - $\mathrm{Ob}(\mathsf{Mat_K}) = \{0, 1, 2, \dots\}$;
   - $\mathrm{Hom}(m, n) = \mathrm{Mat}_K(n, m)$, l'ensemble des matrices à n lignes et m colonnes et coefficients dans K, pour tous $m, n \in \{0, 1, 2, \dots\}$.

   Montrer qu'il s'agit d'une catégorie (pour la composition donnée par la multiplication matricielle).

5. Soit $\mathscr{C}$ une catégorie. Considérons la structure $\mathscr{C}^{\mathrm{op}}$ avec
   - $\mathrm{Ob}(\mathscr{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathscr{C})$;
   - $\mathrm{Hom}_{\mathscr{C}^{\mathrm{op}}}(A, B) = \mathrm{Hom}_{\mathscr{C}}(B, A)$ pour tous A, B dans $\mathrm{Ob}(\mathscr{C}^{\mathrm{op}})$.

   Montrer qu'il s'agit d'une catégorie.
   On parle de la catégorie *duale* ou *opposée* à $\mathscr{C}$.

6. Étant donnée une catégorie $\mathscr{C}$ et un objet $A \in \mathrm{Ob}(\mathscr{C})$, on a vu comment définir une catégorie associée notée $\mathscr{C}_A$. De manière analogue, montrer comment définir une catégorie $\mathscr{C}^A$ dont les objets sont

$$\mathrm{Ob}(\mathscr{C}^A) = \{f \in \mathrm{Hom}_{\mathscr{C}}(A, Z) \mid Z \in \mathrm{Ob}(\mathscr{C})\}.$$

   Avec la notation de l'exercice 5, montrer que pour tout objet A de $\mathscr{C}$, les catégories $(\mathscr{C}^{\mathrm{op}})_A$ et $\left(\mathscr{C}^A\right)^{\mathrm{op}}$ coïncident, de même que les catégories $(\mathscr{C}^{\mathrm{op}})^A$ et $(\mathscr{C}_A)^{\mathrm{op}}$.

7. Tenter de comprendre les catégories $\mathscr{C}_A$ et $\mathscr{C}^A$ pour $\mathscr{C} = \mathsf{Set}$ et A un ensemble à deux éléments. Quels sont les isomorphismes dans ces catégories ?

8. Tenter de comprendre les catégories $\mathscr{C}_A$ et $\mathscr{C}^A$ pour $\mathscr{C}$ la catégorie définie via l'ensemble ordonné $(\mathbb{Z}, \leq)$ et $A \in \mathrm{Ob}(\mathscr{C})$ un élément quelconque $n \in \mathbb{Z}$.

9. Soient $\mathscr{C}$ une catégorie quelconque et $A, B \in \mathrm{Ob}(\mathscr{C})$. Vérifier que la catégorie $\mathscr{C}_{A,B}$ définie en cours est bel et bien une catégorie.

10. Tenter de comprendre les catégories $\mathscr{C}_{A,B}$ et $\mathscr{C}^{A,B}$ pour $\mathscr{C} = \mathsf{Set}$ et $A = B = \{*\}$ un singleton. Quels sont les isomorphismes dans ces catégories ?

11. Considérons la catégorie $\overline{\mathsf{X}}$ définie à partir d'un ensemble X muni d'une relation d'équivalence. Déterminer quand deux objets $x, y \in \mathrm{Ob}(\overline{\mathsf{X}}) = X$ sont isomorphes dans $\overline{\mathsf{X}}$.

12. Montrer que pour tout groupe G, il existe une catégorie $\mathscr{C}$ et un objet $A \in \mathrm{Ob}(\mathscr{C})$ tels que $\mathrm{Aut}_{\mathscr{C}}(A) \simeq G$.

13. (i) Montrer que le monoïde $\mathrm{End}_{\mathsf{Gr}}(\mathbb{Z})$ est isomorphe à $\mathbb{Z}$ muni de la multiplication.
    (ii) En déduire que le groupe $\mathrm{Aut}_{\mathsf{Gr}}(\mathbb{Z})$ est isomorphe à $\{\pm 1\}$.
    (iii) Plus généralement, calculer le monoïde $\mathrm{End}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z})$ et le groupe $\mathrm{Aut}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z})$ pour tout $n \geq 0$.

14. Une catégorie où tous les morphismes sont des isomorphismes est appelée un *groupoïde*.
    (i) Montrer qu'un groupoïde avec un seul objet n'est autre qu'un groupe.

(ii) Dans le cas de la catégorie $\overline{\mathsf{X}}$ construite à partir d'un ensemble préordonné, quand obtient-on un groupoïde ?

15. (i) Montrer que si deux objets X, Y d'une catégorie $\mathscr{C}$ sont isomorphes, alors les monoïdes $\mathrm{End}_{\mathscr{C}}(X)$ et $\mathrm{End}_{\mathscr{C}}(Y)$ sont isomorphes, de même que les groupes $\mathrm{Aut}_{\mathscr{C}}(X)$ et $\mathrm{Aut}_{\mathscr{C}}(Y)$.
(ii) Illustrer ces résultats dans le cas des catégories Set et K-Vect.

16. Déterminer les objets initiaux et finaux de la catégorie $\hat{\mathsf{X}}$ de l'exercice 3.

17. Montrer que $\mathbb{Z}$ est un objet initial dans la catégorie Ann des anneaux.

18. Soit $\overline{\mathsf{X}}$ la catégorie construite à partir d'un ensemble préordonné $(X, \sim)$. Déterminer quand $\overline{\mathsf{X}}$ admet un objet initial/final si le préordre est
(i) une relation d'équivalence ;
(ii) une relation d'ordre.

19. Montrer que si I est un objet initial dans une catégorie $\mathscr{C}$ et A est un objet de $\mathscr{C}$, alors l'unique $f \in \mathrm{Hom}_{\mathscr{C}}(I, A)$ est initial dans la catégorie $\mathscr{C}_A$.

20. Discuter les propriétés universelles du quotient dans les catégories Ab, Ann, Corps et K-Vect, et les théorèmes d'isomorphisme qui en découlent.

21. Vérifier que le produit direct de groupes satisfait bien la propriété universelle du produit dans Grp, tandis que c'est la somme directe d'espaces vectoriels qui la satisfait dans K-Vect.

22. Soient $\overline{\mathsf{X}}$ la catégorie obtenue à partir d'un ensemble préordonné $(X, \sim)$, et x, y deux objets fixés. Étudier l'existence et l'unicité du produit $x \times y$ et du coproduit $x \coprod y$ lorsque $\sim$ est une relation d'ordre, et lorsque c'est une relation d'équivalence.

23. Vérifier que le coproduit de deux groupes abéliens est donné par leur somme directe, et qu'il en va de même dans la catégorie des K-espaces vectoriels.

24. Montrer que les coproduits n'existent en général pas dans la catégorie des corps.

25. (i) Déterminer les produits et coproduits dans la catégorie $\hat{\mathsf{X}}$ (exercice 3).
(ii) Faire de même dans la catégorie Ord (exercice 1).

26. Soit $(X, \sim)$ l'ensemble $\mathbb{Z}$ muni de la relation de divisibilité, usuellement notée $a|b$. Comme cette relation est réflexive et transitive, on peut lui associer une catégorie $\overline{\mathsf{X}}$.
(i) Déterminer quand deux objets de cette catégorie sont isomorphes.
(ii) Cette catégorie admet-elle des objets initiaux ? et finaux ?
(iii) Déterminer les produits et coproduits dans cette catégorie. Quels sont leurs noms conventionels ?

27. Montrer que dans toute catégorie $\mathscr{C}$ et tous objets A, B, les produits $A \times B$ et $B \times A$ sont isomorphes s'ils existent, et de même pour les coproduits $A \coprod B$ et $B \coprod A$.

28. Soient F un objet final dans une catégorie $\mathscr{C}$, et A un objet quelconque de $\mathscr{C}$.

(i) Montrer que le produit $F \times A$ dans $\mathscr{C}$ satisfait $F \times A \simeq A$.
(ii) Illustrer ce fait dans les catégories Set et Grp.

Existe-t-il un énoncé analogue pour les objets initiaux ?

29. Quels sont les objets finaux et initiaux dans la catégorie des catégories ?

30. Montrer que le groupe des unités définit un foncteur covariant $\mathscr{U} : \mathsf{Ann} \to \mathsf{Grp}$.

31. Soient $(X, \sim)$ et $(Y, \sim)$ deux ensembles préordonnés et $f : X \to Y$ une application *croissante*, i.e. telle que

$$x \sim x' \in X \Rightarrow f(x) \sim f(x') \in Y$$

pour tous $x, x' \in X$. Vérifier que f définit un foncteur covariant $\overline{\mathsf{f}} : \overline{\mathsf{X}} \to \overline{\mathsf{Y}}$ via $\overline{\mathsf{f}}(x) = f(x)$ pour tout $x \in \mathrm{Ob}(\overline{\mathsf{X}}) = X$.

32. (i) Vérifier qu'il existe un foncteur oubli $\mathscr{O} : \mathsf{Grp} \to \mathsf{Mon}$.
(ii) Montrer qu'assigner à chaque monoïde E ses éléments inversibles

$$\mathscr{U}(E) := \{x \in E \mid \text{il existe } y \in E \text{ avec } xy = yx = e\}$$

permet de définir un foncteur $\mathscr{U} : \mathsf{Mon} \to \mathsf{Grp}$.
(iii) Vérifier que ces deux foncteurs sont liés de la façon suivante : pour tout groupe G et monoïde E, on a une bijection

$$\mathrm{Hom}_{\mathsf{Mon}}(\mathscr{O}(G), E) \cong \mathrm{Hom}_{\mathsf{Grp}}(G, \mathscr{U}(E)) .$$

Remarque. On dit que $\mathscr{O}$ et $\mathscr{U}$ sont des *foncteurs adjoints*. Plus précisément, on dit que $\mathscr{O}$ est *adjoint à gauche* de $\mathscr{U}$ et que $\mathscr{U}$ est *adjoint à droite* de $\mathscr{O}$.

Chapitre II: Groupes

Le but de ce second chapitre est de poursuivre l'étude de la théorie des groupes initiée en ALGÈBRE I. Certains résultats joueront un rôle majeur dans la suite du cours, en particulier ceux sur les groupes résolubles (Section II.2) en théorie de Galois (Chapitre IV).

II.1 Rappels sur les groupes

Il est toujours très agréable pour les étudiants de commencer un chapitre par des rappels. Mais dans le cas présent, comme ces rappels portent potentiellement sur près de la moitié du cours d'ALGÈBRE I, nous risquons d'y perdre beaucoup de temps et par conséquent, de ne pouvoir atteindre les buts énoncés en introduction.

Pour ces raisons, nous avons décidé de rédiger les rappels les plus utiles dans cette section, avec quelques compléments, mais de le faire de manière très concise et de ne pas les discuter en détail pendant le cours. Vous avez donc la responsabilité de les lire, et la possibilité de poser toutes vos questions lors d'une séance d'exercices (en partie) dédiée.

Comme vous le savez, la *catégorie des groupes*, notée Grp, est définie ainsi :

- Les objets de Grp sont les *groupes*, i.e. les ensembles G munis d'une loi de composition $G \times G \to G$, $(g_1, g_2) \mapsto g_1 g_2$ associative, avec un neutre e_G, et telle que chaque élément $g \in G$ admet un inverse $g^{-1} \in G$.
- Les morphismes de Grp sont les *homomorphismes de groupes*, i.e. les applications $\varphi : G \to G$ telles que $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ pour tous $g_1, g_2 \in G$.

Un sous-ensemble H d'un groupe G est un *sous-groupe* de G, noté $H < G$, si la restriction de la loi de $G \times G$ à $H \times H$ fait de H un groupe. On vérifie que c'est équivalent à demander que H soit non-vide et satisfasse $h_1^{-1} h_2 \in H$ pour tous $h_1, h_2 \in H$.

Pour tout sous-groupe $H < G$ fixé, la relation $g_1 \sim_H g_2 :\Leftrightarrow g_2^{-1} g_1 \in H$ définit une relation d'équivalence sur G. Les classes d'équivalence correspondantes sont les classes à gauche modulo H :

$$[g]_H := \{g' \in G \mid g' \sim_H g\} = \{g' \in G \mid g' \in gH\} = gH\,.$$

On note G/H l'ensemble quotient, et $[G : H] := |G/H|$ est appelé l'*indice* de H dans G. Comme les classes d'équivalences forment une partition de l'ensemble G

et sont toutes en bijection avec H, on obtient le premier résultat non-trivial de la théorie, traditionnellement attribué à Lagrange.

Théorème II.1: Théorème de Lagrange

Pour tout sous-groupe H d'un groupe fini G, on a $|G| = [G : H] \cdot |H|$.

Joseph-Louis Lagrange (1736-1813)

Venons-en aux groupes cycliques. Étant donné un sous-ensemble X d'un groupe G, on note

$$\langle X \rangle := \bigcap_{X \subset H < G} H$$

le *sous-groupe de G engendré par X*. Il s'agit du plus petit sous-groupe de G qui contient X. Pour $X = \{g\}$ un singleton, on a $\langle X \rangle =: \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. S'il existe $g \in G$ tel que $G = \langle g \rangle$, on dit que G est *cyclique*. Ces groupes sont faciles à classifier.

Théorème II.2: Classification des groupes cycliques

Soit G un groupe cyclique. Si G est infini, alors il est isomorphe à $\mathbb{Z}$. Si G est fini, alors il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour $n = |G|$.

Certains sous-groupes jouent un rôle particulièrement important : ce sont les sous-groupes normaux. En effet, on peut vérifier que la loi sur G passe au quotient et induit une loi bien définie sur G/N (faisant de G/N un groupe) si et seulement si N est un sous-groupe *normal* de G, i.e. satisfait $gNg^{-1} = N$ pour tout $g \in G$, ce qui est noté $N \triangleleft G$.

Dans ce cas, la projection canonique $\pi : G \to G/N$ est un homomorphisme de groupes de noyau $\mathrm{Ker}(\pi) = N$ et satisfait la propriété universelle du quotient déjà rappelée en Sous-section I.3.2. On peut la résumer à l'aide du diagramme suivant :

$$\begin{array}{ccc} G & \xrightarrow{\forall \varphi} & G', \\ {\scriptstyle \pi}\downarrow & \nearrow_{\exists ! \overline{\varphi}} & \\ G/N & & \end{array}$$

où l'on suppose $N \subset \mathrm{Ker}(\varphi)$ et $\overline{\varphi} \circ \pi = \varphi$. Comme on l'a vu, cela implique facilement le résultat fondamental suivant.

Théorème II.3: Premier théorème d'isomorphisme

Tout homomorphisme de groupes $\varphi : G \to G'$ induit un isomorphisme de groupes

$$\overline{\varphi} : G/\mathrm{Ker}(\varphi) \longrightarrow \mathsf{Im}(\varphi)\,.$$

L'addition du mot "premier" peut surprendre : c'est qu'il en existe deux autres, qui sont en fait des conséquences faciles du premier, comme vous l'avez vu en ALGÈBRE I.

Théorème II.4: Deuxième théorème d'isomorphisme

Pour N, H des sous-groupes d'un groupe G avec $N \triangleleft G$, l'ensemble NH est un sous-groupe de G avec $N \triangleleft NH$ et $(N \cap H) \triangleleft H$, et on a un isomorphisme

$$NH/N \simeq H/(N \cap H)\,.$$

Théorème II.5: Troisième théorème d'isomorphisme

Soit N un sous-groupe normal d'un groupe G. Les sous-groupes normaux de G/N sont de la forme H/N avec $N \subset H \triangleleft G$, et pour tout tel H, on a un isomorphisme

$$(G/N)/(H/N) \simeq G/H\,.$$

Venons-en à présent aux groupes simples. Rappelons qu'un groupe G non-trivial est dit *simple* s'il n'admet pas de sous-groupe normal propre (i.e. distinct de $\{e\}$ et de G). La classification des groupes simples abéliens est facile, et laissée en exercice.

Proposition II.6. *Soit G un groupe abélien. Alors, le groupe G est simple si et seulement si $G \simeq \mathbb{Z}/p\mathbb{Z}$ avec p premier.*

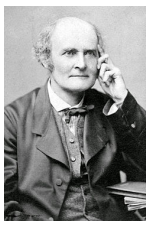
La classification des groupes (non-abéliens) finis simples est infiniment plus difficile, et dépasse de beaucoup le champ de ce cours [1]. Néanmoins, on verra une autre famille infinie de groupes simples ci-dessous (Théorème II.8), à l'aide des groupes symétriques.

Rappelons que pour tout ensemble X, on note

$$S(X) := \mathrm{Aut}_{\mathsf{Set}}(X) = \{f : X \to X \mid f \text{ bijection}\}$$

le *groupe symétrique* sur X. Comme une bijection $X \simeq Y$ induit un isomorphisme $S(X) \simeq S(Y)$, le groupe $S(X)$ ne dépend à isomorphisme près que du cardinal de X. Si X est de cardinal n, on note $S(X) =: S_n$ le *groupe des permutations de n objets* (habituellement $\{1, 2, \ldots, n\}$).

Ces groupes sont d'une importance fondamentale, et "universels" dans le sens du résultat suivant, traditionnellement attribué à CAYLEY, et dont nous verrons une preuve ci-dessous (voir Exemple II.9).



ARTHUR CAYLEY (1821-1895)

1. et les capacités du commun des mortels

Théorème II.7: Théorème de Cayley

Tout groupe est isomorphe à un sous-groupe du groupe symétrique.

Le groupe S_n est engendré par les transpositions, i.e. toute permutation $\sigma \in S_n$ est produit (d'un certain nombre $t(\sigma)$) de transpositions. Ainsi, on peut définir la *signature* de $\sigma \in S_n$ comme $\operatorname{sgn}(\sigma) = (-1)^{t(\sigma)}$. Bien-sûr, l'entier $t(\sigma)$ n'est pas bien défini, mais on peut montrer que sa parité l'est, ce qui définit un homomorphisme de groupes

$$\operatorname{sgn}\colon S_n \longrightarrow \{-1, 1\}\,.$$

Le *groupe alterné* de degré n est le sous-groupe $A_n := \operatorname{Ker}(\operatorname{sgn}) \lhd S_n$, un groupe d'ordre $\frac{n!}{2}$ pour $n \geq 2$. Par exemple, les groupes A_1 et A_2 sont triviaux, le groupe A_3 est cyclique d'ordre 3, tandis que A_4 est un groupe d'ordre 12 constitué de l'identité, des 3 doubles-transpositions, et des 8 3-cycles.

Vous avez vu la preuve (non-triviale) du résultat suivant en ALGÈBRE I. Elle repose en particulier sur le fait que le groupe A_n est engendré par les 3-cycles.

Théorème II.8

Pour tout $n \geq 5$, le groupe alterné A_n est simple.

Passons aux actions de groupes. Comme vous le savez, une *action* d'un groupe G sur un ensemble X, notée $G \curvearrowright X$, est la donnée de

$$G \times X \longrightarrow X\,, \quad (g, x) \longmapsto g \cdot x$$

telle que $e_G \cdot x = x$ et $g \cdot (h \cdot x) = (gh) \cdot x$ pour tous $x \in X$ et $g, h \in G$. C'est équivalent à la donnée d'un homomorphisme de groupes $\varphi\colon G \to S(X)$, via $\varphi(g)(x) = g \cdot x$ pour tous $g \in G$ et $x \in X$.

L'*orbite* de $x \in X$ est $G \cdot x := \{g \cdot x \mid g \in G\}$, tandis que son *stabilisateur* est

$$\operatorname{Stab}(x) := \{g \in G \mid g \cdot x = x\}\,.$$

L'action est dite *transitive* si $G \cdot x = X$ pour un certain $x \in X$ (ou pour tous) et *fidèle* si $\bigcap_{x \in X} \operatorname{Stab}(x) = \{e_G\}$, ce qui est équivalent à l'injectivité de l'homomorphisme associé.

Exemple II.9. Un groupe quelconque G agit sur $X = G$ via la loi de composition $g \cdot x = gx$ pour tous $g, x \in G$. C'est une action fidèle puisque $gx = x$ implique $g = e$. Cela donne donc un homomorphisme injectif $\varphi\colon G \to S(G)$. Par conséquent, on a un isomorphisme $G \simeq \mathsf{Im}(\varphi) < S(X)$, ce qui fournit la démonstration promise du théorème de Cayley (Théorème II.7).

Voici le dernier résultat de ce *crash course* en théorie des groupes.

Théorème II.10: Formule des orbites

Pour tout groupe fini G agissant sur un ensemble X et pour tout $x \in X$,

$$|G| = |G \cdot x| \, |\mathrm{Stab}(x)| \, .$$

II.2 Groupes résolubles

Comme mentionné plus haut, les groupes résolubles jouent un rôle majeur dans l'étude de la résolubilité des équations polynomiales en théorie de Galois : ils forment le sujet principal de cette section. Plus précisément, on commencera par définir et étudier les commutateurs en Sous-section II.2.1, avant de passer aux groupes résolubles proprement dit en Sous-section II.2.2, et de conclure avec l'abélianisation (et la propriété universelle associée) en Sous-section II.2.3.

II.2.1 Commutateurs

Comme à notre habitude, nous introduisons ces objets importants mais pas primordiaux sous la forme d'une nouvelle "terminologie", réservant les définitions numérotées pour les concepts les plus fondamentaux.

Terminologie II.11. Soit G un groupe, et soient $g, h \in G$. Le *commutateur* de g et h est

$$[g,h] := ghg^{-1}h^{-1} \in G \, .$$

Un certain nombre de remarques s'imposent, toutes élémentaires.

Remarques II.12.

1. Le commutateur de g et h est trivial si et seulement si l'on a l'égalité $gh = hg$. Par conséquent, un groupe est abélien si et seulement si tous ses commutateurs sont triviaux.

2. Si $\varphi : G \to G'$ est un homomorphisme et g, h sont deux éléments de G, alors

$$\varphi([g,h]) = \varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = [\varphi(g), \varphi(h)]$$

dans G'.

3. Pour tous $g, h \in G$, on a $[g,h]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h,g]$.

4. Pour tout $g \in G$, on a $[g,e] = [e,g] = e$.

Les Remarques 3 et 4 montrent que l'ensemble $\{[g,h] \,|\, g,h \in G\}$ des commutateurs dans G satisfait deux des trois axiomes d'un sous-groupe. Mais il ne satisfait pas le troisième : en général, la composition de deux commutateurs n'est pas un commutateur [2]. Cela justifie la terminologie suivante.

2. De tels exemples sont difficiles à construire : nous n'en verrons pas ici.

Terminologie II.13. Soit G un groupe. Le *groupe dérivé* de G est le sous-groupe $[G,G]$ de G engendré par les commutateurs, i.e.

$$[G,G] := \langle\, \{[g,h]\,|g,h \in G\}\, \rangle\ .$$

Reprenons le fil de nos remarques II.12.

5. Si H est un sous-groupe d'un groupe G, alors $[H,H]$ est un sous-groupe de $[G,G]$: c'est immédiat.

6. Si $\varphi: G \to G$ est un homomorphisme, alors $\varphi([G,G]) = [\varphi(G),\varphi(G)]$. Une inclusion découle de la Remarque 2, la seconde est un exercice.

7. En appliquant la Remarque 6 à $\varphi: G \to G$ donné par $\varphi(g) = xgx^{-1}$ avec $x \in G$ quelconque, on voit que le groupe dérivé est un sous-groupe normal de G.

8. Comme on a $[G,G] \triangleleft G$ (Remarque 7), on peut considérer le quotient $G/[G,G]$. C'est un groupe abélien (qu'on étudiera en Sous-section II.2.3).

   ⌜ En effet, soient $x, y \in G/[G,G]$ deux éléments quelconques. Comme la projection canonique $\pi: G \to G/[G,G]$ est surjective, il existe $g, h \in G$ avec $\pi(g) = x$ et $\pi(h) = y$. Par la Remarque 2, on a $[x,y] = [\pi(g),\pi(h)] = \pi([g,h]) = e$ puisque $[g,h] \in [G,G] = \mathrm{Ker}(\pi)$. Cela signifie que tous les éléments de $G/[G,G]$ commutent (Remarque 1), et donc que ce quotient est abélien. ⌟

9. La remarque précédente admet la réciproque suivante : si un quotient G/N est abélien, alors le sous-groupe normal N contient $[G,G]$: c'est un exercice.

Après cette longue liste de remarques, venons-en à des exemples explicites de groupes dérivés.

Exemples II.14 (groupes dérivés)**.**

1. Par la Remarque 1 ci-dessus, un groupe G est abélien si et seulement si $[G,G]$ est trivial.

2. Le groupe dérivé de S_n est égal à A_n.

   ⌜ Pour tous $\sigma, \tau \in S_n$ on a $\mathrm{sgn}([\sigma,\tau]) = [\mathrm{sgn}(\sigma),\mathrm{sgn}(\tau)] = 1$ par la Remarque 2 et le fait que $\{-1,1\}$ est abélien, d'où $[\sigma,\tau] \in A_n$. Comme A_n est un sous-groupe de S_n, cela montre l'inclusion $[S_n,S_n] \subset A_n$. Pour vérifier l'autre inclusion, comme A_n est engendré par les 3-cycles, il suffit de montrer que tout 3-cycle est un commutateur. C'est le cas, via l'égalité $(i,j,k) = [(j,k),(i,j)] \in S_n$. ⌟

3. Pour tout corps K et tout entier $n \neq 2$, on a

$$[\mathrm{GL}(n,K),\mathrm{GL}(n,K)] = \mathrm{SL}(n,K)\,, \quad [\mathrm{SL}(n,K),\mathrm{SL}(n,K)] = \mathrm{SL}(n,K)\,.$$

   On verra la preuve en exercices (avec de multiples indications).

II.2.2 Groupes résolubles

Venons-en au sujet principal de cette section. Il existe plusieurs définitions possibles pour les groupes résolubles (voir Proposition II.21) ; nous allons opter pour celle qui repose sur la notion de suite dérivée.

Terminologie II.15. Pour un groupe G, on note

$$G^{(0)} := G, \quad G^{(1)} := [G, G], \quad \dots \quad , \quad G^{(k+1)} := [G^{(k)}, G^{(k)}] \text{ pour tout } k \geq 0\,.$$

On obtient donc une suite de sous-groupes normaux

$$\cdots \lhd G^{(k+1)} \lhd G^{(k)} \lhd \cdots \lhd G^{(2)} \lhd G^{(1)} \lhd G^{(0)} = G\,,$$

appelée la *suite dérivée* de G.

Définition II.16

Un groupe G est dit **résoluble** s'il existe $n \geq 0$ tel que $G^{(n)} = \{e\}$.

Commençons par quelques remarques, avant de passer aux exemples. Des résultats plus profonds suivront.

Remarques II.17.

1. Pour un sous-groupe $H < G$, on a l'inclusion $H^{(k)} \subset G^{(k)}$ pour tout $k \geq 0$. Cela se démontre par récurrence sur $k \geq 0$ au moyen de la Remarque II.12.5. Par conséquent, tout sous-groupe d'un groupe résoluble est résoluble.
2. Pour un homomorphisme $\varphi : G \to G'$, on a l'égalité $\varphi(G)^{(k)} = \varphi(G^{(k)})$ pour tout $k \geq 0$: la preuve se fait par récurrence sur $k \geq 0$ en se basant sur la Remarque II.12.6. Par conséquent, l'image d'un groupe résoluble par un homomorphisme est résoluble.

Exemples II.18 (groupes résolubles)**.**

1. Un groupe G est trivial si et seulement si $G^{(0)} = \{e\}$. Ainsi, un groupe trivial (par exemple, le groupe S_1) est résoluble.
2. Un groupe G est abélien si et seulement si $G^{(1)} = \{e\}$. Ainsi, un groupe abélien (par exemple, le groupe S_2) est résoluble.
3. Qu'en est-il de S_3 ? Par l'Exemple II.14.2 ci-dessus, on a $S_3^{(1)} = [S_3, S_3] = A_3$ qui est abélien. Ainsi, on a $S_3^{(2)} = [A_3, A_3] = \{e\}$, et S_3 est aussi résoluble.
4. Qu'en est-il de S_4 ? Comme ci-dessus, on a $S_4^{(1)} = [S_4, S_4] = A_4$, et l'on va voir en exercice que $S_4^{(2)} = [A_4, A_4]$ est isomorphe au groupe de Klein V, qui est abélien. Ainsi, on a $S_4^{(3)} = [V, V] = \{e\}$, et S_4 est aussi résoluble.

Cette liste d'exemples laisse à penser que S_n est résoluble pour tout n, avec $S_n^{(n-1)} = \{e\}$. Il n'en est rien.

Théorème II.19

Le groupe symétrique S_n est résoluble si et seulement si $n \leq 4$.

Démonstration. Par les exemples ci-dessus, tout groupe S_n avec $n \geq 4$ est résoluble. Il reste donc à voir que S_n n'est pas résoluble pour $n \geq 5$. Comme on connaît l'égalité $[S_n, S_n] = A_n$, il nous faut calculer le groupe dérivé $[A_n, A_n] \subset A_n$. Nous allons montrer que pour tout $n \geq 5$, on a l'égalité $[A_n, A_n] = A_n$. Cela implique le théorème, puisque qu'on a alors $S_n^{(k)} = A_n \neq \{e\}$ pour tout $k \geq 1$.

Pour vérifier cette affirmation, il faut donc montrer que tout élément de A_n est produit de commutateurs d'éléments de A_n. Comme A_n est engendré par les 3-cycles, il suffit de vérifier que tous les 3-cycles sont des commutateurs d'éléments de A_n. Soit donc (i, j, k) un 3-cycle quelconque dans A_n. Comme on suppose $n \geq 5$, il existe $\ell, m \in \{1, \ldots, n\}$ tels que i, j, k, ℓ, m sont tous distincts. On calcule alors :

$$\begin{aligned}[(i,\ell,k),(k,j,m)] &= (i,\ell,k)(k,j,m)(i,\ell,k)^{-1}(k,j,m)^{-1} \\ &= (i,j,m)(m,j,k) = (i,j,k)\,.\end{aligned}$$

On a donc bien $(i, j, k) \in [A_n, A_n]$, ce qui conclut la preuve. □

Remarques II.20.

1. Notons que le Théorème II.19 ci-dessus, plus précisément le fait que S_n n'est pas résoluble pour $n \geq 5$, peut aussi s'obtenir comme une conséquence directe du Théorème II.8.

   ⌜ En effet, supposons $n \geq 5$ et considérons le sous-groupe $N := [A_n, A_n]$ de A_n, qui est normal par la Remarque II.12.7. Comme A_n est simple, on a soit $N = \{e\}$, soit $N = A_n$. Le premier cas signifie que A_n est abélien, ce qui est faux pour $n \geq 4$ (et a fortiori pour $n \geq 5$). On a donc bien $[A_n, A_n] = A_n$, ce qui implique que S_n n'est pas résoluble comme on l'a vu ci-dessus. ⌟

Walter Feit (1930-2004)

2. Cette discussion n'est pas sans rappeler l'introduction du cours, et ce n'est pas un hasard. En effet, comme on le verra au Chapitre IV, le théorème ci-dessus est la raison algébrique fondamentale pour laquelle l'équation polynomiale générale de degré n est résoluble par radicaux si et seulement si $n \leq 4$.
3. Il est possible de montrer que tout groupe d'ordre impair est résoluble : c'est le fameux théorème de Feit-Thompson, qui date de 1962. Mais la preuve originale fait 255 pages !

John Thompson (1932-)

Nous terminons cette sous-section avec le résultat promis sur les diverses définitions équivalentes des groupes résolubles, et deux conséquences, qui nous seront utiles en théorie de Galois.

Proposition II.21. *Pour G un groupe quelconque, sont équivalents :*

(i) G est résoluble.

(ii) Il existe une suite $\{e\} = H_n \lhd H_{n-1} \lhd \cdots \lhd H_1 \lhd H_0 = G$ avec H_{k-1}/H_k abélien pour tout $k = 1, \ldots, n$.

Démonstration. Supposons dans un premier temps que G est un groupe résoluble, et considérons la suite dérivée $H_k := G^{(k)}$. On a bien $H_0 = G^{(0)} = G$, de même que

$$H_k = G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \lhd G^{(k-1)} = H_{k-1}$$

par la Remarque II.12.7, avec quotient $H_{k-1}/H_k = G^{(k-1)}/[G^{(k-1)}, G^{(k-1)}]$ abélien par la Remarque II.12.8 et $H_n = G^{(n)} = \{e\}$ pour un certain $n \geq 0$ puisque G est résoluble. Cela montre l'implication du second point par le premier.

Supposons réciproquement qu'il existe $\{e\} = H_n \lhd H_{n-1} \lhd \cdots \lhd H_1 \lhd H_0 = G$ avec H_{k-1}/H_k abélien pour tout $k \geq 1$. On va montrer l'inclusion $G^{(k)} \subset H_k$ pour $k \geq 0$, ce qui implique $G^{(n)} = \{e\}$ et donc que G est résoluble. Cette vérification se fait par induction sur $k \geq 0$. Le départ de cette induction étant triviale puisque $G^{(0)} = H_0 = G$, supposons l'inclusion $G^{(k-1)} \subset H_{k-1}$ valide pour un $k \geq 1$ fixé. On a alors

$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \subset [H_{k-1}, H_{k-1}] \subset H_k \,,$$

où l'inclusion du milieu est une conséquence de l'hypothèse de récurrence et de la Remarque II.12.5, tandis que l'inclusion de droite découle de la Remarque II.12.9 et du fait que H_{k-1}/H_k est abélien. Cela conclut la preuve. □

Proposition II.22. *Pour tout sous-groupe normal N d'un groupe G quelconque, le groupe G est résoluble si et seulement si N et G/N le sont.*

Démonstration. Soient N un sous-groupe normal d'un groupe G, et $\pi : G \to G/N$ la projection canonique. Si G est résoluble, alors par la Remarque II.17.1, le sous-groupe N est résoluble, de même que $G/N = \pi(G)$ par la Remarque II.17.2.

Supposons réciproquement que $N \lhd G$ est résoluble, ainsi que le quotient G/N. Par la Proposition II.21 appliquée à N, il existe une suite

$$\{e\} = N_m \lhd N_{m-1} \lhd \cdots \lhd N_1 \lhd N_0 = N \tag{II.1}$$

avec N_{k-1}/N_k abélien pour tout $k = 1, \ldots, m$. Par cette même Proposition II.21 appliquée à G/N, et par le Théorème II.5 sur les sous-groupes normaux des groupes quotients, il existe une suite $\{e\} = H_n/N \lhd \cdots \lhd H_1/N \lhd H_0/N = G/N$ avec $(H_{k-1}/N)/(H_k/N)$ abélien pour tout $k = 1, \ldots, n$. Par le Théorème II.5, cela définit une suite

$$N = H_n \lhd H_{n-1} \lhd \cdots \lhd H_1 \lhd H_0 = G \,, \tag{II.2}$$

avec les quotients successifs $H_{k-1}/H_k \simeq (H_{k-1}/N)/(H_k/N)$ abéliens par hypothèse. En mettant bout à bout les suites de (II.1) et (II.2) et en utilisant une dernière fois la Proposition II.21, on obtient que G est résoluble. □

Voici le dernier résultat de cette sous-section, sur les groupes résolubles *finis*. La preuve est inclue par souci de complétude, mais ne sera pas discutée en détail en cours et ne fait pas partie du champ des examens.

Lemme II.23. *Si G est fini, alors G est résoluble si et seulement s'il existe une suite $\{e\} = G_m \triangleleft G_{m-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$ avec G_{k-1}/G_k cyclique d'ordre premier pour tout $k = 1, \ldots, m$.*

Démonstration. Supposons dans un premier temps que G admette une suite comme dans l'énoncé. Les quotients successifs étant abéliens, la Proposition II.21 implique que G est résoluble.

Supposons à présent que G est fini et résoluble. Par la Proposition II.21, il existe une suite $\{e\} = H_n \triangleleft H_{n-1} \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = G$ avec H_{k-1}/H_k fini et abélien pour tout $k = 1, \ldots, n$. Si chacun de ces quotients est d'ordre premier (et donc cyclique), alors on a terminé. Dans le cas contraire, fixons un indice k tel que H_{k-1}/H_k n'est *pas* d'ordre premier, et un élément $a \in H_{k-1}/H_k$ d'ordre $o(a)$ satisfaisant $1 < o(a) < \#(H_{k-1}/H_k)$. Notons qu'un tel élément existe (car le groupe n'est pas d'ordre premier), par exemple par le *théorème de Cauchy* dont vous verrez (à nouveau) la preuve en Sous-section II.6.2. Notons $H := \pi^{-1}(\langle a \rangle) \triangleleft H_{k-1}$ l'image réciproque par la projection $\pi : H_{k-1} \to H_{k-1}/H_k$ du sous-groupe $\langle a \rangle \triangleleft H_{k-1}/H_k$ engendré par a. Cela définit une suite allongée

$$\{e\} = H_n \triangleleft H_{n-1} \triangleleft \cdots \triangleleft H_k \triangleleft H \triangleleft H_{k-1} \triangleleft \cdots \triangleleft H_1 \triangleleft H_0 = G\,,$$

avec H/H_k abélien car sous-groupe de H_{k-1}/H_k abélien, et H_{k-1}/H abélien car isomorphe par le Théorème II.5 à $(H_{k-1}/H_k)/(H/H_k)$ qui est un quotient de groupe abélien. En conclusion, cette suite allongée a elle aussi tous ses quotients successifs abéliens. Mais l'hypothèse sur l'ordre de a est équivalente à $\{e\} \subsetneq \langle a \rangle \subsetneq H_{k-1}/H_k$, et donc à $H_k \subsetneq H \subsetneq H_{k-1}$. Cela signifie que l'isomorphisme $(H_{k-1}/H_k)/(H/H_k) \simeq H_{k-1}/H$ induit une factorisation non-triviale

$$\#(H_{k-1}/H_k) = \#(H_{k-1}/H) \cdot \#(H/H_k)$$

de l'ordre (non-premier) de H_{k-1}/H_k. Comme G est fini, un nombre fini de tels allongements de suites résulte en une suite $\{e\} = G_m \triangleleft G_{m-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$ avec G_{k-1}/G_k d'ordre premier (et donc cyclique) pour tout $k = 1, \ldots, m$. □

II.2.3 Abélianisation

Les commutateurs donnent une définition possible des groupes résolubles, mais ils permettent également de répondre à la question suivante :

Comment transformer un groupe G en un groupe abélien "de la façon la plus efficace possible" ?

Ce sujet ne sera pas discuté en détail au cours. Pour cette raison, il ne fait pas partie du champ des examens et figure dans ce polycopié "pour votre culture".

Bien entendu, cette question n'est pas encore posée de manière formelle. Cette formalisation se fait à l'aide d'une nouvelle propriété universelle, de la façon suivante. Pour G un groupe fixé, considérons la catégorie $\mathscr{A}^G$ définie via :

- $\mathrm{Ob}(\mathscr{A}^G) = \{\varphi \in \mathrm{Hom}_{\mathsf{Grp}}(G, A) \mid A \text{ groupe abélien}\}$;

- les morphismes de $\mathscr{A}^G$ entre $\begin{array}{c} G \\ \downarrow{\scriptstyle \varphi_1} \\ A_1 \end{array}$ et $\begin{array}{c} G \\ \downarrow{\scriptstyle \varphi_2} \\ A_2 \end{array}$ sont les diagrammes commutatifs de la forme $\begin{array}{ccc} & G & \\ {\scriptstyle \varphi_1}\swarrow & & \searrow{\scriptstyle \varphi_2} \\ A_1 & \xrightarrow{\sigma} & A_2 \end{array}$ avec $\sigma \in \mathrm{Hom}_{\mathsf{Grp}}(A_1, A_2)$.
- La composition est définie comme dans la catégorie $\mathscr{C}^A$ (Exemple I.3.9).

Les objets de $\mathscr{A}^G$ sont à comprendre comme des "transformations" du groupe G fixé en un groupe abélien. Ce que l'on recherche, c'est une transformation $G \to A$ telle que toute transformation de G en un groupe abélien puisse être obtenue à partir de celle-ci. En d'autres termes, la question (vague) ci-dessus se formalise en la question (précise) suivante :

Pour un groupe G fixé, comment construire un objet initial dans $\mathscr{A}^G$?

Voici la réponse à cette question.

Définition II.24

Le quotient $G_{\mathrm{ab}} := G/[G,G]$ est appelé l'**abélianisé** de G.

Intuitivement, la raison est claire : en quotientant par le groupe dérivé, on "trivialise" tous les commutateurs, ce qui est exactement ce qu'il faut pour qu'un groupe devienne abélien. Plus formellement, la proposition suivante montre que la projection $G \to G_{\mathrm{ab}}$ est un objet initial dans $\mathscr{A}^G$.

Proposition II.25. *Le groupe $G_{\mathrm{ab}} = G/[G,G]$ est abélien, et la projection canonique $\pi\colon G \to G_{\mathrm{ab}}$ satisfait la propriété universelle*[3] *suivante : pour tout homomorphisme $\varphi\colon G \to A$ avec A abélien, il existe un unique homomorphisme $\overline{\varphi}\colon G_{\mathrm{ab}} \to A$ tel que $\overline{\varphi} \circ \pi = \varphi$.*

$$\begin{array}{ccc} G & \xrightarrow{\forall \varphi} & A\,. \\ {\scriptstyle \pi}\downarrow & \nearrow{\scriptstyle \exists ! \overline{\varphi}} & \\ G_{\mathrm{ab}} & & \end{array}$$

Démonstration. Soit donc G un groupe quelconque. Comme $[G,G] \triangleleft G$ par la Remarque II.12.7, on peut considérer le quotient $G_{\mathrm{ab}} := G/[G,G]$, qui est abélien par la Remarque II.12.8. Soit à présent $\varphi\colon G \to A$ un homomorphisme avec A abélien. Par les Remarques II.12.2 et II.12.1, on a $\varphi([g,h]) = [\varphi(g), \varphi(h)] = e$, d'où $[g,h] \in \mathrm{Ker}(\varphi)$ pour tout $g, h \in G$, ce qui implique l'inclusion de $[G,G]$ dans $\mathrm{Ker}(\varphi)$. Par la propriété universelle du quotient de G par $[G,G]$, il existe un unique homomorphisme $\overline{\varphi}\colon G_{\mathrm{ab}} \to A$ tel que $\overline{\varphi} \circ \pi = \varphi$. □

Exemples II.26 (abélianisés)**.**

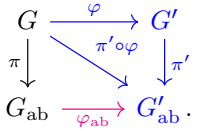
1. Si G est abélien, alors $[G,G] = \{e\}$, d'où $G_{\mathrm{ab}} \simeq G$ comme il se doit. Réciproquement, si $G_{\mathrm{ab}} \simeq G$, alors G est abélien puisque G_{ab} l'est. Ainsi, un groupe est abélien si et seulement s'il est isomorphe à son abélianisé.

3. Bien entendu, on parle de la *propriété universelle de l'abélianisé.*

2. Comme $[S_n, S_n] = A_n$, on a $(S_n)_{\mathrm{ab}} = S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$ pour $n \geq 2$.
3. Considérons les groupes alternés A_n. Pour $n \leq 3$, le groupe A_n est abélien, et donc isomorphe à son abélianisé. Pour $n = 4$, on vérifie en exercice que $[A_4, A_4] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; par Lagrange, $(A_4)_{\mathrm{ab}}$ est d'ordre $\frac{12}{4} = 3$, et donc cyclique d'ordre 3. Finalement, pour $n \geq 5$, on a vu dans la preuve du Théorème II.19 l'égalité $[A_n, A_n] = A_n$, qui implique que l'abélianisé de A_n est trivial. En résumé, le groupe $(A_n)_{\mathrm{ab}}$ est (cyclique) d'ordre 3 pour $n = 3, 4$, et trivial sinon.
4. Rappelons que pour tout corps K et tout entier $n \geq 3$, le groupe dérivé de $\mathrm{GL}(n, K)$ est $\mathrm{SL}(n, K)$ (Exemple II.14.3). Cela implique donc
$$\mathrm{GL}(n, K)_{\mathrm{ab}} = \mathrm{GL}(n, K)/\mathrm{SL}(n, K) \simeq K^*$$
via l'isomophisme induit par l'homomorphisme surjectif $\det\colon \mathrm{GL}(n, K) \to K^*$.

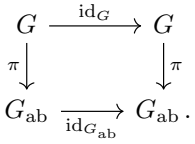
Proposition II.27. *L'abélianisation définit un foncteur* $\mathscr{F}\colon \mathsf{Grp} \to \mathsf{Ab}$.

Démonstration. À tout objet G de la catégorie Grp des groupes, on a bien associé un objet $\mathscr{F}(G) := G_{\mathrm{ab}}$ de la catégorie Ab des groupes abéliens. Étant donnés deux groupes G, G' et un morphisme $\varphi \in \mathrm{Hom}_{\mathsf{Grp}}(G, G')$, il s'agit maintenant de construire $\mathscr{F}(\varphi) =: \varphi_{\mathrm{ab}} \in \mathrm{Hom}_{\mathsf{Ab}}(G_{\mathrm{ab}}, G'_{\mathrm{ab}})$. Cela se fait à l'aide de la propriété universelle de l'abélianisé (Proposition II.25) : comme G'_{ab} est abélien, l'homomorphisme $\pi' \circ \varphi\colon G \to G'_{\mathrm{ab}}$ induit un unique homomorphisme $\varphi_{\mathrm{ab}}\colon G_{\mathrm{ab}} \to G'_{\mathrm{ab}}$ tel que $\varphi_{\mathrm{ab}} \circ \pi = \pi' \circ \varphi$:



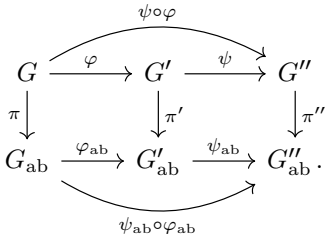
Les axiomes de fonctorialité (Définition I.22) se vérifient via l'unicité de la définition de $\mathscr{F}(\varphi) = \varphi_{\mathrm{ab}}$, comme suit.

(i) Pour tout groupe G, le morphisme $\mathrm{id}_{G_{\mathrm{ab}}}$ satisfait $\mathrm{id}_{G_{\mathrm{ab}}} \circ \pi = \pi = \pi \circ \mathrm{id}_G$:



Par unicité dans la définition de $\mathscr{F}(\mathrm{id}_G)$, on a donc bien
$$\mathscr{F}(1_G) = (\mathrm{id}_G)_{\mathrm{ab}} = \mathrm{id}_{G_{\mathrm{ab}}} = 1_{\mathscr{F}(G)}\,.$$

(ii) Pour tous groupes G, G', G'' et tous morphismes $\varphi \in \mathrm{Hom}_{\mathsf{Grp}}(G, G')$ et $\psi \in \mathrm{Hom}_{\mathsf{Grp}}(G', G'')$, les définitions de φ_{ab} et de ψ_{ab} impliquent
$$\begin{aligned}(\psi_{\mathrm{ab}} \circ \varphi_{\mathrm{ab}}) \circ \pi &= \psi_{\mathrm{ab}} \circ (\varphi_{\mathrm{ab}} \circ \pi) = \psi_{\mathrm{ab}} \circ (\pi' \circ \varphi) \\ &= (\psi_{\mathrm{ab}} \circ \pi') \circ \varphi = (\pi'' \circ \psi) \circ \varphi = \pi'' \circ (\psi \circ \varphi)\,,\end{aligned}$$
comme illustré dans le diagramme ci-dessous :



Par unicité dans la définition de $(\varphi \circ \psi)_{\mathrm{ab}}$, on a donc bien

$$\mathscr{F}(\psi\varphi) = (\psi \circ \varphi)_{\mathrm{ab}} = \psi_{\mathrm{ab}} \circ \varphi_{\mathrm{ab}} = \mathscr{F}(\psi)\mathscr{F}(\varphi)\,.$$

Cela conclut la preuve de la proposition. □

Comme un foncteur envoie les isomorphismes sur des isomorphismes (Remarque I.23.3), on a le corollaire suivant.

Corollaire II.28. *Si G et G' sont des groupes isomorphes, alors leurs abélanisés G_{ab} et G'_{ab} sont des groupes abéliens isomorphes.* □

II.3 Groupes libres, présentation par générateurs et relations

Le premier but de cette section est de construire ce qu'on appelle le *groupe libre* sur un ensemble donné. Ce groupe se caractérise par une propriété universelle, qu'on verra en Sous-section II.3.1, et admet une construction explicite expliquée en Sous-section II.3.2. On montrera ensuite, en Sous-section II.3.3, comment caractériser et construire les objets analogues dans la catégorie Ab, ce qu'on appelle les *groupes abéliens libres*. Ces constructions induisent une façon extrêmement commode de caractériser un groupe quelconque à isomorphisme près : les *présentations par générateurs et relations*, qu'on verra en Sous-section II.3.4. À leur tour, ces présentations fournissent une construction explicite du coproduit dans la catégorie des groupes, appelé *produit libre*, et qui sera traité en Sous-section II.3.5.

II.3.1 Propriété universelle du groupe libre

Les groupes libres donnent une réponse à la question suivante, que l'on pose d'abord de manière informelle :

Étant donné un ensemble X, comment construire un groupe contenant X "de la façon la plus efficace possible" ?

La formalisation de cette question se fait à l'aide d'une propriété universelle. Pour X un ensemble fixé, considérons la catégorie $\mathscr{C}^X$ définie via :

- $\mathrm{Ob}(\mathscr{C}^X) = \{j \in \mathrm{Hom}_{\mathsf{Set}}(X, G) \mid G \text{ groupe}\}$;
- les morphismes de $\mathscr{C}^X$ entre $\begin{array}{c} X \\ \downarrow{\scriptstyle j_1} \\ G_1 \end{array}$ et $\begin{array}{c} X \\ \downarrow{\scriptstyle j_2} \\ G_2 \end{array}$ sont les les diagrammes commutatifs

de la forme $\begin{array}{ccc} & X & \\ {\scriptstyle j_1}\swarrow & & \searrow{\scriptstyle j_2} \\ G_1 & \xrightarrow{\sigma} & G_2 \end{array}$ avec $\sigma \in \mathrm{Hom}_{\mathsf{Grp}}(G_1, G_2)$.

Il faut interpréter les objets de $\mathscr{C}^X$ comme des "groupes contenant X", ou des "plongements" de l'ensemble X fixé dans un groupe. Ce que l'on recherche, c'est

un plongement $X \to G$ telle que tout plongement de X dans un groupe puisse être obtenue à partir de celui-ci. En d'autres termes, la formalisation de la question ci-dessus est la suivante :

Pour un ensemble X fixé, comment construire un objet initial dans $\mathscr{C}^X$?

Un tel objet est ce qu'on appelle un *groupe libre* sur X. Voici cette définition écrite en toutes lettres, via la *propriété universelle du groupe libre* sur X.

Définition II.29

Soit X un ensemble. Un **groupe libre** sur X est la donnée d'un groupe $F(X)$ et d'une application $j : X \to F(X)$ qui satisfait la propriété universelle suivante : pour toute application $f : X \to G$ avec G un groupe, il existe un unique homomorphisme $\varphi : F(X) \to G$ tel que $\varphi \circ j = f$.

$$\begin{array}{ccc} X & \xrightarrow{\forall f} & G\,. \\ {\scriptstyle j}\downarrow & \nearrow_{\exists ! \varphi} & \\ F(X) & & \end{array} \tag{II.3}$$

Remarques II.30.

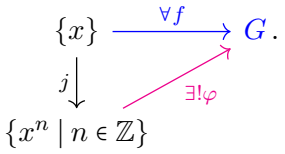
1. Par la Remarque I.11.3, si un groupe libre sur X existe, alors il est unique à unique isomorphisme près dans $\mathscr{C}^X$. En particulier, deux groupes libres sur un même ensemble X sont isomorphes, et l'on parlera donc souvent *du* groupe libre (plutôt que *d'un* groupe libre) sur X.
2. Cette propriété universelle dit que la donnée d'une application $X \to G$ est équivalente à la donnée d'un homomorphisme de groupes $F(X) \to G$. En particulier, un homomorphisme de groupe $F(X) \to G$ est entièrement déterminé par son image sur $j(X)$. On peut donc penser à X comme l'analogue d'une base pour le groupe $F(X)$.

Exemples II.31 (groupes libres)**.**

1. Considérons l'ensemble vide $X = \varnothing$. Le groupe trivial $\{e\}$ (muni de l'unique application $j : \varnothing \to \{e\}$) satisfait la propriété universelle du groupe libre sur $X = \varnothing$: en effet, pour tout groupe G (muni de l'unique application $f : \varnothing \to G$), il existe un unique homomorphisme $\varphi : \{e\} \to G$ (tel que $\varphi \circ j = f$). Ainsi, le groupe libre sur l'ensemble vide est le groupe trivial : $F(\varnothing) = \{e\}$.
2. Soit à présent $X = \{x\}$ un singleton. Considérons le groupe infini cyclique $\mathbb{Z}$, qu'on va noter multiplicativement [4] avec générateur x. En d'autres termes, soit
$$F(\{x\}) := \{x^n \mid n \in \mathbb{Z}\} \simeq \mathbb{Z}\,,$$
muni de l'application $j : \{x\} \to F(\{x\})$ donnée par $j(x) = x$. Il satisfait bien la propriété universelle du groupe libre sur $X = \{x\}$: pour tout groupe G et

4. Bien-sûr, il n'est pas absolument nécessaire d'adopter la notation multiplicative, mais cela permet de mieux faire le lien avec la construction générale qui suivra sous peu.

toute application $f\colon\{x\} \to G$ (i.e. pour tout élément $f(x)$ d'un groupe G), il existe un unique homomorphisme $\varphi\colon\{x^n \mid n \in \mathbb{Z}\} \to G$ tel que $\varphi \circ j = f$ (i.e. tel que $\varphi(x) = f(x)$), celui défini par $\varphi(x^n) = f(x)^n$:



Ainsi, le groupe libre sur un singleton est infini cyclique : $F(\{x\}) \simeq \mathbb{Z}$.

Une construction explicite du groupe libre sur X quelconque sera donnée en Sous-section II.3.2. Pour l'instant, nous allons nous contenter d'en étudier quelques propriétés générales.

Proposition II.32. *Si $j\colon X \to F(X)$ est un groupe libre sur X, alors :*

(i) j est injective[5] *;*

(ii) $F(X)$ est engendré par $j(X)$.

De plus, cette construction définit un foncteur $\mathscr{F}\colon \mathsf{Set} \to \mathsf{Grp}$.

Démonstration. Une application $j\colon X \to F(X)$ est toujours injective si $\#X \leq 1$; supposons donc $\#X \geq 2$, et soient $x_1 \neq x_2$ deux éléments distincts de X. Posons $f\colon X \to \mathbb{Z}$ définie par $f(x) = 1$ si $x = x_1$ et $f(x) = 0$ sinon. Par la propriété universelle du groupe libre sur X, il existe un (unique) homomorphisme $\varphi\colon F(X) \to \mathbb{Z}$ tel que $\varphi \circ j = f$. On a donc

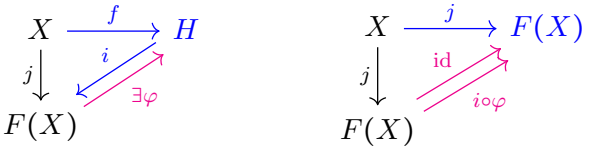
$$\varphi(j(x_1)) = f(x_1) = 1 \neq 0 = f(x_2) = \varphi(j(x_2))\,,$$

d'où $j(x_1) \neq j(x_2)$. Cela montre que j est injective.

Pour le second point, considérons le sous-groupe $H := \langle j(X)\rangle$ de $F(X)$ engendré par $j(X) \subset F(X)$. Soient $f\colon X \to H$ l'application donnée par $f(x) = j(x)$ pour $x \in X$, et $i\colon H \to F(X)$ l'inclusion ; notons qu'on a $i \circ f = j$ par construction. Par la propriété universelle, il existe un homomorphisme $\varphi\colon F(X) \to H$ tel que $\varphi \circ j = f$ (voir diagramme de gauche dans (II.4) ci-dessous). Ainsi, l'endomorphisme $i \circ \varphi\colon F(X) \to F(X)$ satisfait

$$(i \circ \varphi) \circ j = i \circ (\varphi \circ j) = i \circ f = j = \mathrm{id}_{F(X)} \circ j\,.$$

Par l'unicité dans la propriété universelle (voir diagramme de droite en (II.4)), on a donc $i \circ \varphi = \mathrm{id}_{F(X)}$. Cela implique que i est surjective, d'où $H = F(X)$, ce qui montre le second point.



(II.4)

5. On "plonge" donc bien X dans un groupe, comme formulé en début de section.

À tout objet X de la catégorie Set des ensembles, la Définition II.29 associe un objet $\mathscr{F}(X) := F(X)$ de la catégorie Grp des groupes (qu'il reste à construire, voir Sous-section II.3.2). Étant donnés deux ensembles X, Y et une application $f \in \mathrm{Hom}_{\mathsf{Set}}(X,Y)$, on considère $\mathscr{F}(f)$ dans $\mathrm{Hom}_{\mathsf{Grp}}(F(X),F(Y))$ défini via la propriété universelle comme l'unique homomorphisme $\mathscr{F}(f)\colon F(X) \to F(Y)$ tel que $\mathscr{F}(f) \circ j_X = j_Y \circ f$:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle j_X}\downarrow & \searrow^{j_Y \circ f} & \downarrow{\scriptstyle j_Y} \\ F(X) & \xrightarrow[\mathscr{F}(f)]{} & F(Y)\,. \end{array}$$

Les axiomes de fonctorialité (Définition I.22) se vérifient via l'unicité de la définition de $\mathscr{F}(f)$, comme suit.

(i) Pour tout ensemble X, l'homomorphisme de groupes $\mathrm{id}_{F(X)}\colon F(X) \to F(X)$ satisfait $\mathrm{id}_{F(X)} \circ j_X = j_X = j_X \circ \mathrm{id}_X$:

$$\begin{array}{ccc} X & \xrightarrow{\mathrm{id}_X} & X \\ {\scriptstyle j_X}\downarrow & & \downarrow{\scriptstyle j_X} \\ F(X) & \xrightarrow[\mathrm{id}_{F(X)}]{} & F(X)\,. \end{array}$$

Par unicité dans la définition de $\mathscr{F}(\mathrm{id}_X)$, on a donc bien

$$\mathscr{F}(1_X) = \mathscr{F}(\mathrm{id}_X) = \mathrm{id}_{F(X)} = 1_{\mathscr{F}(X)}\,.$$

(ii) Pour tous ensembles X, Y, Z et toutes applications $f \in \mathrm{Hom}_{\mathsf{Set}}(X,Y)$ et $g \in \mathrm{Hom}_{\mathsf{Set}}(Y,Z)$, les définitions de $\mathscr{F}(f)$ et de $\mathscr{F}(g)$ impliquent

$$\begin{aligned}(\mathscr{F}(g) \circ \mathscr{F}(f)) \circ j_X &= \mathscr{F}(g) \circ (\mathscr{F}(f) \circ j_X) = \mathscr{F}(g) \circ (j_Y \circ f) \\ &= (\mathscr{F}(g) \circ j_Y) \circ f = (j_Z \circ g) \circ f = j_Z \circ (g \circ f)\,,\end{aligned}$$

comme illustré dans le diagramme ci-dessous :

$$\begin{array}{ccccc} & & {\scriptstyle g\circ f}\frown & & \\ X & \xrightarrow{f} & Y & \xrightarrow{g} & Z \\ {\scriptstyle j_X}\downarrow & & \downarrow{\scriptstyle j_Y} & & \downarrow{\scriptstyle j_Z} \\ F(X) & \xrightarrow{\mathscr{F}(f)} & F(Y) & \xrightarrow{\mathscr{F}(g)} & F(Z)\,. \\ & & {\scriptstyle \mathscr{F}(g)\circ\mathscr{F}(f)}\smile & & \end{array}$$

Par unicité dans la définition de $\mathscr{F}(g \circ f)$, on a donc bien

$$\mathscr{F}(g \circ f) = \mathscr{F}(g) \circ \mathscr{F}(f)\,.$$

Cela conclut la preuve de la proposition. □

Par la Remarque I.23.3, on a immédiatement le corollaire suivant.

Corollaire II.33. *Si deux ensembles X et Y sont en bijection, alors les groupes libres $F(X)$ et $F(Y)$ sont isomorphes.* □

II.3.2 Construction du groupe libre

C'est bien joli, mais à l'exception des ensembles X avec au plus un élément, on ne sait toujours pas si le groupe libre $F(X)$ existe ! Le but de cette sous-section est de donner, pour un ensemble X quelconque, une construction explicite de $j\colon X \to F(X)$ satisfaisant la propriété universelle (Définition II.29).

Soit donc X un ensemble quelconque. La construction se fait par étapes.

- Soit X' un ensemble disjoint de X muni d'une bijection $X \to X'$ notée $x \mapsto x^{-1}$.
- Considérons les éléments de $X \sqcup X'$ comme des *lettres*, et $X \sqcup X'$ comme un *alphabet*. Un *mot* sur X est une suite finie $w = (x_1, x_2, \dots, x_n)$ avec $n \geq 0$, où chaque lettre x_i est soit de la forme $x \in X$, soit de la forme $x^{-1} \in X'$. Un tel mot sera simplement noté $w = x_1 x_2 \cdots x_n$.
- Soit $W(X)$ l'ensemble des mots sur X, qui contient en particulier le mot vide, noté $w = (\,)$. Voici quelques exemples :
  - Pour $X = \varnothing$, l'ensemble $W(X)$ ne contient qu'un seul mot, le mot vide.
  - Pour $X = \{x\}$ un singleton, l'ensemble $W(X)$ contient tous les mots en les lettres $\{x, x^{-1}\}$, comme x, xx^{-1}, $x^{-1}x^{-1}xxxx^{-1}x$, $xx^{-1}x^{-1}x$, etc.
  - L'ensemble $W(\{x, y\})$ contient des mots tels que $xy^{-1}x^{-1}x^{-1}x^{-1}xyy^{-1}$.

  Notons que l'ensemble $W(X)$ muni de la juxtaposition des mots $(w, w') \mapsto ww'$ satisfait les axiomes d'un monoïde, mais pas l'existence d'un inverse. Voici comment y remédier.
- Soit $R\colon W(X) \to W(X)$ l'application de *réduction* définie comme suit :
  - étant donné un mot $w \in W(X)$, on cherche la première apparition (de gauche à droite) dans w de deux lettres consécutives de la forme xx^{-1} ou $x^{-1}x$;
  - on efface ces deux lettres, et on recommence.

  Comme le mot w est fini, après un nombre fini de telles opérations, on obtient un mot $R(w)$ qui est *réduit* : il ne contient plus de telles paires de lettres adjacentes. Voici un exemple d'une telle réduction :

$$w = x\underline{y^{-1}y}xyxx^{-1}y \longmapsto xxxy\underline{xx^{-1}}y \longmapsto xxxyy = R(w)\,.$$

- Notons $F(X) \subset W(X)$ l'image de $R\colon W(X) \to W(X)$, donc l'ensemble des mots réduits sur X.
- On munit l'ensemble $F(X)$ de la loi de composition donnée par juxtaposition-et-réduction : pour w, w' deux mots réduits, on pose donc $w \cdot w' := R(ww')$. Par exemple, on a

$$xxy \cdot y^{-1}x^{-1}xy = R(xxyy^{-1}x^{-1}xy) = xxy\,.$$

- Finalement, soit $j\colon X \to F(X)$ l'application qui associe à $x \in X$ le mot réduit à une lettre $j(x) = x \in F(X)$.

La proposition suivante nous garantit que cette construction donne bien le groupe libre sur X.

Proposition II.34. *$F(X)$ est un groupe, et $j\colon X \to F(X)$ satisfait la propriété universelle du groupe libre sur X.*

Démonstration. Dans un premier temps, il s'agit de vérifier que $F(X)$ est bien un groupe pour la loi de composition $w \cdot w' := R(ww')$. Cette loi de composition est associative[6], car la réduction $R(w)$ d'un mot w ne dépend pas de l'ordre dans lequel on efface les paires de lettres xx^{-1} et $x^{-1}x$. Le mot vide $e := (\ )$ est clairement l'élément neutre, puisque $e \cdot w = w \cdot e = w$ pour tout $w \in F(X)$. Finalement, tout mot $w \in F(X)$ admet l'inverse w^{-1} obtenu en renversant l'ordre des lettres et en remplaçant $x \in X$ par $x^{-1} \in X'$ et vice-versa.

Maintenant que nous savons que $F(X)$ est bien un groupe, montrons que $j\colon X \to F(X)$ satisfait la propriété universelle du groupe libre sur X donnée en (II.3). Soit donc $f\colon X \to G$ une application quelconque dans un groupe G. Par définition de l'ensemble $W(X)$ des mots sur X, l'application f s'étend en une unique application $\widetilde{f}\colon W(X) \to G$ telle que

(i) $\widetilde{f}(x) = f(x)$ pour $x \in X$ et $\widetilde{f}(x^{-1}) = f(x)^{-1}$ pour $x^{-1} \in X'$;

(ii) $\widetilde{f}(ww') = \widetilde{f}(w)\widetilde{f}(w')$ pour tous $w, w' \in W(X)$.

Notons que cette application $\widetilde{f}$ satisfait

$$\widetilde{f}(xx^{-1}) \overset{\text{(ii)}}{=} \widetilde{f}(x)\widetilde{f}(x^{-1}) \overset{\text{(i)}}{=} f(x)f(x)^{-1} = e_G$$

pour tout $x \in X$, et similairement $\widetilde{f}(xx^{-1}) = e_G$, ce qui implique $\widetilde{f}(R(w)) = \widetilde{f}(w)$ pour tout $w \in W(X)$. Ainsi, si l'on définit $\varphi\colon F(X) \to G$ comme la restriction de $\widetilde{f}$ aux mots réduits, on a

$$\varphi(w \cdot w') = \widetilde{f}(w \cdot w') = \widetilde{f}(R(ww')) = \widetilde{f}(ww') \overset{\text{(ii)}}{=} \widetilde{f}(w)\widetilde{f}(w') = \varphi(w)\varphi(w')$$

pour tous $w, w' \in F(X)$, et φ est donc bien un homomorphisme. Pour tout $x \in X$, il satisfait

$$(\varphi \circ j)(x) = \varphi(j(x)) = \varphi(x) = \widetilde{f}(x) \overset{\text{(i)}}{=} f(x)\,.$$

Finalement, comme $F(X)$ est engendré par $j(X)$, l'homomorphisme φ est uniquement déterminé par l'égalité $\varphi \circ j = f$. □

Voici quelques exemples explicites, à comparer avec les Exemples II.31 ci-dessus.

Exemples II.35 (groupes libres)**.**

1. Pour $X = \varnothing$, on a $F(\varnothing) = W(\varnothing) = \{e\}$, le groupe trivial formé du mot vide.
2. Pour $X = \{x\}$ un singleton, on a

$$\begin{aligned} F(\{x\}) &= \{\text{mots réduits en } x \text{ et } x^{-1}\} \\ &= \{\dots, x^{-1}x^{-1}x^{-1}, x^{-1}x^{-1}, x^{-1}, e, x, xx, xxx \dots\} = \{x^n \mid n \in \mathbb{Z}\}\,, \end{aligned}$$

le groupe infini cyclique.

6. Une preuve parfaitement formelle est pénible à écrire sans être éclairante, raison pour laquelle nous n'en rédigeons pas.

3. Pour $X = \{x, y\}$, c'est déjà beaucoup plus compliqué. Le groupe $F(\{x, y\})$ est infini et non-abélien (voir Remarque II.36.1 ci-dessous). Il est instructif de visualiser ses éléments comme les sommets d'un graphe infini, partiellement esquissé [7] en Figure 2. Le sommet du milieu correspond au neutre, chaque

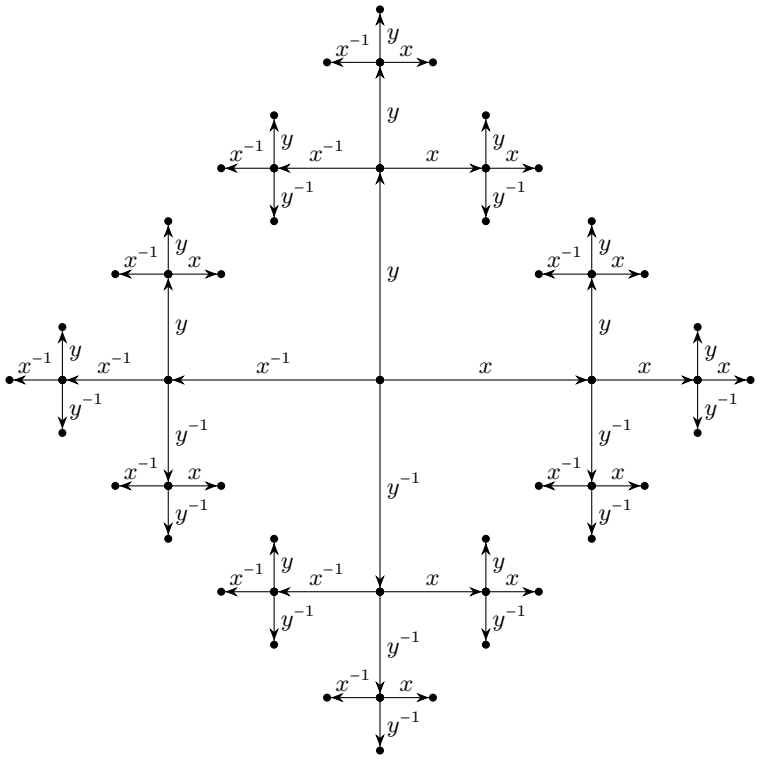


FIGURE 2 – Une approximation d'ordre 3 du graphe décoré correspondant à F_2.

pas à droite (resp. à gauche) correspond à la multiplication du mot par x (resp. x^{-1}), et chaque pas vers le haut (resp. le bas) à la multiplication par y (resp. y^{-1}). Une meilleure approximation de ce graphe infini, cette fois sans les décorations, est donnée en Figure 3.

Terminons cette sous-section avec quelques remarques.

Remarques II.36.

1. Le groupe libre $F(X)$ est infini pour X non-vide, puisqu'il contient en particulier toutes les puissances de tout $x \in X$. De plus, il est non-abélien pour $\#X > 1$, puisque $xy \neq yx \in F(X)$ pour tous $x, y \in X$ distincts.
2. Comme on l'a vu en Corollaire II.33, le groupe $F(X)$ ne dépend à isomorphisme près que du cardinal $\#X$ de X. Pour $\#X = n$, on note $F(X) =: F_n$ le *groupe libre de rang* n.
3. Au Théorème II.42, on verra qu'en fait, deux groupes libres $F(X)$ et $F(Y)$ sont isomorphes si et seulement si X et Y ont même cardinal. En particulier, les groupes F_n et F_m ne sont pas isomorphes si $n \neq m$.

7. Voir ce lien pour une manière de générer ce dessin, et celui de la Figure 3.

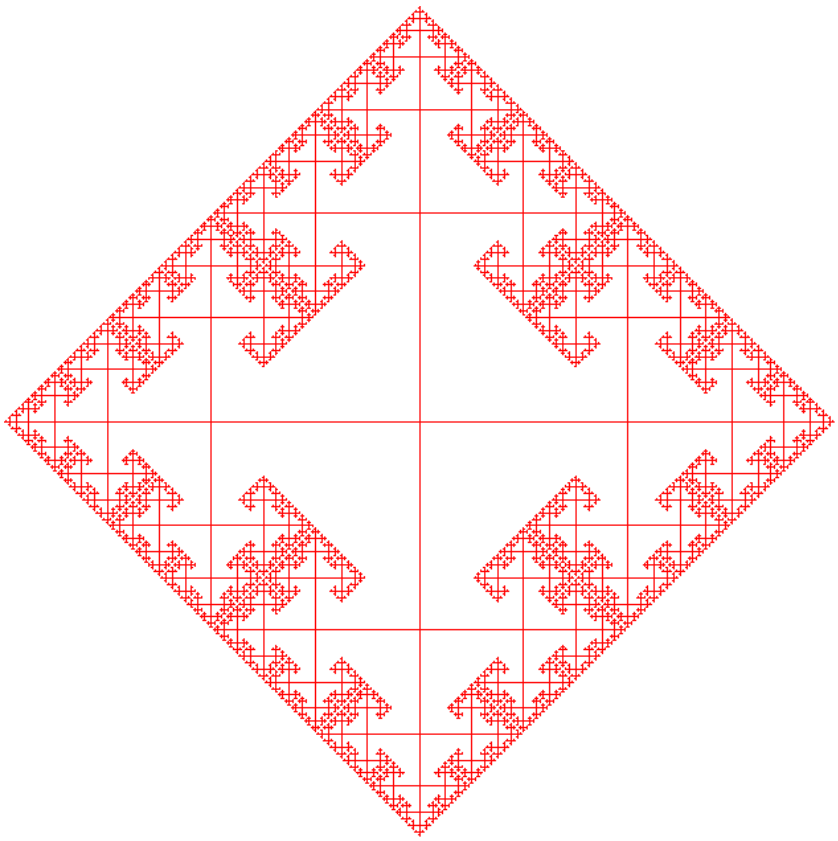


FIGURE 3 – Une approximation d'ordre 7 du graphe correspondant à F_2.

4. Vous verrez en TOPOLOGIE ALGÉBRIQUE le résultat suivant : tout sous-groupe d'un groupe libre est libre. Ce n'est pas très suprenant pour F_0 (tout sous-groupe du groupe trivial est trivial) ni pour F_1 (tout sous-groupe de $\mathbb{Z}$ est trivial ou isomorphe à $\mathbb{Z}$). De manière plus étonnante, le groupe F_n avec $n \geq 2$ contient des sous-groupes libres de rang $m > n$.

II.3.3 Groupes abéliens libres

Il est instructif de jouer le même jeu dans la catégorie Ab des groupes abéliens au lieu de la catégorie Grp des groupes. Ainsi, la question à laquelle on tente de répondre est la suivante :

Étant donné un ensemble X, comment construire un groupe abélien $F_{\mathrm{ab}}(X)$ contenant X "de la façon la plus efficace possible" ?

À nouveau, la formalisation de cette question se fait au moyen d'un objet initial d'une catégorie $\mathscr{C}_{\mathrm{ab}}^X$ associée à l'ensemble X, ce qui se traduit en la propriété universelle suivante.

Définition II.37

Soit X un ensemble. Un **groupe abélien libre** sur X est la donnée d'un groupe abélien $F_{\mathrm{ab}}(X)$ et d'une application $j\colon X \to F_{\mathrm{ab}}(X)$ qui satisfait la propriété universelle suivante : pour toute application $f\colon X \to A$ avec A un groupe abélien, il existe un unique homomorphisme $\varphi\colon F_{\mathrm{ab}}(X) \to A$ tel que $\varphi \circ j = f$.

$$\begin{array}{ccc} X & \xrightarrow{\forall f} & A\,. \\ {\scriptstyle j}\downarrow & \nearrow_{\exists!\varphi} & \\ F_{\mathrm{ab}}(X) & & \end{array} \tag{II.5}$$

Exactement comme pour les groupes libres, on montre que si $F_{\mathrm{ab}}(X)$ existe :

(i) Il est unique à unique isomorphisme près (dans la catégorie $\mathscr{C}_{\mathrm{ab}}^{X}$) ; en particulier, deux groupes abéliens libres sur X sont isomorphes.

(ii) L'application j est injective.

(iii) Le groupe $F_{\mathrm{ab}}(X)$ est engendré par $j(X)$.

(iv) L'association $\mathscr{F}(X) = F_{\mathrm{ab}}(X)$ et $\mathscr{F}(f\colon X \to Y)\colon F_{\mathrm{ab}}(X) \to F_{\mathrm{ab}}(X)$ l'unique homomorphisme tel que $\mathscr{F}(f) \circ j_X = j_Y \circ f$ définit un foncteur $\mathscr{F}\colon \mathsf{Set} \to \mathsf{Ab}$.

Reste à construire le groupe abélien libre : c'est le but de la proposition suivante.

Proposition II.38. *Pour tout ensemble X, il existe un groupe abélien libre $F_{\mathrm{ab}}(X)$.*

Démonstration. Pour X un ensemble quelconque, on connaît le groupe abélien [8]

$$\mathbb{Z}^X := \mathrm{Hom}_{\mathsf{Set}}(X, \mathbb{Z}) = \{\alpha\colon X \to \mathbb{Z}\}\,.$$

Considérons le sous-ensemble

$$\mathbb{Z}^{\oplus X} := \{\alpha\colon X \to \mathbb{Z} \mid \alpha(x) \neq 0 \text{ pour un nombre fini de } x \in X\}$$

de $\mathbb{Z}^X$, qui est clairement un sous-groupe. Par exemple, si X est de cardinal fini n, alors on obtient simplement

$$\mathbb{Z}^{\oplus X} = \mathbb{Z}^X \simeq \overbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}^{n} =: \mathbb{Z}^n\,. \tag{II.6}$$

La première égalité vient de la définition de $\mathbb{Z}^{\oplus X}$, et l'isomorphisme est donné par un ordre total arbitraire sur les éléments de X.

Soit encore $j\colon X \to \mathbb{Z}^{\oplus X}$, $x \mapsto j_x$ l'application donnée par $j_x(x') = 1$ si $x' = x$ et $j_x(x') = 0$ sinon. Dans le cas de $\#X = n$ fini, cette application $j\colon X \to \mathbb{Z}^n$ envoie le premier élément de X sur $j_1 := (1, 0, \ldots, 0)$, le second sur $j_2 := (0, 1, 0, \ldots, 0)$, et ainsi de suite jusqu'au dernier sur $j_n := (0, \ldots, 0, 1)$.

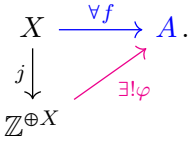
Notons que tout $\alpha \in \mathbb{Z}^{\oplus X}$ s'écrit de manière unique comme combinaison $\mathbb{Z}$-linéaire des $\{j_x\}_{x \in X}$ via

$$\alpha = \sum_{x \in X} \alpha(x) j_x\,, \tag{II.7}$$

8. Rappelons que pour tout ensemble X et tout groupe abélien $(A, +)$, l'ensemble A^X est un groupe pour la loi de composition $(\alpha + \beta)(x) = \alpha(x) + \beta(x)$ pour $\alpha, \beta \in A^X$ et $x \in X$.

une somme finie par définition de $\mathbb{Z}^{\oplus X}$: cela se vérifie en évaluant les deux côtés en un élément arbitraire de X. Dans le cas de $\#X = n$ fini, cela signifie simplement que tout élément de $\mathbb{Z}^n$ s'écrit de manière unique comme combinaison $\mathbb{Z}$-linéaire des $\{j_1, \dots, j_n\}$, et les $\alpha(x)$ sont les coordonnées du vecteur α.

Nous allons à présent vérifier que $j\colon X \to \mathbb{Z}^{\oplus X}$ satisfait la propriété universelle du groupe abélien libre sur X illustrée ci-dessous :



Soit donc $f\colon X \to A$ une application avec A un groupe abélien. Si $\varphi\colon \mathbb{Z}^{\oplus X} \to A$ est un homomorphisme tel que $\varphi \circ j = f$, il satisfait nécessairement

$$\varphi(\alpha) \overset{(II.7)}{=} \varphi\Big(\sum_{x\in X} \alpha(x) j_x\Big) = \sum_{x\in X} \alpha(x)\varphi(j_x) = \sum_{x\in X} \alpha(x)(\varphi\circ j)(x) = \sum_{x\in X} \alpha(x) f(x)\,.$$

Ainsi, un tel homomorphisme est uniquement déterminé, et il reste juste à vérifier que l'application $\varphi\colon \mathbb{Z}^{\oplus X} \to A$ définie via $\varphi(\alpha) = \sum_{x\in X} \alpha(x) f(x)$ est bien un homomorphisme. Et en effet, pour tous $\alpha, \beta \in \mathbb{Z}^{\oplus X}$, on a

$$\begin{aligned}\varphi(\alpha+\beta) &\overset{(II.7)}{=} \varphi\Big(\sum_{x\in X} \alpha(x) j_x + \sum_{x\in X} \beta(x) j_x\Big) = \varphi\Big(\sum_{x\in X} (\alpha(x)+\beta(x)) j_x\Big) \\ &\overset{\text{def}\varphi}{=} \sum_{x\in X} (\alpha(x)+\beta(x)) f(x) = \sum_{x\in X} \alpha(x) f(x) + \sum_{x\in X} \beta(x) f(x) = \varphi(\alpha) + \varphi(\beta)\,.\end{aligned}$$

Cela conclut la preuve. □

Notons que cette preuve implique un isomorphisme $F_{\text{ab}}(X) \simeq \mathbb{Z}^{\oplus X}$. En particulier, pour X fini de cardinal n, on a $F_{\text{ab}}(X) \simeq \mathbb{Z}^n$. Cela motive la terminologie suivante.

Terminologie II.39. On dit que $\mathbb{Z}^n$ est le *groupe abélien libre de rang n*.

Remarque II.40. Il est possible et souvent instructif de jouer ce même jeu non seulement dans les catégories Grp et Ab, mais encore dans les catégories K-Vect, Ann, Top, et autres. Pour être précis, on peut définir la notion d'*objet libre* dans n'importe quelle *catégorie concrète*, c'est-à-dire une catégorie $\mathscr{C}$ munie d'un foncteur oubli $\mathscr{G}\colon \mathscr{C} \to \mathsf{Set}$ tel que tout $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ est déterminé par l'application $\mathscr{G}(f)\colon \mathscr{G}(A) \to \mathscr{G}(B)$. Cela sera discuté en exercice.

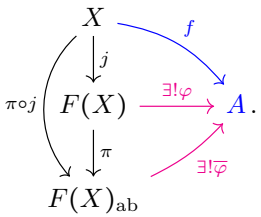
Nous terminons cette section par une discussion d'une construction alternative du groupe abélien libre, qui mènera au résultat remarquable annoncé en Remarque II.36.3. : deux groupes libres $F(X)$ et $F(Y)$ sont isomorphes si et seulement si les ensembles X et Y sont en bijection. Néanmoins, cette construction alternative est basée sur l'abélianisation (du groupe libre). Comme ce concept n'a pas été vu en détail en cours, nous ferons de même avec cette discussion qui figure ici pour votre culture et ne fait pas partie du champ des examens.

Démonstration alternative de la Proposition II.38. Cette seconde preuve est de nature abstraite et repose sur l'existence du groupe libre, établie en Sous-section II.3.2, et de l'abélianisé (Proposition II.25). Soient $j\colon X \to F(X)$ le groupe libre sur un ensemble quelconque X, et $\pi\colon F(X) \to F(X)_{\mathrm{ab}} = F(X)/[F(X), F(X)]$ la projection canonique. Nous allons vérifier que $\pi \circ j\colon X \to F(X)_{\mathrm{ab}}$ satisfait la propriété universelle du groupe abélien libre, ce qui impliquera donc $F_{\mathrm{ab}}(X) \simeq F(X)_{\mathrm{ab}}$ et justifera la notation.

Soit donc $f\colon X \to A$ une application avec A un groupe abélien. Par la propriété universelle du groupe libre, il existe un unique homomorphisme $\varphi\colon F(X) \to A$ tel que $\varphi \circ j = f$. Par la propriété universelle de l'abélianisé, il existe un unique homomorphisme $\overline{\varphi}\colon F(X)_{\mathrm{ab}} \to A$ tel que $\overline{\varphi} \circ \pi = \varphi$. Ainsi, cet homomorphisme satisfait bien

$$\overline{\varphi} \circ (\pi \circ j) = (\overline{\varphi} \circ \pi) \circ j = \varphi \circ j = f\,,$$

une situation résumée dans le diagramme suivant :



De plus, si un homomorphisme $\psi\colon F(X)_{\mathrm{ab}} \to A$ satisfait $\psi \circ (\pi \circ j) = f$, alors on a $(\psi \circ \pi) \circ j = f$, d'où $\psi \circ \pi = \varphi$ par unicité dans la propriété universelle du groupe libre, ce qui implique $\psi = \overline{\varphi}$ par unicité dans la propriété universelle de l'abélianisé. Ainsi, cet homomorphisme est bien unique, ce qui termine la preuve alternative. □

Corollaire II.41. *Pour tout ensemble X, on a un isomorphisme $F(X)_{\mathrm{ab}} \simeq \mathbb{Z}^{\oplus X}$. En particulier, pour X de cardinal n fini, on a $(F_n)_{\mathrm{ab}} \simeq \mathbb{Z}^n$.*

Démonstration. La preuve alternative donne un isomorphisme $F(X)_{\mathrm{ab}} \simeq F_{\mathrm{ab}}(X)$ et la première preuve l'isomorphisme $F_{\mathrm{ab}}(X) \simeq \mathbb{Z}^{\oplus X}$. Pour $\#X = n$, on a $F(X) = F_n$ par définition et $\mathbb{Z}^{\oplus X} \simeq \mathbb{Z}^n$ par (II.6). □

Nous pouvons maintenant démontrer le résultat annoncé en Remarque II.36.3.

Théorème II.42

Pour deux ensembles X et Y, les énoncés suivants sont équivalents :

(i) Les ensembles X et Y sont en bijection.

(ii) Les groupes libres $F(X)$ et $F(Y)$ sont isomorphes.

(iii) Les groupes abéliens libres $F_{\mathrm{ab}}(X)$ et $F_{\mathrm{ab}}(Y)$ sont isomorphes.

Démonstration. Le fait que le point (i) implique le point (ii) n'est autre que le Corollaire II.33, une conséquence immédiate de la fonctorialité du groupe libre. Similairement, comme $F_{\mathrm{ab}}(X) \simeq F(X)_{\mathrm{ab}}$ (par la seconde preuve de la Proposition II.38), l'implication de (iii) par (ii) découle du Corollaire II.28, lui-même une conséquence de la fonctorialité de l'abélianisation.

Ainsi, il reste à montrer que le point (iii) implique le point (i). Par la première preuve de la Proposition II.38, cela revient à montrer que si $\mathbb{Z}^{\oplus X}$ et $\mathbb{Z}^{\oplus Y}$ sont isomorphes, alors X et Y ont même cardinal. Pour démontrer ce fait, nous allons utiliser

la construction suivante : à tout groupe abélien A, on peut associer le groupe abélien quotient $A/2A$ par le sous-groupe (normal) $2A \coloneqq \{2\alpha \mid \alpha \in A\}$. Comme on le verra en exercice, cela définit un foncteur $\mathscr{F}\colon \mathsf{Ab} \to \mathbb{F}_2\text{-}\mathsf{Vect}$ de la catégorie des groupes abéliens dans la catégorie des espaces vectoriels sur $\mathbb{F}_2$. Si $\mathbb{Z}^{\oplus X}$ et $\mathbb{Z}^{\oplus Y}$ sont isomorphes, alors les $\mathbb{F}_2$-espaces vectoriels $\mathscr{F}(\mathbb{Z}^{\oplus X})$ et $\mathscr{F}(\mathbb{Z}^{\oplus Y})$ sont également isomorphes. Par la classification des espaces vectoriels, ils ont même dimension, qu'il reste à calculer. On vérifie comme en (II.7) que tout $[\alpha] \in \mathbb{Z}^{\oplus X}/2\mathbb{Z}^{\oplus X}$ s'écrit de manière unique comme combinaison $\mathbb{F}_2$-linéaire des $\{j_x\}_{x\in X}$ via

$$[\alpha] = \sum_{x\in X} [\alpha(x)] j_x \,,$$

où $[a] \in \mathbb{F}_2$ est la classe de $a \in \mathbb{Z}$ modulo 2. En d'autres termes, la famille $\{j_x\}_{x\in X}$ forme une base de $\mathscr{F}(\mathbb{Z}^{\oplus X})$. Par définition, sa dimension est donc le cardinal de X. On obtient donc $\#X = \dim(\mathscr{F}(\mathbb{Z}^{\oplus X})) = \dim(\mathscr{F}(\mathbb{Z}^{\oplus Y})) = \#Y$, ce qui conclut la preuve. □

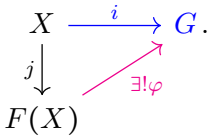
II.3.4 Présentations par générateurs et relations

Entre autres applications, les groupes libres servent à "présenter les groupes par générateurs et relations". C'est le but de cette sous-section.

Rappelons qu'un sous-ensemble $X \subset G$ est un ensemble de *générateurs* de G si on a $\langle X \rangle = G$. Bien entendu, un tel ensemble existe toujours, par exemple en prenant $X = G$ tout entier.

Lemme II.43. *Si $X \subset G$ est un ensemble de générateurs, alors on a un isomorphisme $G \simeq F(X)/N$ pour un certain sous-groupe normal $N \triangleleft F(X)$.*

Démonstration. Soit donc G un groupe quelconque, et $X \subset G$ tel que $\langle X \rangle = G$. Par la propriété universelle du groupe libre $F(X)$ appliquée à l'inclusion $i\colon X \to G$, il existe un unique homomorphisme $\varphi\colon F(X) \to G$ tel que $\varphi \circ j = i$:



Ainsi, $\mathsf{Im}(\varphi)$ est un sous-groupe de G qui contient $\mathsf{Im}(\varphi \circ j) = \mathsf{Im}(i) = X$, d'où $G = \langle X \rangle \subset \mathsf{Im}(\varphi)$ et φ est surjectif. On conclut avec le théorème d'isomorphisme (Théorème II.3) appliqué à φ avec $N \coloneqq \mathrm{Ker}(\varphi) \triangleleft F(X)$. □

Ainsi, tout ensemble de générateurs X induit un isomorphisme $G \simeq F(X)/N$ pour un certain $N \triangleleft F(X)$, i.e. pour certain ensemble N de mots réduits sur X. Comment "se donner" cet ensemble N de manière économe ?

Terminologie II.44. Étant donné un sous-ensemble R d'un groupe G, on note

$$\langle\langle R \rangle\rangle = \bigcap_{R \subset N \triangleleft G} N$$

l'intersection des sous-groupes normaux de G qui contiennent R. On parle du *sous-groupe normal engendré* par $R \subset G$. Il s'agit du plus petit sous-groupe normal de G qui contient R (exercice).

Nous pouvons finalement introduire la notion centrale de cette sous-section.

Définition II.45

Soit G un groupe. Une **présentation** de G est la donnée :

- d'un ensemble X, dont les éléments sont les **générateurs** ;
- d'un ensemble $R \subset F(X)$ de mots réduits en X, les **relations** ;
- d'un isomorphisme explicite $F(X)/\langle\langle R\rangle\rangle \simeq G$.

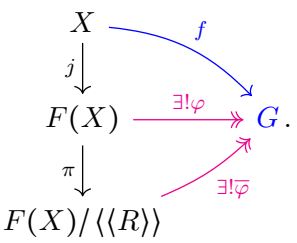
On note alors :

$$G = \langle X \mid R\rangle \ .$$

Remarques II.46.

1. Par le Lemme II.43, tout groupe admet une présentation : il suffit de prendre $X = G$ et $R = N$. En fait, tout groupe admet une infinité de présentations. Mais bien entendu, on va avoir tendance à chercher les présentations les plus simples possibles.
2. Par définition, un groupe G est déterminé à isomorphisme près par une présentation.
3. Toute présentation définit un groupe : c'est donc un outil extrêmement commode pour se donner un groupe.
4. Dans la pratique, si l'on souhaite démontrer qu'un groupe admet une présentation $G = \langle X \mid R\rangle$, il convient souvent de procéder comme suit :
   - Commencer par trouver une application[9] $f : X \to G$ telle que $f(X)$ engendre G.
   - Par la propriété universelle du groupe libre, il existe un unique homomorphisme $\varphi : F(X) \to G$ tel que $\varphi \circ j = f$. Comme l'image de f engendre G, l'homomorphisme φ est surjectif (voir la preuve du Lemme II.43).
   - On vérifie que $\varphi(w) = e$ pour tout $w \in R$. On a donc $R \subset \mathrm{Ker}(\varphi) \lhd F(X)$, d'où $\langle\langle R\rangle\rangle \subset \mathrm{Ker}(\varphi)$ par minimalité du sous-groupe normal engendré (Terminologie II.44). Par la propriété universelle du quotient, il existe un unique homomorphisme $\overline{\varphi} : F(X)/\langle\langle R\rangle\rangle \to G$, qui est surjectif car φ l'est.
   - Le dernier point, très souvent le plus difficile, est de vérifier que $\overline{\varphi}$ est injectif. Cela implique que $\overline{\varphi}$ est l'isomorphisme recherché.

   Cette construction est illustrée par le diagramme ci-dessous, où les flèches doubles dénotent la surjectivité :



(II.8)

9. qui permet d'interpréter chaque $x \in X$ comme un élément $f(x) \in G$.

Voyons à présent quelques exemples.

Exemples II.47 (présentations)**.**

1. Le groupe libre sur X admet la présentation
$$F(X) = \langle X \mid \varnothing \rangle \ .$$
En effet, comme $\langle\langle \varnothing \rangle\rangle = \{e\}$, on a bien un isomorphisme $F(X)/\{e\} \simeq F(X)$. (Avec les notations du diagramme (II.8), on a simplement $f = j$ et $\varphi = \mathrm{id}$.) C'est d'ailleurs dans ce sens que ce groupe est *libre* : respectivement à l'ensemble de générateurs X, il n'est sujet à aucune relation.
En particulier, on a donc les présentations
$$\{e\} = \langle \varnothing \mid \varnothing \rangle \ , \quad \mathbb{Z} \simeq F_1 = \langle x \mid \varnothing \rangle \ , \quad F_2 = \langle x, y \mid \varnothing \rangle \ .$$
Mais le groupe trivial admet également la présentation $\{e\} = \langle x \mid x \rangle$, par exemple, puisqu'avec $X = R = \{x\}$, on obtient
$$F(X)/\langle\langle R \rangle\rangle = \{x^k \mid k \in \mathbb{Z}\}/\langle\langle x \rangle\rangle = \langle x \rangle / \langle x \rangle = \{e\} \, .$$
2. Le groupe cyclique d'ordre n admet la présentation
$$\mathbb{Z}/n\mathbb{Z} = \langle x \mid x^n \rangle \ .$$
En effet, considérons la projection canonique $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. En adoptant la notation multiplicative $\mathbb{Z} = \{x^k \mid k \in \mathbb{Z}\} = F(\{x\})$, on obtient un homomorphisme surjectif $\varphi\colon F(\{x\}) \to \mathbb{Z}/n\mathbb{Z}$ donné par $\varphi(x^k) = [k]$, de noyau $\mathrm{Ker}(\varphi) = \{(x^n)^\ell \mid \ell \in \mathbb{Z}\} = \langle\langle x^n \rangle\rangle$. Par le premier théorème d'isomorphisme, cela induit l'isomorphisme voulu. (Avec les notations du diagramme (II.8), on aurait $f\colon \{x\} \to \mathbb{Z}/n\mathbb{Z}$ défini via $f(x) = [1]$.)
3. Le groupe abélien libre de rang 2 admet la présentation
$$\mathbb{Z}^2 = \langle x, y \mid [x, y] \rangle \ .$$
C'est intuitivement clair : comme $\mathbb{Z}^2 \simeq (F_2)_{\mathrm{ab}} = F_2/[F_2, F_2]$, il suffit de vérifier que le sous-groupe normal de F_2 engendré par $[x, y]$ donne $[F_2, F_2]$. (Avec les notations du diagramme (II.8), on aurait $f\colon \{x, y\} \to \mathbb{Z}^2$ défini via $f(x) = (1, 0)$ et $f(y) = (0, 1)$.) Mais si l'inclusion $\langle\langle [x, y] \rangle\rangle \subset [F_2, F_2]$ est triviale, l'autre est assez pénible à vérifier formellement, ce que nous ne ferons pas, car ce résultat peut également s'obtenir comme une conséquence de la Proposition II.48 ci-dessous. Plus généralement, cette proposition implique que le groupe abélien libre de rang n admet la présentation
$$\mathbb{Z}^n = \langle x_1, \ldots, x_n \mid [x_i, x_j],\ i \neq j \rangle \ .$$
Profitons de cet exemple pour une remarque générale. Parfois, on notera une relation w comme une égalité $w = e$. Par exemple, la relation $[x, y]$ signifie $[x, y] = e$, qui est équivalente à l'égalité $xy = yx$. Ainsi, on peut noter
$$\mathbb{Z}^2 = \langle x, y \mid xy = yx \rangle \ .$$
Cette notation donne tout son sens à la terminologie *relation* : l'égalité $xy = yx$ est une relation satisfaite par les deux générateurs x et y.

4. Le groupe symétrique de degré 3 admet la présentation [10]

$$S_3 = \langle x, y \mid x^2, y^2, xyx = yxy \rangle .$$

Appliquons la méthode de la Remarque II.46.4. Soit $f: X = \{x, y\} \to S_3$ donnée par $f(x) = (1,2)$ et $f(y) = (2,3)$. Comme ces deux cycles engendrent S_3, on obtient un homomorphisme sujectif $\varphi: F_2 \to S_3$. De plus, comme $\varphi(x^2) = \varphi(x)^2 = f(x)^2 = (1,2)^2 = \mathrm{id}$ et $\varphi(y^2) = \varphi(y)^2 = f(y)^2 = (2,3)^2 = \mathrm{id}$, tandis que

$$\varphi(xyx) = (1,2)(2,3)(1,2) = (1,3) = (2,3)(1,2)(2,3) = \varphi(yxy),$$

on a bien $R \subset \mathrm{Ker}(\varphi)$, d'où un homomorphisme sujectif $\overline{\varphi}: F_2/\langle\langle R \rangle\rangle \to S_3$. Comme S_3 est d'ordre 6, il reste à énumérer les éléments du quotient. On se convainc facilement de l'égalité

$$F_2/\langle\langle R \rangle\rangle = \langle x, y \mid x^2, y^2, xyx = yxy \rangle = \{e, x, y, xy, yx, xyx\},$$

d'où un quotient également d'ordre 6. L'homomorphisme $\overline{\varphi}$ est donc bien un isomorphisme.

5. Pour tout $n \geq 3$, le groupe diédral D_{2n} admet la présentation

$$D_{2n} = \langle x, y \mid x^2, y^n, xyxy \rangle .$$

C'est un exercice.

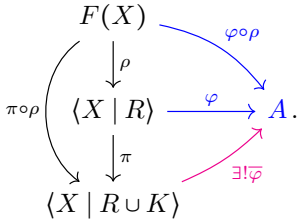
La proposition ci-dessous est utile pour les exemples, mais sa preuve ne sera pas discutée en cours et ne fait donc pas partie du champ des examens.

Proposition II.48. *Si un groupe G admet la présentation $G = \langle X \mid R \rangle$, alors son abélianisé admet la présentation*

$$G_{\mathrm{ab}} = \langle X \mid R \cup \{[x, y] \mid x, y \in X\} \rangle .$$

Démonstration. Adoptons les notations $\langle X \mid R \rangle = F(X)/\langle\langle R \rangle\rangle$ (et similairement pour d'autres présentations) et $K := \{[x, y] \mid x, y \in X\}$. Notons tout d'abord que la propriété universelle du quotient via la projection $\rho: F(X) \to \langle X \mid R \rangle$ implique que la projection $F(X) \to \langle X \mid R \cup K \rangle$ induit un unique homomorphisme $\pi: \langle X \mid R \rangle \to \langle X \mid R \cup K \rangle$. Nous allons vérifier qu'il satisfait la propriété universelle de l'abélianisation de $\langle X \mid R \rangle$, ce qui impliquera $G_{\mathrm{ab}} = \langle X \mid R \cup K \rangle$.

Pour ce faire, notons que $\langle X \mid R \cup K \rangle$ est bien abélien, puisqu'il est engendré par un ensemble de générateurs qui commutent tous les uns avec les autres. Soit à présent $\varphi: \langle X \mid R \cup K \rangle \to A$ un homomorphisme avec A abélien. Considérons le diagramme ci-dessous :



10. où l'on a noté des deux premières relations comme des mots, et la troisième comme une égalité

Comme $(\varphi \circ \rho)(w) = e$ pour tout $w \in R$ (car $\rho(w) = e$) et pour tout $w \in K$ (car A est abélien), la propriété universelle du quotient appliquée au triangle extérieur implique qu'il existe un unique homomorphisme $\overline{\varphi}\colon \langle X \mid R \cup K\rangle \to A$ tel que $\overline{\varphi} \circ (\pi \circ \rho) = \varphi \circ \rho$. Comme ρ est surjectif, cela implique $\overline{\varphi} \circ \pi = \varphi$, et l'on a bien vérifié la propriété universelle de l'abélianisation. □

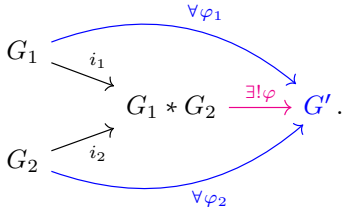
Terminons cette sous-section avec une dernière remarque. La situation peut paraître idyllique, puisque tout groupe est déterminé par une donnée combinatoire. [11] Malheureusement, il est souvent très difficile en pratique de déterminer si deux présentations donnent des groupes isomorphes, ou même si un mot est trivial ou non dans une présentation donnée. [12]

II.3.5 Produit libre

Il s'avère que les présentations par générateurs et relations donnent une construction simple du coproduit dans la catégorie des groupes, appelé le *produit libre*. Par manque de temps, nous n'allons pas en discuter en détail en cours. Cette section figure donc ici pour votre culture, et n'est pas exigible aux examens.

Définition II.49

Le **produit libre** de deux groupes G_1 et G_2 consiste en la donnée d'un groupe $G_1 * G_2$ et d'homomorphismes $i_1\colon G_1 \to G_1 * G_2$, $i_2\colon G_2 \to G_1 * G_2$ satisfaisant la propriété universelle suivante : pour tout groupe G' et tous homomorphismes $\varphi_1\colon G_1 \to G'$ et $\varphi_2\colon G_2 \to G'$, il existe un unique homomorphisme $\varphi\colon G_1 * G_2 \to G'$ avec $\varphi \circ i_1 = \varphi_1$ et $\varphi \circ i_2 = \varphi_2$:



Comme d'habitude, on sait que s'il existe, le produit libre de deux groupes fixés est unique à isomorphisme près. Il s'avère que les présentations donnent une façon de le construire, et ainsi de démontrer son existence.

Proposition II.50. *Si deux groupes admettent les présentations $G_1 = \langle X_1 \mid R_1\rangle$ et $G_2 = \langle X_2 \mid R_2\rangle$, alors le groupe présenté par $\langle X_1 \sqcup X_2 \mid R_1 \sqcup R_2\rangle$ est un produit libre de G_1 et G_2.*

Démonstration. Soient donc $G_1 = \langle X_1 \mid R_1\rangle$ et $G_2 = \langle X_2 \mid R_2\rangle$, et posons $G_1 * G_2 := \langle X_1 \sqcup X_2 \mid R_1 \sqcup R_2\rangle$. On définit $i_1\colon \langle X_1 \mid R_1\rangle \to \langle X_1 \sqcup X_2 \mid R_1 \sqcup R_2\rangle$ via les propriétés universelles du groupe libre et du quotient, comme l'unique homomorphisme $i_1\colon G_1 \to$

11. Et la théorie qui en découle est ce qu'on appelle la *théorie combinatoire des groupes*.
12. Ces problèmes sont en fait *indécidables* : il n'y a en général pas d'algorithme pour leur donner une réponse.

$G_1 * G_2$ tel que $i_1([x_1]) = [x_1]$ pour[13] tout $x_1 \in X_1$. Cette construction est illustrée ci-dessous, où l'on utilise l'inclusion $R_1 \subset R_1 \sqcup R_2 \subset \mathrm{Ker}(\pi \circ \alpha_1)$ pour conclure à l'existence de i_1 :

$$\begin{array}{ccc} X_1 & \xrightarrow{\text{inclusion}} & X_1 \sqcup X_2 \\ \downarrow{\scriptstyle j_1} & & \downarrow{\scriptstyle j} \\ F(X_1) & \xrightarrow{\exists! \alpha_1} & F(X_1 \sqcup X_2) \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi} \\ F(X_1)/\langle\langle R_1 \rangle\rangle & \xrightarrow[\exists! i_1]{} & F(X_1 \sqcup X_2)/\langle\langle R_1 \sqcup R_2 \rangle\rangle \,. \end{array}$$

On procède de même pour la construction de $i_2 : G_2 \to G_1 * G_2$.

Maintenant que l'objet $G_1 * G_2$ et les deux morphismes i_1, i_2 ont été construits, il s'agit de montrer qu'ils satisfont la propriété universelle du produit libre. Soit donc G' un groupe et $\varphi_1 : G_1 \to G'$, $\varphi_2 : G_2 \to G'$ deux homomorphismes. On cherche un homomorphisme $\varphi : G_1 * G_2 \to G'$ tel que $\varphi \circ i_1 = \varphi_1$ et $\varphi \circ i_2 = \varphi_2$, i.e. tel que

$$\varphi([x_1]) = \varphi_1([x_1]) \quad \text{et} \quad \varphi([x_2]) = \varphi_2([x_2]) \tag{II.9}$$

pour tous $x_1 \in X_1$ et $x_2 \in X_2$. Comme $X_1 \sqcup X_2$ engendre $G_1 * G_2$, ces conditions déterminent φ uniquement, et il reste à montrer que φ est bien défini. Pour ce faire, considérons l'application $f : X_1 \sqcup X_2 \to G'$ donnée par $f(x_1) = \varphi_1([x_1])$ et $f(x_2) = \varphi_2([x_2])$ pour $x_1 \in X_1$ et $x_2 \in X_2$. Par la propriété universelle du groupe libre, il existe un unique homomorphisme $\psi : F(X_1 \sqcup X_2) \to G'$ qui étend f. Pour tout $x_1 \in R_1$ (resp. $x_2 \in R_2$), on a $[x_1] = 0 \in G_1$ (resp. $[x_2] = 0 \in G_2$), d'où l'inclusion $R_1 \sqcup R_2 \subset \mathrm{Ker}(\psi)$. L'homomorphisme ψ passe donc au quotient et induit $\varphi : F(X_1 \sqcup X_2)/\langle\langle R_1 \sqcup R_2 \rangle\rangle \to G'$ satisfaisant (II.9). C'est illustré ci-dessous :

$$\begin{array}{ccc} X_1 \sqcup X_2 & & \\ \downarrow{\scriptstyle j} & \overset{f}{\searrow} & \\ F(X_1 \sqcup X_2) & \xrightarrow{\psi} & G' \,. \\ \downarrow{\scriptstyle \pi} & \overset{\exists! \varphi}{\nearrow} & \\ F(X_1 \sqcup X_2)/\langle\langle R_1 \sqcup R_2 \rangle\rangle & & \end{array}$$

Ainsi, $G_1 * G_2$ satisfait bien la propriété universelle du produit libre. □

Voici quelques exemples.

Exemples II.51 (produit libre)**.**

1. Pour tout groupe G, on a
$$G * \{e\} \simeq G \,.$$
Cela se démontre à l'aide de la propriété universelle, ou via la Proposition II.50 et la présentation $\langle \varnothing \,|\, \varnothing \rangle$ du groupe trivial.
2. Par la Proposition II.50 on a plus généralement :
$$F(X) * F(Y) \simeq F(X \sqcup Y) \,.$$
Ainsi, le foncteur $\mathsf{Set} \to \mathsf{Grp}$ du groupe libre préserve les coproduits. Par exemple :
$$\underbrace{\mathbb{Z} * \cdots * \mathbb{Z}}_{n} \simeq F_n \quad \text{et} \quad F_n * F_m \simeq F_{n+m} \,.$$

13. Ici, le premier $[x_1]$ dénote la classe modulo $\langle\langle R_1 \rangle\rangle$, et le second la classe modulo $\langle\langle R_1 \sqcup R_2 \rangle\rangle$.

3. Considérons le produit libre des plus petits groupes non triviaux :

$$\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} \simeq \left\langle a \mid a^2 \right\rangle * \left\langle b \mid b^2 \right\rangle = \left\langle a, b \mid a^2, b^2 \right\rangle .$$

On montrera en exercice que ce groupe est isomorphe au *groupe diédral infini*

$$D_\infty = \left\langle x, y \mid x^2, xyxy \right\rangle ,$$

un groupe infini non-abélien.

Terminons cette sous-section, et cette section, avec quelques remarques.

Remarques II.52.

1. En utilisant les propriétés universelles du produit libre de groupes, du coproduit de groupes abéliens, et de l'abélianisé, on montrera en exercice que pour tous groupes G, G', on a
$$(G * G')_{\mathrm{ab}} \simeq G_{\mathrm{ab}} \oplus G'_{\mathrm{ab}} .$$
Ainsi, le foncteur d'abélianisation $\mathsf{Grp} \to \mathsf{Ab}$ préserve les coproduits.
2. Si deux groupes admettent les présentations $G_1 = \langle X_1 \mid R_1 \rangle$ et $G_2 = \langle X_2 \mid R_2 \rangle$, alors leur produit admet la présentation
$$G_1 \times G_2 = \langle X_1 \sqcup X_2 \mid R_1 \sqcup R_2 \sqcup \{[x_1, x_2] \mid x_1 \in X_1,\, x_2 \in X_2\} \rangle .$$
La preuve repose sur les propriétés universelles du produit de groupes et du quotient. Nous ne la verrons pas en détail, mais il est intéressant de comparer ce fait avec la Proposition II.50.
3. Il existe une construction plus explicite du produit libre qui n'utilise pas de présentation, mais généralise la construction du groupe libre vue en Sous-section II.3.2 : on considère les mots réduits en l'alphabet $G_1 \sqcup G_2$, où cette fois, la réduction consiste à effacer les occurrences de e_{G_1} et e_{G_2} et à remplacer deux lettres consécutives de G_i ($i = 1, 2$) par leur produit dans G_i.
4. Si G_1 et G_2 sont tous deux non-triviaux, alors leur produit libre $G_1 * G_2$ est infini non-abélien. C'est plausible au vu de l'Exemple II.51.3 ci-dessus, mais un peu difficile à montrer avec nos outils. En revanche, la construction mentionnée en Remarque 3 ci-dessus permet de le démontrer facilement.

II.4 Produit semi-direct

Le but de cette section est de présenter une généralisation du produit direct de groupes qui apparaît très naturellement en Géométrie I dans le contexte des isométries euclidiennes, et qui nous sera en particulier utile pour classifier les groupes finis d'ordre donné (Section II.6). On commencera en Sous-section II.4.1 par des rappels et des compléments sur le produit direct (interne et externe), avant de présenter les versions interne et externe du produit semi-direct en Sous-sections II.4.2 et II.4.3.

II.4.1 Produit direct

Rappelons que si G_1 et G_2 sont deux groupes, alors le produit cartésien $G_1 \times G_2$ muni de la loi de composition $(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$ est un groupe, appelé le *produit direct* de G_1 et G_2, et les projections $G_1 \times G_2 \overset{\pi_1}{\rightarrow} G_1$, $G_1 \times G_2 \overset{\pi_2}{\rightarrow} G_2$ satisfont la propriété universelle du produit dans Grp (Définition I.17).

On parle parfois de cette construction comme le produit direct *externe*, par opposition à la version interne que voici.

Terminologie II.53. Un groupe G est *produit direct interne* de sous-groupes $H_1, H_2 < G$ si on a :

(i) $H_1 \cap H_2 = \{e\}$ et $H_1 H_2 = G$;

(ii) H_1 et H_2 sont normaux dans G.

Remarque II.54. La condition (i) ci-dessus est équivalente à l'énoncé suivant : tout élément $g \in G$ s'écrit de manière unique comme $g = h_1 h_2$ avec $h_1 \in H_1$ et $h_2 \in H_2$. C'est un exercice.

Le rapport entre les versions internes et externes du produit direct est donné par la proposition suivante. Ce résultat justifie le fait qu'on parle souvent de *produit direct* sans se soucier de préciser la version.

Proposition II.55. *1. Si $G = G_1 \times G_2$ est le produit direct externe de G_1 et G_2, alors il existe des sous-groupes H_1, H_2 de G avec $H_1 \simeq G_1$, $H_2 \simeq G_2$ et G produit direct interne de H_1 et H_2.*

2. Réciproquement, si un groupe G est produit direct interne de sous-groupes $H_1, H_2 < G$, alors on a un isomorphisme $G \simeq H_1 \times H_2$.

Démonstration. Pour le premier point, soit $G = G_1 \times G_2$ le produit direct de deux groupes G_1 et G_2. Considérons les sous-groupes

$$H_1 = \{(g_1, e_{G_2}) \mid g_1 \in G_1\} = G_1 \times \{e_{G_2}\} \simeq G_1 \,,$$
$$H_2 = \{(e_{G_1}, g_2) \mid g_2 \in G_2\} = \{e_{G_1}\} \times G_2 \simeq G_2 \,.$$

Ces sous-groupes satisfont $H_1 \cap H_2 = \{(e_{G_1}, e_{G_2})\} = \{e_G\}$. On a aussi $H_1 H_2 = G$ puisqu'un élément arbitraire de G s'écrit $(g_1, g_2) = h_1 h_2$ avec $h_1 = (g_1, e_{G_2}) \in H_1$ et $h_2 = (e_{G_1}, g_2) \in H_2$. Finalement, ce sont des sous-groupes normaux de G, par exemple parce que G_1 (resp. G_2) est le noyau de l'homomorphisme π_2 (resp. π_1). Ainsi, le groupe G est bien produit direct interne de H_1 et H_2.

Venons-en au second point. Soit G un groupe qui est produit direct interne de sous-groupes $H_1, H_2 < G$. Considérons l'application

$$\varphi \colon H_1 \times H_2 \longrightarrow G \,, \quad (h_1, h_2) \longmapsto \varphi(h_1, h_2) = h_1 h_2 \,.$$

Nous allons vérifier qu'il s'agit d'un isomorphisme, ce qui conclura la preuve. Pour ce faire, notons tout d'abord que comme H_1 et H_2 sont des sous-groupes

normaux de G, pour tous $h_1 \in H_1$ et $h_2 \in H_2$, on a

$$[h_1, h_2] = h_1 \underbrace{h_2 h_1^{-1} h_2^{-1}}_{\in H_1} \in H_1 \quad \text{et} \quad [h_1, h_2] = \underbrace{h_1 h_2 h_1^{-1}}_{\in H_2} h_2^{-1} \in H_2 \,,$$

d'où $[h_1, h_2] \in H_1 \cap H_2 \overset{(i)}{=} \{e\}$, et donc $h_1 h_2 = h_2 h_1$. Ainsi, pour tous $h_1, h_1' \in H_1$ et $h_2, h_2' \in H_2$, on obtient

$$\varphi((h_1, h_2)(h_1', h_2')) = \varphi(h_1 h_1', h_2 h_2') = h_1 h_1' h_2 h_2' = h_1 h_2 h_1' h_2' = \varphi(h_1, h_2)\varphi(h_1', h_2') \,,$$

et φ est bien un homomorphisme. De plus, comme

$$\mathsf{Im}(\varphi) = \{h_1 h_2 \mid h_1 \in H_1,\ h_2 \in H_2\} = H_1 H_2 \overset{(i)}{=} G \,,$$

cet homomorphisme est surjectif. Finalement, si (h_1, h_2) est dans le noyau de φ, cela signifie $h_1 h_2 = e$, d'où $h_1 = h_2^{-1} \in H_1 \cap H_2 = \{e\}$ et $h_1 = h_2 = e$. Ainsi le noyau $\mathrm{Ker}(\varphi)$ est réduit au neutre (e, e) de $H_1 \times H_2$, et φ est bien un isomorphisme. □

Remarque II.56. Le second point de la proposition ci-dessus est le plus intéressant : pour conclure qu'un groupe G est isomorphe au produit direct de sous-groupes H_1, H_1, il suffit de vérifier les deux conditions de la Terminologie II.53. C'est l'analogue en théorie des groupes de l'énoncé suivant d'algèbre linéaire : si un espace vectoriel E admet deux sous-espaces F_1, F_2 tels que $F_1 \cap F_2 = \{0\}$ et $F_1 + F_2 = E$, alors on a $E \simeq F_1 \oplus F_2$.

II.4.2 Produit semi-direct interne

Considérons à présent la situation suivante, plus générale que celle du produit direct interne.

Terminologie II.57. Soient G un groupe, et $N, H < G$ des sous-groupes. On dit que G est *produit semi-direct interne de N par H* si on a :

(i) $N \cap H = \{e\}$ et $NH = G$;

(ii) N est normal dans G.

Remarques II.58.

1. Si $NH = G$, alors la condition (ii) est équivalente à $hnh^{-1} \in N$ pour tous $n \in N$ et $h \in H$. C'est un exercice.
2. Par cette condition (ii), le groupe H agit sur N par conjugaison. En d'autres termes, on a un homomorphisme de groupes

$$\gamma : H \longrightarrow \mathrm{Aut}(N) \,, \qquad h \longmapsto \left(\gamma_h : n \mapsto hnh^{-1}\right) . \tag{II.10}$$

3. La remarque fondamentale à ce stade, et l'une des motivations de cette terminologie, est la suivante : la loi de composition du groupe G est entièrement déterminée par la donnée des groupes H, N, et de l'homomorphisme $\gamma : H \to \mathrm{Aut}(N)$.

⌜ En effet, par la condition (i), tout élément $g \in G$ s'écrit de manière unique sous la forme $g = nh$ avec $n \in N$ et $h \in H$ (Remarque II.54). De plus, pour tous $g_1 = n_1h_1$ et $g_2 = n_2h_2$ avec $n_1, n_2 \in N$ et $h_1, h_2 \in H$, on a

$$g_1g_2 = (n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1})(h_1h_2) = (n_1\gamma_{h_1}(n_2))(h_1h_2). \tag{II.11}$$

On a donc écrit la composition g_1g_2 comme $g_1g_2 = nh$ avec $n = n_1\gamma_{h_1}(n_2) \in N$ et $h = h_1h_2 \in H$, entièrement déterminés par les lois dans H, N et par γ. ⌟

Exemples II.59 (produits semi-directes internes)**.**

1. Un groupe G est produit direct interne de sous-groupes N, H si et seulement si G est produit semi-direct interne de N par H avec γ trivial (i.e. avec $hn = nh$ pour tous $h \in H$ et $n \in N$). C'est un exercice.
2. Soit
$$G = D_{2n} = \langle x, y \mid x^2, y^n, xyxy \rangle$$
le groupe diédral d'ordre $2n$. Soient $N = \langle y \rangle$ le sous-groupe cyclique d'ordre n engendré par y et $H = \langle x \rangle$ le sous-groupe d'ordre 2 engendré par x. On a clairement $NH = D_{2n}$ et $N \cap H = \{e\}$ puisque tout élément de D_{2n} s'écrit de manière unique sous la forme y^ix^ε avec $0 \leq i < n$ et $\varepsilon \in \{0, 1\}$. De plus, on a également $N \lhd D_{2n}$ via la relation
$$xy^ix^{-1} = (xyx^{-1})^i = (xyx)^i = (y^{-1})^i = y^{-i} \in N$$
et la Remarque II.58.1. Ainsi, le groupe diédral D_{2n} est le produit semi-direct interne de $N \simeq \mathbb{Z}/n\mathbb{Z}$ par $H \simeq \mathbb{Z}/2\mathbb{Z}$.
Cette discussion s'étend au cas $n = 0$, et montre que le groupe diédral infini
$$D_\infty = \langle x, y \mid x^2, xyxy \rangle$$
est le produit semi-direct interne de $\langle y \rangle \simeq \mathbb{Z}$ par $\langle x \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.
3. Soit G le groupe des isométries de l'espace euclidien $\mathbb{R}^n$, à savoir
$$G := \mathrm{Isom}(\mathbb{R}^n) = \{f : \mathbb{R}^n \to \mathbb{R}^n \mid \|f(x) - f(y)\| = \|x - y\| \text{ pour tous } x, y \in \mathbb{R}^n\}.$$
Pour tout $x \in \mathbb{R}^n$, notons $\tau_x \in \mathrm{Isom}(\mathbb{R}^n)$ la translation par le vecteur x définie par $\tau_x(y) = y + x$ pour $y \in \mathbb{R}^n$. Considérons les sous-groupes
$$N := \{\tau_x \in \mathrm{Isom}(\mathbb{R}^n) \mid x \in \mathbb{R}^n\} \simeq \mathbb{R}^n$$
des translations et
$$H := \{\alpha \in \mathrm{Isom}(\mathbb{R}^n) \mid \alpha(0) = 0\}$$
des isométries qui fixent l'origine. On a $N \cap H = \{\mathrm{id}\}$ puisqu'une translation qui fixe l'origine est l'identité. De plus, on a également $G = NH$: en effet, toute isométrie f s'écrit $f = \tau_{f(0)} \circ \alpha$ avec $\tau_{f(0)} \in N$ et $\alpha = \tau_{-f(0)} \circ f \in H$, puisque $\alpha(0) = \tau_{-f(0)}(f(0)) = f(0) - f(0) = 0$. Par la Remarque II.58.1, il reste à vérifier que $\alpha \circ \tau_x \circ \alpha^{-1} \in N$ pour tous $\alpha \in H$ et $x \in \mathbb{R}^n$. Pour ce faire, on peut utiliser un résultat vu en GÉOMÉTRIE I : le sous-groupe H consiste

en les isométries linéaires (d'où un isomorphisme $H \simeq \mathrm{O}(n)$). Par conséquent, on a

$$\begin{aligned}\left(\alpha \circ \tau_x \circ \alpha^{-1}\right)(y) = \alpha(\tau_x(\alpha^{-1}(y))) = \alpha(\alpha^{-1}(y) + x) &\overset{\alpha \text{ lin.}}{=} \alpha(\alpha^{-1}(y)) + \alpha(x) \\ &= y + \alpha(x) = \tau_{\alpha(x)}(y)\end{aligned}$$

pour tout $y \in \mathbb{R}^n$, et donc

$$\alpha \circ \tau_x \circ \alpha^{-1} = \tau_{\alpha(x)} \in N\,. \tag{II.12}$$

Par conséquent, le groupe d'isométries $\mathrm{Isom}(\mathbb{R}^n)$ est produit semi-direct interne de $N \simeq \mathbb{R}^n$ par $H \simeq \mathrm{O}(n)$.

Le dernier exemple ci-dessus est l'une des motivations de l'introduction du concept de produit semi-direct (interne) : si l'on veut comprendre le groupe très naturel des isométries de l'espace euclidien, il faut comprendre les sous-groupes $N \simeq \mathbb{R}^n$ des translations et $H \simeq \mathrm{O}(n)$ des isométries linéaires, mais ça ne suffit pas tout à fait. En effet, les élements de ces sous-groupes ne commutent pas en général (auquel cas on aurait eu $\mathrm{Isom}(\mathbb{R}^n) \simeq N \times H$), mais satisfont la relation (II.12) pour tous $x \in \mathbb{R}^n$ et $\alpha \in H$. Par la Remarque II.58.3, la donnée des sous-groupes N, H et de cette relation détermine ce groupe d'isométries.

II.4.3 Produit semi-direct externe

Maintenant que nous avons généralisé la version interne du produit direct, reste à étendre la version externe, et à faire le lien entre ces deux versions à la façon de la Proposition II.55. C'est le but de cette sous-section.

Soient donc N, H des groupes quelconques, et soit

$$\theta \colon H \longrightarrow \mathrm{Aut}(N)\,, \qquad h \longmapsto \theta_h$$

un homomorphisme arbitraire. En s'inspirant de la formule (II.11), considérons la loi de composition suivante sur l'ensemble $N \times H$:

$$(n_1, h_1) \bullet_\theta (n_2, h_2) \coloneqq (n_1 \theta_{h_1}(n_2), h_1 h_2)\,. \tag{II.13}$$

Lemme II.60. *L'ensemble $N \times H$ muni de la loi de composition $\bullet_\theta$ est un groupe.*

Démonstration. Le neutre est donné par (e_N, e_H), car pour tout $(n, h) \in N \times H$, on a

$$(e_N, e_H) \bullet_\theta (n, h) = (e_N \theta_{e_H}(n), e_H h) \overset{\theta \text{ hom}}{=} (e_N n, e_H h) = (n, h)$$

et

$$(n, h) \bullet_\theta (e_N, e_H) = (n\theta_h(e_N), h e_H) \overset{\theta_h \text{ hom}}{=} (n e_N, h e_H) = (n, h)\,.$$

L'inverse de (n, h) est donné par $(n, h)^{-1} = (\theta_{h^{-1}}(n^{-1}), h^{-1})$, puisqu'on a

$$\begin{aligned}(n, h) \bullet_\theta (\theta_{h^{-1}}(n^{-1}), h^{-1}) = (n\theta_h(\theta_{h^{-1}}(n^{-1})), h h^{-1}) &\overset{\theta \text{ hom}}{=} (n\theta_{h h^{-1}}(n^{-1}), e_H) \\ = (n\theta_{e_H}(n^{-1}), e_H) &\overset{\theta \text{ hom}}{=} (n n^{-1}, e_H) = (e_N, e_H)\end{aligned}$$

et

$$(\theta_{h^{-1}}(n^{-1}), h^{-1}) \bullet_\theta (n,h) = (\theta_{h^{-1}}(n^{-1})\theta_{h^{-1}}(n), h^{-1}h) \overset{\theta_{h^{-1}}\text{ hom}}{=} (\theta_{h^{-1}}(n^{-1}n), e_H)$$
$$= (\theta_{h^{-1}}(e_N), e_H) \overset{\theta_{h^{-1}}\text{ hom}}{=} (e_N, e_H)\,.$$

Finalement, l'associativité se vérifie directement, ce qui est laissé en exercice. □

Définition II.61

Le groupe $(N \times H, \bullet_\theta)$ est appelé le *produit semi-direct externe de N par H*, et noté $N \rtimes_\theta H$.

Remarque II.62. Cette terminologie est universelle, mais prête malheureusement à confusion : on parle *du* produit semi-direct de N par H, alors qu'il n'est souvent pas unique. En effet, comme nous le verrons dans l'Exemple II.63.2 ci-dessous, différents homomorphismes $\theta : H \to \mathrm{Aut}(N)$ (avec les mêmes groupes H et N) peuvent donner des groupes non-isomorphes. Nous tentons de remédier à cet abus de terminologie en gardant le symbole θ en indice dans $\bullet_\theta$ et $\rtimes_\theta$.

Exemples II.63 (produits semi-directs externes)**.**

1. Soient N, H des groupes quelconques, et $\theta : H \to \mathrm{Aut}(N)$ l'homomorphisme trivial. Dans ce cas, on a $(n_1, h_1) \bullet_\theta (n_2, h_2) = (n_1 n_2, h_1 h_2)$, et le produit semi-direct externe n'est autre que le produit direct externe $N \times H$.
2. Soient $N = \mathbb{Z}/n\mathbb{Z}$ (avec $n \geq 1$) et $H = \mathbb{Z}/2\mathbb{Z}$. Dans un premier temps, tentons de comprendre les actions possibles de H sur N. Rappelons l'isomorphisme

$$\mathrm{Aut}(N) = \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^* = \{[k] \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{pgcd}(n,k) = 1\}\,,$$

de (I.3), où l'élément $[k] \in (\mathbb{Z}/n\mathbb{Z})^*$ induit l'automorphisme de $\mathbb{Z}/n\mathbb{Z}$ donné par la multiplication par $k \in \mathbb{Z}$. Comme un homomorphisme

$$\theta : H = \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(N) \simeq (\mathbb{Z}/n\mathbb{Z})^*\,, \quad h \longmapsto \theta_h$$

est équivalent à la donnée d'un élément $\theta_{[1]} =: [k] \in (\mathbb{Z}/n\mathbb{Z})^*$ tel que $[k]^2 = [1]$, nous cherchons donc un entier $k \in \mathbb{Z}$ premier à n tel que $k^2 \equiv 1 \pmod{n}$.

- L'entier $k = 1$ est une solution, mais induit l'homomorphisme θ trivial. Par l'exemple 1 ci-dessus, cela donne le produit direct $N \times H = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- L'entier $k = -1$ en est une autre (pour autant que $n \neq 1, 2$), et induit donc la formule $\theta_h = (-1)^h \mathrm{id}_N$ pour $h \in H$. Par (II.13), on obtient la loi de composition

$$(n_1, h_1) \bullet_\theta (n_2, h_2) = (n_1 + (-1)^{h_1} n_2, h_1 + h_2)$$

définissant le produit-semi direct externe $\mathbb{Z}/n\mathbb{Z} \rtimes_\theta \mathbb{Z}/2\mathbb{Z}$.

Notons que pour $n = 1, 2$, les classes $[-1]$ et $[1]$ coïncident dans $\mathbb{Z}/n\mathbb{Z}$, et on obtient à nouveau le produit direct. En revanche, le groupe $\mathbb{Z}/n\mathbb{Z} \rtimes_\theta \mathbb{Z}/2\mathbb{Z}$ n'est pas abélien [14] pour $n > 2$, et donc pas isomorphe au produit direct $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Notons également que toute cette discussion s'étend *verbatim* au cas $n = 0$, ce qui donne deux groupes non-isomorphes : le produit direct $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et le produit semi-direct $\mathbb{Z} \rtimes_\theta \mathbb{Z}/2\mathbb{Z}$.

3. Plus généralement, soient les groupes $N = \mathbb{Z}/n\mathbb{Z}$ (avec $n \geq 0$) et $H = \mathbb{Z}/m\mathbb{Z}$ (avec $m \geq 2$). La donnée d'un homomorphisme

$$\theta : H = \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathrm{Aut}(N) \simeq (\mathbb{Z}/n\mathbb{Z})^* \ , \quad h \longmapsto \theta_h$$

est équivalente à la donnée de $\theta_{[1]} =: [k] \in (\mathbb{Z}/n\mathbb{Z})^*$ tel que $[k]^m = [1]$, i.e. d'un entier $k \in \mathbb{Z}$ premier à n tel que $k^m \equiv 1 \pmod{n}$. Chaque tel k définit un homomorphisme θ, et un produit-semi direct externe

$$\mathbb{Z}/n\mathbb{Z} \rtimes_\theta \mathbb{Z}/m\mathbb{Z} \tag{II.14}$$

dont la loi de composition est

$$(n_1, h_1) \bullet_\theta (n_2, h_2) = (n_1 + k^{h_1} n_2, h_1 + h_2) \tag{II.15}$$

pour $n_1, n_2 \in N$ et $h_1, h_2 \in H$.
Ce groupe est non-abélien (et donc pas isomorphe au produit direct $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$) si et seulement si $[k] \neq [1] \in \mathbb{Z}/n\mathbb{Z}$, ce qui implique $n \neq 1, 2$.

⌜ En effet, si $[k] = [1] \in \mathbb{Z}/n\mathbb{Z}$, alors on obtient le produit direct par construction. Réciproquement, si $[k] \neq [1] \in (\mathbb{Z}/n\mathbb{Z})^*$, alors on a

$$([0], [1]) \bullet_\theta ([1], [0]) = ([k], [1]) \neq ([1], [1]) = ([1], [0]) \bullet_\theta ([0], [1]) \, ,$$

et ce groupe est non-abélien. Finalement, comme $(\mathbb{Z}/n\mathbb{Z})^*$ est trivial pour $n = 1, 2$, l'existence de $[k] \neq [1] \in (\mathbb{Z}/n\mathbb{Z})^*$ implique $n \neq 1, 2$. ⌟

La relation promise entre produits directes interne et externe est donnée par la proposition suivante, qui étend la Proposition II.55.

Proposition II.64. *(i) Soit $G = N \rtimes_\theta H$ le produit semi-direct externe d'un groupe N par un groupe H via un homomomorphisme $\theta : H \to \mathrm{Aut}(N)$. Alors, il existe des sous-groupes N', H' de G avec $N' \simeq N$ et $H' \simeq H$, tels que G est produit semi-direct interne de N' par H', et θ est réalisé [15] par la conjugaison de N' par les éléments de H'.*

(ii) Réciproquement, si un groupe G est produit semi-direct interne d'un sous-groupe N par un sous-groupe H, alors on a un isomorphisme $G \simeq N \rtimes_\gamma H$ avec $\gamma : H \to \mathrm{Aut}(N)$ donné par la conjugaison (II.10).

14. Un fait plus général est traité en Exemple 3 ci-dessous.

15. Cette dernière affirmation est légèrement floue : son sens précis est à trouver dans la formule (II.16).

Démonstration. Pour vérifier le premier point, considérons donc des groupes N, H arbitraires, un homomorphisme $\theta\colon H \to \mathrm{Aut}(N)$, et soit $G = N \rtimes_\theta H$ le produit semi-direct externe correspondant. Notons tout d'abord que les applications $N \to G$ et $H \to G$ données respectivement par $n \mapsto (n, e_H)$ et $h \mapsto (e_N, h)$ sont des homomorphismes injectifs : cela découle de la définition (II.13) de la loi de composition. Ainsi, les sources de ces applications sont isomorphes à leurs images, qui sont des sous-groupes de G :

$$N \simeq \mathsf{Im}(N \to G) = \{(n, e_H) \mid n \in N\} = N \times \{e_H\} =: N',$$
$$H \simeq \mathsf{Im}(H \to G) = \{(e_N, h) \mid h \in H\} = \{e_N\} \times H =: H'.$$

On a clairement $N' \cap H' = \{(e_N, e_H)\} = \{e_G\}$. On a aussi $N'H' = G$ puisqu'un élément arbitraire (n, h) de G s'écrit $(n, h) = (n, e_H) \bullet_\theta (e_N, h)$. De plus, on vérifie immédiatement que la projection $\pi\colon G \to H$ donnée par $\pi(n, h) = h$ est un homomorphisme de noyau $\mathrm{Ker}(\pi) = N'$, ce qui implique que N' est normal dans G. Finalement, pour tous $n \in N$ et $h \in H$, les éléments correspondants $(n, e_H) \in N'$ et $(e_N, h) \in H'$ satisfont

$$\begin{aligned}(e_N, h) \bullet_\theta (n, e_H) \bullet_\theta (e_N, h)^{-1} &= (e_N \theta_h(n), h e_H) \bullet_\theta (e_N, h^{-1}) \\ &= (\theta_h(n), h) \bullet_\theta (e_N, h^{-1}) = (\theta_h(n)\theta_h(e_N), h h^{-1}) \\ &= (\theta_h(n), e_H) \in N'. \end{aligned} \tag{II.16}$$

C'est la signification précise de la dernière affirmation du premier point.

Passons au second. Soit donc G un groupe qui est produit semi-direct interne d'un sous-groupe N par un sous-groupe H. Considérons l'application

$$\varphi\colon N \rtimes_\gamma H \longrightarrow G, \quad (n, h) \longmapsto \varphi(n, h) = nh.$$

C'est un homomorphisme car pour tous (n_1, h_1) et (n_2, h_2) dans $N \times H$, on a

$$\begin{aligned}\varphi\left((n_1, h_1) \bullet_\gamma (n_2, h_2)\right) &= \varphi\left(n_1 \gamma_{h_1}(n_2), h_1 h_2\right) = \varphi\left(n_1 (h_1 n_2 h_1^{-1}), h_1 h_2\right) \\ &= n_1 (h_1 n_2 h_1^{-1})(h_1 h_2) = n_1 h_1 n_2 h_2 = \varphi(n_1, h_1)\varphi(n_2, h_2).\end{aligned}$$

De plus, comme $\mathsf{Im}(\varphi) = \{nh \mid h \in N,\ h \in H\} = NH = G$, cet homomorphisme est surjectif. Finalement, si (n, h) est dans le noyau de φ, cela signifie $nh = e$, d'où $n = h^{-1} \in N \cap H = \{e\}$ et $h = n = e$. Ainsi le noyau de φ est trivial, et φ est bien un isomorphisme. □

Pour illustrer (le second point de) cette proposition, reprenons les trois exemples de produits semi-directes internes traités en Exemples II.59.

Exemples II.65.

1. Considérons un groupe G produit semi-direct interne de sous-groupes N, H, avec γ trivial (i.e. $hn = nh$ pour tous $h \in H$ et $n \in N$, ce qui implique $H \triangleleft G$). Par la Proposition II.64(ii) et l'Exemple II.63.1, on a un isomorphisme $G \simeq N \times H$. Bien évidemment, ce résultat n'est autre que le second point de la Proposition II.55.

2. Par la Proposition II.64(ii) appliquée à l'Exemple II.59.2 avec $n \geq 1$, on a un isomorphisme

$$D_{2n} = \langle x, y \mid x^2, y^n, xyxy \rangle \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_\gamma \mathbb{Z}/2\mathbb{Z}\,,$$

avec $\langle y \rangle \simeq \mathbb{Z}/n\mathbb{Z}$, $\langle x \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, et l'action $\gamma\colon \langle x \rangle \to \mathrm{Aut}(\langle y \rangle)$ donnée par

$$\gamma_x(y) = xy^i x^{-1} = y^{-i}\,.$$

Dans le cas $n = 0$, on obtient un isomorphisme

$$D_\infty = \langle x, y \mid x^2, xyxy \rangle \simeq \mathbb{Z} \rtimes_\gamma \mathbb{Z}/2\mathbb{Z}$$

avec $\gamma_x(y) = xyx^{-1} = y^{-1}$.

Dans tous les cas, l'action du générateur de $\mathbb{Z}/2\mathbb{Z}$ envoie un élément de $\mathbb{Z}/n\mathbb{Z}$ sur son inverse : on retrouve donc précisément les produits semi-directs externes construits en Exemple II.63.2 (en notation multiplicative).

3. De même, par la Proposition II.64(ii) appliquée à l'Exemple II.59.3, on a un isomorphisme

$$\mathrm{Isom}(\mathbb{R}^n) \simeq \mathbb{R}^n \rtimes_\gamma \mathrm{O}(n)\,,$$

avec $\gamma\colon \mathrm{O}(n) \to \mathrm{Aut}(\mathbb{R}^n)$ donnée par $\gamma_\alpha(x) = \alpha(x)$ pour $\alpha \in \mathrm{O}(n)$ et $x \in \mathbb{R}^n$ puisque l'action par conjugaison satisfait l'égalité (II.12).

Nous terminons cette section avec un dernier résultat dont nous aurons besoin pour la classification des groupes d'ordre produit de deux premiers (Théorème II.110). La preuve est inclue par souci de complétude, mais ne sera pas discutée en cours et ne fait pas partie du champ des examens.

Lemme II.66. *Soient $p < q$ deux nombres premiers avec $q \equiv 1 \pmod p$. À isomorphisme près, il existe un unique produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ qui n'est pas isomorphe au produit direct.*

Démonstration. Cet énoncé se situe dans le cadre de l'Exemple II.63.3, dont nous reprenons les notations et résultats (avec $n = q$ et $m = p$). Rappelons qu'un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes_\theta \mathbb{Z}/p\mathbb{Z}$ non isomorphe au produit direct est déterminé par un homomorphisme non-trivial $\theta\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^*$, lui-même équivalent à la donnée d'un élément $[k] \neq [1] \in (\mathbb{Z}/q\mathbb{Z})^*$ tel que $[k]^p = [1]$, i.e. d'un élément d'ordre p dans $(\mathbb{Z}/q\mathbb{Z})^*$.

Comme vous l'avez vu en Algèbre I, q premier implique que $\mathbb{Z}/q\mathbb{Z} =: \mathbb{F}_q$ est un corps, et que $(\mathbb{Z}/q\mathbb{Z})^* = \mathbb{F}_q^*$ est cyclique d'ordre $q-1$: notons $\alpha \in (\mathbb{Z}/q\mathbb{Z})^*$ un générateur. Comme p est premier et divise $q-1$ par hypothèse, la liste complète des éléments d'ordre p dans $(\mathbb{Z}/q\mathbb{Z})^*$ est donnée par $\{\beta^i \mid 1 \leq i \leq p-1\}$ avec $\beta = \alpha^{(q-1)/p}$. Ainsi, tout $i = 1, \ldots, p-1$ définit un produit semi-direct non-abélien $\mathbb{Z}/q\mathbb{Z} \rtimes_{\theta_i} \mathbb{Z}/p\mathbb{Z}$, dont la loi de composition est donnée, via (II.15), par

$$(n_1, h_1) \bullet_{\theta_i} (n_2, h_2) = (n_1 + \beta^{ih_1} n_2, h_1 + h_2)$$

pour $n_1, n_2 \in \mathbb{Z}/q\mathbb{Z}$ et $h_1, h_2 \in \mathbb{Z}/p\mathbb{Z}$. Mais on vérifie directement que l'application

$$\varphi\colon \mathbb{Z}/q\mathbb{Z} \rtimes_{\theta_i} \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z} \rtimes_{\theta_1} \mathbb{Z}/p\mathbb{Z}\,, \qquad (n, h) \longmapsto (n, ih)$$

est un isomorphisme. Ainsi, tous ces groupes sont isomorphes. □

II.5 Groupes abéliens finis, modules

Le but de cette section est de classifier les groupes abéliens finis. Il s'avère que cette étude se situe à l'intersection de la théorie des groupes et de l'algèbre linéaire, une observation formalisée par la structure de *module* sur un anneau.

On commencera donc par énoncer et discuter le théorème de classification des groupes abéliens finis en Sous-section II.5.1. La preuve sera donnée en Sous-section II.5.2, tandis que la Sous-section II.5.3 consiste en une introduction à la théorie des modules.

II.5.1 Classification des groupes abéliens finis

Un théorème de classification des groupes finis à isomorphisme près est et restera toujours hors de portée : les groupes finis sont tout simplement trop riches pour être classifiés. Il est plus raisonnable de se concentrer sur les groupes finis simples, qu'on peut interpréter comme les "particules élémentaires" à partir desquelles les groupes finis se construisent. Leur classification a effectivement été achevée, l'énoncé portant le doux nom de *théorème énorme*. Et pour cause : la démonstration complète repose sur plus de 500 articles publiés entre 1955 et 1983 par plus de 100 mathématiciens, et couvrant plus de 10'000 pages.

En revanche, l'ajout de l'épithète "abélien" au terme "groupe" nous fait changer de monde : la classification des groupes abéliens finis est suffisamment élémentaire pour faire partie de ce cours. Elle a été obtenue par Leopold Kronecker en 1870.

Leopold Kronecker (1823-1891)

Théorème II.67: Classification des groupes abéliens finis

Soit G un groupe abélien fini. Alors, il existe une suite $p_1^{\nu_1}, \dots, p_n^{\nu_n}$ de puissances positives de nombres premiers pas forcément distincts telle que

$$G \simeq \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{\nu_n}\mathbb{Z}\,.$$

De plus, cette suite est unique à l'ordre près,

Remarques II.68.

1. Insistons sur le fait que ce théorème consiste en réalité en deux énoncés : un résultat de décomposition (tout groupe abélien fini est produit direct de groupes cycliques d'ordre une puissance d'un premier), et un résultat d'unicité (cette suite de puissance de premiers est unique à l'ordre près).
2. Rappelons que si a et b sont des entiers premiers entre eux, alors on a un isomorphisme $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \simeq \mathbb{Z}/ab\mathbb{Z}$. C'est l'objet du *théorème chinois* dont nous avons vu deux preuves en exercices.
3. Si l'on souhaite donner la liste des groupes abéliens d'ordre m fixé à isomorphisme près, il suffit donc de faire la liste des façons d'écrire $m = p_1^{\nu_1} \cdots p_n^{\nu_n}$ avec $p_1, \dots, p_n$ premiers pas forcément distincts et $\nu_1, \dots, \nu_n \geq 1$.

Exemples II.69 (Groupes abéliens d'ordre donné)**.**

1. Soit $m = p$ premier. La seule décomposition possible est $m = p^1$, d'où $n = 1$ et $p_1 = p$, $\nu_1 = 1$. Ainsi, tout groupe abélien d'ordre p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (ce qu'on savait déjà par le théorème de Lagrange et la classification des groupes cycliques, sans l'hypothèse de commutativité).
2. Pour $m = 4$, on obtient les deux décompositions $m = 2^1 \cdot 2^1$ ($n = 2$, $p_1 = p_2 = 2$, $\nu_1 = \nu_2 = 1$) et $m = 2^2$ ($n = 1$ et $p_1 = 2$, $\nu_1 = 2$). Ainsi, tout groupe abélien d'ordre 4 est isomorphe à exactement un groupe parmi $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$ (ce qu'il est facile démontrer, sans l'hypothèse de commutativité [16]).
3. Pour $m = 36$, on obtient les décompositions

$$m = 2^1 \cdot 2^1 \cdot 3^1 \cdot 3^1 = 2^2 \cdot 3^1 \cdot 3^1 = 2^1 \cdot 2^1 \cdot 3^2 = 2^2 \cdot 3^2 .$$

Ainsi, tout groupe abélien d'ordre 36 est isomorphe à exactement un des 4 groupes suivants :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} .$$

Notons que, par le théorème chinois, on a $\mathbb{Z}/36\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. Le groupe cyclique d'ordre 36 fait donc bien partie de cette liste, comme il se doit.

II.5.2 Preuve du théorème de classification

Nous aurons besoin d'étendre légèrement la Terminologie II.53 sur le produit direct interne, de deux facteurs à un nombre fini de facteurs. Cela peut se faire dans le cadre général des groupes, mais le cas abélien suffit ici.

Terminologie II.70. Un groupe abélien G est *produit direct interne* de sous-groupes $H_1, \dots, H_m < G$ si tout $x \in G$ s'écrit de manière unique $x = h_1 + \cdots + h_m$ avec $h_1 \in H_1, \dots, h_m \in H_m$.

Remarque II.71. Dans le cas $m = 2$, un groupe abélien G est produit direct interne de $H_1, H_2 \subset G$ si et seulement si $H_1 + H_1 = G$ et $H_1 \cap H_2 = \{0\}$ (voir Remarque II.54). Ainsi, il s'agit bien d'une extension du produit direct interne vu en Terminologie II.53.

La Proposition II.55(ii) prend alors la forme suivante.

Lemme II.72. *Si G est le produit direct interne de sous-groupes $H_1, \dots, H_m < G$, alors G est isomorphe au produit direct externe $H_1 \times \cdots \times H_m$ des groupes $H_1, \dots, H_m$.*

Démonstration. Considérons l'application

$$\varphi : H_1 \times \cdots \times H_m \longrightarrow G , \quad (h_1, \dots, h_m) \longmapsto h_1 + \cdots + h_m .$$

Il s'agit clairement d'un homomorphisme de groupes abéliens, qui est surjectif et injectif par définition du produit direct interne. C'est donc un isomorphisme. □

16. Moins facile : cela reste vrai pour tout groupe d'ordre p^2 avec p premier, voir Théorème II.94.

Nous terminons ces préliminaires avec un petit rappel.

Remarque II.73. Soit G un groupe abélien dont la loi de composition est notée additivement. Pour tout $x \in G$ et $b \in \mathbb{Z}$, la $b^{\text{ième}}$ puissance de x en notation additive est simplement notée bx.

Avec cette notation, un sous-groupe $H < G$ est cyclique s'il existe $x \in H$ tel que pour tout $h \in H$, il existe $b \in \mathbb{Z}$ avec $h = bx$. Notons que cet entier b n'est pas unique en général : par exemple, dans $H = \mathbb{Z}/2\mathbb{Z}$, le générateur $x = [1]$ peut s'écrire $x = bx$ avec $b = 1$ ou $b = 3$ (en fait, avec tout $b \in \mathbb{Z}$ impair).

Le coeur de la preuve du Théorème II.67 repose sur un énoncé de décomposition, que voici.

Proposition II.74. *Un groupe abélien fini est le produit direct interne d'un nombre fini de sous-groupes cycliques.*

Démonstration. Définissons le *rang* d'un groupe abélien fini G comme le cardinal (fini) d'un ensemble de générateurs de taille minimale. On va démontrer le théorème par récurrence sur le rang de G.

Par convention, un groupe abélien de rang 0 est trivial (produit direct interne de 0 sous-groupe cyclique), tandis que par définition, un groupe abélien de rang 1 est cyclique, donc produit direct interne de 1 sous-groupe cyclique (à savoir lui-même). Le départ de récurrence est donc vérifié.

Soit à présent G un groupe abélien de rang $m \geq 2$, et supposons le théorème démontré pour tout groupe abélien fini de rang au plus $m-1$. Commençons par reformuler ce que l'on souhaite démontrer. On cherche à trouver des éléments $x_1, \ldots, x_m \in G$ tels que tout $x \in G$ s'écrive $x = b_1x_1 + \cdots + b_mx_m$ avec $b_1, \ldots, b_m \in \mathbb{Z}$, et ce de manière unique dans le sens suivant : si on a $b_1x_1 + \cdots + b_mx_m = b'_1x_1 + \cdots + b'_mx_m$ avec $b_i, b'_i \in \mathbb{Z}$, on veut avoir $b_ix_i = b'_ix_i$ pour tout $i = 1, \ldots, m$. En effet, cela signifie précisément que G est le produit direct interne des sous-groupes cycliques engendrés par $x_1, \ldots, x_m$.

Considérons un ensemble $x_1, \ldots, x_m$ de générateurs de G de taille minimale. Supposons qu'on ait la condition suivante :

$$\text{Si } a_1x_1 + \cdots + a_mx_m = 0 \text{ avec } a_1, \ldots, a_m \in \mathbb{Z}, \text{ alors } a_1x_1 = \cdots = a_mx_m = 0\,. \quad (*)$$

Cela impliquerait la proposition, car l'égalité $b_1x_1 + \cdots + b_mx_m = b'_1x_1 + \cdots + b'_mx_m$ s'écrit $(b_1 - b'_1)x_1 + \cdots + (b_m - b'_m)x_m = 0$, ce qui par $(*)$ impliquerait $(b_i - b'_i)x_i = 0$ pour tout i, et donc $b_ix_i = b'_ix_i$ comme voulu. En revanche, si la condition $(*)$ n'est pas satisfaite, il existe des éléments $a_1, \ldots, a_m \in \mathbb{Z}$ non-tous nuls qui satisfont $a_1x_1 + \cdots + a_mx_m = 0$. On a donc une "relation" pour les générateurs $x_1, \ldots, x_m \in G$ avec "coefficients" non-tous nuls $a_1, \ldots, a_m \in \mathbb{Z}$.

L'idée cruciale est la suivante : parmi tous les coefficients non-nuls apparaissant dans toutes les relations pour tous les ensembles de générateurs de taille minimale, choisissons-en un de valeur absolue minimale. Ce coefficient apparait dans une certaine relation pour certains générateurs $y_1, \ldots, y_m$: disons qu'il s'agit du coefficient b_1 dans la relation

$$b_1y_1 + \cdots + b_my_m = 0\,. \quad (**)$$

La stratégie est maintenant de modifier y_1 en y_1^* de telle manière que G soit le produit direct interne du sous-groupe cyclique engendré par y_1^* et du sous-groupe abélien engendré par $y_2, \dots, y_m$. Les détails de l'argument reposent sur trois affirmations, dont voici la première.

Affirmation 1. Si $a_1 y_1 + \cdots + a_m y_m = 0$ avec $a_i \in \mathbb{Z}$, alors $b_1 \mid a_1$ dans $\mathbb{Z}$.

⌜ Comme b_1 non-nul, il existe $q, r \in \mathbb{Z}$ tels que $a_1 = qb_1 + r$ avec $r = 0$ ou $|r| < |b_1|$. Or, les deux relations pour $y_1, \dots, y_m$ impliquent

$$0 = 0 - q \cdot 0 = (a_1 y_1 + \cdots + a_m y_m) - q(b_1 y_1 + \cdots + b_m y_m) = r y_1 + \cdots + (a_m - q b_m) y_m \,.$$

Par minimalité de b_1, on ne peut pas avoir $|r| < |b_1|$. On a donc bien $r = 0$, d'où $a_1 = qb_1$ et donc $b_1 \mid a_1$ comme affirmé. ⌟

Voici la seconde affirmation, qui nous permettra de construire y_1^*.

Affirmation 2. Pour tout $2 \leq i \leq m$, on a $b_1 \mid b_i$ dans $\mathbb{Z}$.

⌜ Comme b_1 non-nul, il existe $q, r \in \mathbb{Z}$ tels que $b_2 = qb_1 + r$ avec $r = 0$ ou $|r| < |b_1|$. Comme l'ensemble $y_1, \dots, y_m$ engendre G, il en va de même pour la famille $y_1' \coloneqq y_1 + qy_2, y_2, \dots, y_m$, et l'on a

$$b_1 y_1' + r y_2 + b_3 y_3 + \cdots + b_m y_m = b_1 y_1 + b_2 y_2 + \cdots + b_m y_m \overset{(**)}{=} 0 \,.$$

Par minimalité de b_1, on ne peut pas avoir $|r| < |b_1|$, d'où $b_1 \mid b_2$. On procède de même pour $b_3, \dots, b_m$. ⌟

Par cette affirmation, on peut écrire $b_i = q_i b_1$ avec $q_i \in \mathbb{Z}$ pour tout $i = 2, \dots, m$. Considérons le sous-groupe $H_1 \subset G$ engendré par

$$y_1^* \coloneqq y_1 + q_2 y_2 + \cdots + q_m y_m \,,$$

et le sous-groupe $H_2 \subset G$ engendré par $y_2, \dots, y_m$.

Affirmation 3. On a $H_1 + H_2 = G$ et $H_1 \cap H_2 = \{0\}$.

⌜ Comme $y_1, \dots, y_m$ engendrent G, la définition de y_1^* implique qu'il en va de même pour $y_1^*, y_2, \dots, y_m$. Cela montre que $H_1 + H_2 = G$.

Soit $x \in H_1 \cap H_2$. Il existe donc $a_1, \dots, a_m \in \mathbb{Z}$ tels que $x = a_1 y_1^* = a_2 y_2 + \cdots + a_m y_m$. Cela implique

$$0 = x - x = a_1 y_1^* - a_2 y_2 - \cdots - a_m y_m = a_1 y_1 + (a_1 q_2 - a_2) y_2 + \cdots + (a_1 q_m - a_m) y_m \,.$$

Par l'affirmation 1, on a $a_1 = qb_1$ pour un certain $q \in \mathbb{Z}$, d'où

$$x = a_1 y_1^* = q b_1 y_1^* = q(b_1 y_1 + b_1 q_2 y_2 + \cdots + b_1 q_m y_m) = q(b_1 y_1 + \cdots + b_m y_m) \overset{(**)}{=} q \cdot 0 = 0 \,.$$

Cela conclut la preuve de l'affirmation. ⌟

Comme on l'a vu en Remarque II.71, cette troisième affirmation est équivalente au fait que G est produit direct interne de H_1 et de H_2. Par définition, le sous-groupe H_1 est cyclique ; le rang de H_2 étant au plus $m - 1$, nous savons par hypothèse de récurrence que H_2 est produit direct interne d'un nombre fini de sous-modules cycliques. Il en va donc de même pour G, ce qui conclut la preuve. □

Nous sommes maintenant en mesure de démontrer le théorème de classification des groupes abéliens finis.

Démonstration du Théorème II.67. Soit G un groupe abélien fini. Par la Proposition II.74, il est le produit direct interne de sous-groupes cycliques $H_1, \dots, H_m < G$. Par la classification des groupes cycliques, il existe des entiers $a_1, \dots, a_m \geq 0$ tels que $H_i \simeq \mathbb{Z}/a_i\mathbb{Z}$ pour tout $i = 1, \dots, m$. Par le Lemme II.72, on a donc un isomorphisme

$$G \simeq H_1 \times \cdots \times H_m \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_m\mathbb{Z}\,.$$

Analysons à présent ces différents facteurs, tous de la forme $\mathbb{Z}/a\mathbb{Z}$ pour $a \geq 0$.

- Si $a = 0$, alors $\mathbb{Z}/a\mathbb{Z} \simeq \mathbb{Z}$: c'est impossible puisque G est fini.
- Si $a = 1$, alors $\mathbb{Z}/a\mathbb{Z} = \{0\}$: ce facteur ne contribue pas au produit.
- Si $a \geq 2$, alors par le théorème fondamental de l'arithmétique, il existe des premiers distincts $p_1, \dots, p_\ell$ et des entiers $\mu_1, \dots, \mu_\ell$ tels que $a = p_1^{\mu_1} \cdots p_\ell^{\mu_\ell}$. Comme les premiers $p_1, \dots, p_\ell$ sont distincts, les entiers $p_1^{\mu_1}, \dots, p_\ell^{\mu_\ell}$ sont deux à deux premiers entre eux. Par le théorème des restes chinois, on a un isomorphisme

$$\mathbb{Z}/a\mathbb{Z} = \mathbb{Z}/p_1^{\mu_1} \cdots p_\ell^{\mu_\ell}\mathbb{Z} \simeq \mathbb{Z}/p_1^{\mu_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell^{\mu_\ell}\mathbb{Z}\,.$$

En mettant ensemble ces facteurs pour chacun des $\mathbb{Z}/a_i\mathbb{Z}$, on obtient la décomposition annoncée :

$$G \simeq \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{\nu_n}\mathbb{Z}\,.$$

Il reste à démontrer l'unicité de cette décomposition, ce que nous ne ferons pas en tout détail ici. En supposant qu'on ait un isomorphisme

$$\mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{\nu_n}\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/q_1^{\lambda_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k^{\lambda_k}\mathbb{Z}\,,$$

il s'agit donc de vérifier que les suites $p_1^{\nu_1}, \dots, p_n^{\nu_n}$ et $q_1^{\lambda_1}, \dots, q_k^{\lambda_k}$ coïncident à l'ordre près. Pour tout premier p et groupe abélien G, considérons le sous-groupe

$$G_p := \{x \in G \mid p^\nu x = 0 \text{ pour un } \nu \geq 0\} < G\,.$$

Pour tout premier p, l'isomorphisme $\varphi : G \to G'$ ci-dessus se restreint à un isomorphisme $\varphi_p : G_p \to G'_p$, avec G_p le produit des $\mathbb{Z}/p_i^{\nu_i}\mathbb{Z}$ avec $p_i = p$, et G'_p le produit des $\mathbb{Z}/q_j^{\lambda_j}\mathbb{Z}$ avec $q_j = p$. Il reste donc à montrer que si

$$G_p \simeq \mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_\ell}\mathbb{Z}$$

avec p premier, alors la suite d'entiers $n_1, \dots, n_\ell$ est déterminée par G_p à permutations près. Cela peut se faire en considérant les ordres $|p^i G_p / p^{i+1} G_p| = p^{d_i}$: les entiers d_i sont déterminés par G_p et permettent de reconstruire la suite $n_1, \dots, n_\ell$ à permutations près. Les détails seront vus en exercice. □

De manière étonnante, cette preuve relève plus de l'algèbre linéaire que de la théorie des groupes. Cette observation est confirmée de manière formelle dans la sous-section suivante.

II.5.3 Introduction aux modules

Comme nous allons le voir, le Théorème II.67 peut être vu comme un cas très particulier d'un résultat beaucoup plus général : la classification des modules de génération finie sur un anneau euclidien (ou même principal). Dans cette sous-section, nous allons expliquer les termes dans ce théorème, l'énoncer, donner une idée de la démonstration, et en tirer quelques conséquences. Le but principal est d'illustrer par ce résultat le pouvoir unificateur de l'algèbre formel.

Définition II.75

Soit A un anneau, et soit M un ensemble muni d'une loi de composition interne

$$M \times M \longrightarrow M, \quad (x, y) \longmapsto x + y$$

et d'une loi de composition externe

$$A \times M \longrightarrow M, \quad (a, x) \longmapsto a \cdot x\,.$$

On dit que M est **module sur** A (ou A**-module**) s'il satisfait les axiomes suivants :

$(M1)$ $(M, +)$ est un groupe abélien,

$(M2)$ $a \cdot (b \cdot x) = (ab) \cdot x$,

$(M3)$ $(a + b) \cdot x = a \cdot x + b \cdot x$,

$(M4)$ $a \cdot (x + y) = a \cdot x + a \cdot y$,

$(M5)$ $1_A \cdot x = x$,

pour tous $a, b \in A$ et $x, y \in M$.

Exemples II.76 (modules)**.**

1. Pour A un corps K, par définition, les A-modules coïncident avec les K-espaces vectoriels.
2. Pour A l'anneau des entiers $\mathbb{Z}$, les $\mathbb{Z}$-modules coïncident avec les groupes abéliens. [17]

   ⌜ Par l'axiome $(M1)$, tout $\mathbb{Z}$-module est un groupe abélien. Réciproquement, tout groupe abélien $(G, +)$ admet la loi de composition interne donnée par l'addition, mais aussi la loi de composition externe $\mathbb{Z} \times G \to G$ donnée par $(n, g) \mapsto n \cdot g$, la $n^{\text{ième}}$ puissance de g en notation additive. De plus, les égalités

   $$m \cdot (n \cdot g) = (mn) \cdot g \qquad (n + m) \cdot g = n \cdot g + m \cdot g \qquad n \cdot (g + h) = n \cdot g + n \cdot h$$

   sont satisfaites [18] pour tous $n, m \in \mathbb{Z}$ et $g, h \in G$, ce qui correspond aux axiomes $(M2)$, $(M3)$ et $(M4)$. L'axiome $(M5)$ est également satisfait, puisque $1 \cdot g = g$. ⌟

17. Le sens précis de cette affirmation est à trouver dans sa preuve ci-dessous.
18. En notation multiplicative, elles s'écrivent $(g^n)^m = g^{nm}$, $g^{n+m} = g^n g^m$ et $(gh)^n = g^n h^n$.

Ainsi, les modules généralisent à la fois les espaces vectoriels et les groupes abéliens, et les groupes abéliens peuvent s'étudier à l'aide de "l'algèbre linéaire sur $\mathbb{Z}$".

3. Soit E un K-espace vectoriel muni d'un *endomorphisme* $f \in \mathrm{End}(E)$, i.e. d'une application linéaire $f\colon E \to E$. On vérifiera en exercices que cela définit une structure de $K[X]$-module sur E via la loi externe $K[X]\times E \to E, (P, v) \mapsto P\cdot v$ donnée par

$$\Big(\sum_{i\geq 0} \lambda_i X^i\Big)\cdot v = \sum_{i\geq 0} \lambda_i f^i(v)\,, \quad \text{où } f^0 = \mathrm{id} \text{ et } f^i = \overbrace{f\circ\cdots\circ f}^{i} \in \mathrm{End}(E)\,.$$

Cette structure dépendant de f, on notera E_f le $K[X]$-module correspondant.
Réciproquement, un $K[X]$-module M est un K-espace vectoriel, et on vérifie que l'application $f\colon M \to M$ donnée par $f(x) = X\cdot x$ est un endomorphisme linéaire de M. C'est un autre exercice.
En conclusion : les $K[X]$-modules coïncident avec les K-espaces vectoriels munis d'un endomorphisme, dans le sens précis explicité ci-dessus.

4. Si $M_1, \ldots, M_n$ sont des A-modules, alors $M\times\cdots\times M_n$ est un A-module pour les lois

$$(x_1,\ldots,x_n) + (y_1,\ldots,y_n) = (x_1+y_1,\ldots,x_n+y_n)$$
$$a\cdot(x_1,\ldots,x_n) = (a\cdot x_1,\ldots,a\cdot x_n)\,.$$

Il est noté $M_1\oplus\cdots\oplus M_n$, et appelé *la somme directe (externe)* de $M_1,\ldots,M_n$.
Si $M_1 = \cdots = M_n = M$, on le note simplement M^n.
Notons que dans le cas de $\mathbb{Z}$-module, on retrouve la construction du produit direct de groupes abéliens.

Bien évidemment, les A-modules sont les objets d'une catégorie. En voici les morphismes (et les isomorphismes).

Définition II.77

Soient M, M' deux modules sur un anneau A. Une application $\varphi\colon M \to M'$ dite **A-linéaire** si elle satisfait

$$\varphi(x+y) = \varphi(x) + \varphi(y) \quad \text{et} \quad \varphi(a\cdot x) = a\cdot\varphi(x)$$

pour tous $x, y \in M$ et $a \in A$. C'est un **isomorphisme A-linéaire** s'il existe $\psi\colon M' \to M$ A-linéaire avec $\psi\circ\varphi = \mathrm{id}_M$ et $\varphi\circ\psi = \mathrm{id}_{M'}$.

Exemples II.78 (applications A-linéaires)**.**

1. Si $A = K$ est un corps, alors on retombe sur la notion d'application (et d'isomorphisme) K-linéaire.

2. Les applications $\mathbb{Z}$-linéaires coïncident avec les homomorphismes de groupes abéliens.

   ⌜ Par la première condition, une application $\mathbb{Z}$-linéaire est un homomorphisme de groupes. Réciproquement, on sait [19] qu'un homomorphisme de groupes $\varphi: G \to G'$ satisfait $\varphi(n \cdot g) = n \cdot \varphi(g)$ pour tous $n \in \mathbb{Z}$ et $g \in G$. ⌟

3. Considérons le cas $A = K[X]$. Soient E, E' deux K-espaces vectoriels munis d'endomorphismes $f \in \mathrm{End}(E), f' \in \mathrm{End}(E')$. On peut vérifier qu'une application $\varphi: E_f \to E'_{f'}$ entre les $K[X]$-modules correspondants est $K[X]$-linéaire si et seulement si $\varphi: E \to E'$ est K-linéaire et satisfait $\varphi \circ f = f' \circ \varphi$. C'est un exercice.

   En posant $E' = E$, on obtient que deux $K[X]$-modules E_f et $E_{f'}$ sont isomorphes si et seulement s'il existe un isomorphisme K-linéaire $\varphi: E \to E$ tel que $\varphi \circ f = f' \circ \varphi$, i.e. si et seulement si les endomorphismes $f, f' \in \mathrm{End}(E)$ sont conjugués par un automorphisme K-linéaire de E.

Remarques II.79.

1. Comme énoncé ci-dessus, on vérifie facilement que pour tout anneau A fixé, les A-modules et les applications A-linéaires forment une catégorie. Elle est habituellement notée A-Mod.
2. Par les Exemples II.76.1 et II.78.1, la catégorie K-Mod coïncide avec K-Vect pour tout corps K. De même, par les Exemples II.76.2 et II.78.2, la catégorie $\mathbb{Z}$-Mod coïncide avec Ab.
3. On vérifie facilement que le produit et le coproduit dans la catégorie A-Mod sont donnés par la somme directe définie en Exemple II.76.4. Cela généralise les cas de K-Vect et de Ab déjà vus en Exemples I.19.3 et I.19.4, et en Exemples I.21.3 et I.21.4.

Un dernier concept est nécessaire pour énoncer le théorème de classification.

Terminologie II.80. Un A-module M est dit *de génération finie (sur A)* s'il existe des éléments $x_1, \ldots, x_n \in M$ tels que tout $x \in M$ s'écrit $x = a_1 x_1 + \cdots + a_n x_n$ avec $a_1, \ldots, a_n \in A$.

Exemples II.81 (modules de génération finie)**.**

1. Par définition, un K-module est de génération finie si et seulement si c'est un K-espace vectoriel de dimension finie.
2. Trivialement, un groupe abélien fini est un $\mathbb{Z}$-module de génération finie (par exemple, engendré par tous ses éléments).
3. Clairement, si E est un K-espace vectoriel de dimension finie muni d'un endomorphisme f, alors le $K[X]$-module associé E_f est de génération finie.

Nous pouvons finalement énoncer le résultat principal de cette sous-section : la classification des modules de génération finie sur un anneau principal.

19. En notation multiplicative, c'est l'identité bien connue $\varphi(g^n) = \varphi(g)^n$.

Théorème II.82

Soit M un module de génération finie sur A un anneau principal. Alors, il existe des entiers $r, n \geq 0$, une suite de premiers $p_1, \ldots, p_n \in A$ (pas forcément distincts) et des entiers $\nu_1, \ldots, \nu_n \geq 1$, tels que

$$M \simeq A^r \oplus A/(p_1^{\nu_1}) \oplus \cdots \oplus A/(p_n^{\nu_n}) .$$

De plus, l'entier r est uniquement déterminé par M, de même que les paires $(p_1, \nu_1), \ldots, (p_n, \nu_n)$ à l'ordre près.

La preuve de ce résultat n'est pas hors de portée, mais nécessiterait un investissement en temps qui n'est pas justifié dans le cadre de ce cours.

Notons néanmoins qu'une preuve pour le cas des anneaux euclidiens n'est pas plus difficile que celle pour $A = \mathbb{Z}$ donnée en Sous-section II.5.2, du moins en ce qui concerne l'énoncé de décomposition [20]. Et comme tous les exemples d'applications ci-dessous sont avec des anneaux euclidiens, ce cas particulier suffira à notre bonheur. Voici les grandes lignes de cette démonstration :

- La preuve de la Proposition II.74 s'étend *verbatim* du cas $A = \mathbb{Z}$ au cas de A euclidien [21] : il suffit de remplacer la valeur absolue par l'application $A \setminus \{0\} \to \mathbb{N}$ qui fait de A un anneau euclidien. On obtient donc un énoncé de décomposition de tout A-module de génération finie M en somme directe interne (la généralisation évidente de la Terminologie II.70) de sous-modules cycliques (i.e. engendrés par un élément).
- Par la généralisation immédiate du Lemme II.72, M est isomorphe à une somme directe externe de modules cycliques.
- Un module cyclique sur un anneau A est toujours de la forme A/I pour un certain idéal $I \subset A$; si A est principal, tout module cyclique est donc de la forme $A/(a)$ pour un $a \in A$. Cela généralise la classification des groupes (abéliens) cycliques. Ainsi, le A-module M est isomorphe à une somme directe de modules de la forme $A/(a)$. Les facteurs avec $a \in A^*$ ne contribuent pas, ceux avec $a = 0$ contribuent à A^r.
- Comme un anneau principal est factoriel, tout $a \in A \setminus (A^* \cup \{0\})$ se décompose en produit de puissances d'éléments premiers. Il ne reste plus qu'à observer que le théorème chinois est valable pour tout anneau (principal), ce qui permet d'obtenir la décomposition annoncée.

Il est très instructif d'explorer quelques exemples de résultats obtenus comme corollaires de cet unique théorème.

1. $A = K$ un corps

Commençons avec le cas de $A = K$ un corps. C'est bien un anneau principal (en fait, euclidien). De plus, un K-module de génération finie n'est autre qu'un K-

20. Celui d'unicité requière un peu plus de travail dans le cas général que dans le cas $A = \mathbb{Z}$, même si les idées sont les mêmes.

21. Elle a même été rédigée dans cet esprit.

espace vectoriel de dimension finie (Exemple II.81.1). Finalement, comme on le sait, il n'y a pas d'éléments premiers dans un corps. On obtient donc l'énoncé suivant.

Théorème II.83

Si E un espace vectoriel de dimension finie sur un corps K, il existe un unique entier $r \geq 0$ tel que $E \simeq K^r$.

Vous aurez reconnu le théorème de classification des espaces vectoriels de dimension finie. Cet unique entier r associé à E n'est autre que sa dimension.

2. $A = \mathbb{Z}$

Soit G un groupe abélien fini. Par l'Exemple II.81.2, c'est un $\mathbb{Z}$-module de génération finie. Comme $\mathbb{Z}$ est un anneau principal (en fait, euclidien), on peut appliquer le Théorème II.82, d'où une décomposition de la forme

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}/(p_1^{\nu_1}) \oplus \cdots \oplus \mathbb{Z}/(p_n^{\nu_n}) .$$

Mais comme G est fini, on a forcément $r = 0$. Finalement, comme observé en Exemple II.76.4, la somme directe des $\mathbb{Z}$-modules correspond au produit direct des groupes abéliens. On obtient donc le théorème de classification des groupes abéliens finis (Théorème II.67).

Notons qu'on obtient en fait un énoncé plus général : la classification des groupes abéliens de génération finie, où l'entier $r \geq 0$ n'est pas forcément nul.

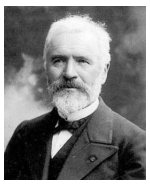
3. $A = \mathbb{C}[X]$

Comme troisième et dernier exemple, considérons le cas $A = \mathbb{C}[X]$. Comme on l'a vu en Exemple II.81.3, un $\mathbb{C}$-espace vectoriel E de dimension finie muni d'un endomorphisme $f \in \mathrm{End}(E)$ définit un $\mathbb{C}[X]$-module E_f de génération finie. Comme l'anneau $\mathbb{C}[X]$ est principal (en fait, euclidien), nous pouvons appliquer le Théorème II.82. Notons que comme $\mathbb{C}$ est algébriquement clos, les éléments premiers de $\mathbb{C}[X]$ sont de la forme $p_i = (X - \lambda_i)$ pour un certain $\lambda_i \in \mathbb{C}$. Ainsi, il existe des entiers $r, n \geq 0$, une suite de nombres complexes $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ (pas nécessairement distincts) et des entiers $\nu_1, \ldots, \nu_n \geq 1$ avec un isomorphisme de $\mathbb{C}[X]$-modules

$$E_f \simeq \mathbb{C}[X]^r \oplus \mathbb{C}[X]/((X - \lambda_1)^{\nu_1}) \oplus \cdots \oplus \mathbb{C}[X]/((X - \lambda_n)^{\nu_n}) .$$

Comme E est dimension finie sur $\mathbb{C}$, on a forcément $r = 0$.

Par l'Exemple II.78.3, cet énoncé se traduit en une classification des endomorphismes de E à conjuguaison près. Sans entrer dans les détails, l'énoncé en question n'est autre que le théorème de la forme normale de JORDAN pour les endomorphismes complexes.



CAMILLE JORDAN (1838-1922)

Théorème II.84: Forme normale de Jordan

Soit E un espace vectoriel de dimension finie sur $\mathbb{C}$, et soit $f \in \mathrm{End}(E)$. Alors, il existe une base de E dans laquelle la matrice de f est donnée par

$$J_{\nu_1}(\lambda_1) \oplus \cdots \oplus J_{\nu_n}(\lambda_n)$$

pour certains nombres complexes $\lambda_1, \ldots, \lambda_n$ pas forcément distincts, et certains entiers $\nu_1, \ldots, \nu_n \geq 1$, où

$$J_\nu(\lambda) = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \lambda & 1 \\ & & & \lambda \end{pmatrix}.$$

De plus, la suite de paires $(\nu_1, \lambda_1), \ldots, (\nu_n, \lambda_n)$ est unique à l'ordre près.

II.6 Groupes finis

Le but de cette dernière section sur les groupes est de présenter quelques unes des techniques disponibles pour tenter de classifier les groupes finis à isomorphisme près. Sans surprise, abandonner l'hypothèse de commutativité complique considérablement la donne. Néanmoins, certains outils existent.

Nous commencerons en Sous-section II.6.1 par rappeler le résultat fondamental appelé *équation des classes*, qui sera ensuite appliqué au p-groupes en Sous-section II.6.2. La Sous-section II.6.3 traitera des fameux *théorèmes de Sylow*, dont on verra quelques applications classiques en Sous-section II.6.4.

II.6.1 Équation des classes

Ce résultat a déjà été vu en Algèbre I, mais comme il est relativement technique et sera utilisé à de multiples reprises par la suite, nous avons choisi d'en faire un rappel ici.

Soit $G \curvearrowright X$ une action d'un groupe G sur un ensemble X. On notera

$$X^G := \{x \in X \mid g \cdot x = x \text{ pour tout } g \in G\}$$

l'ensemble des points fixes de cette action. Rappelons qu'un sous-ensemble $S \subset X$ est un *ensemble de représentants des orbites* si S contient exactement un élément de chaque orbite de cette action.

Proposition II.85. *Pour toute action d'un groupe G fini sur un ensemble X fini et tout ensemble de représentants des orbites $S \subset X$, on a :*

$$|X| = |X^G| + \sum_{x \in S \setminus X^G} [G : \mathrm{Stab}(x)], \tag{II.17}$$

avec $2 \leq [G : \mathrm{Stab}(x)]$ un diviseur de $|G|$ pour tout $x \in S \setminus X^G$.

Démonstration. Comme l'ensemble X se partitionne en les orbites, la formule des orbites (Théorème II.10) le théorème de Lagrange (Théorème II.1) impliquent

$$|X| = \sum_{x\in S} |G\cdot x| = \sum_{x\in S} [G:\mathrm{Stab}(x)] = \sum_{x\in X^G} \overbrace{[G:\mathrm{Stab}(x)]}^{=1} + \sum_{x\in S\smallsetminus X^G} \overbrace{[G:\mathrm{Stab}(x)]}^{\geq 2}.$$

Notons que $x \in X$ satisfait $[G:\mathrm{Stab}(x)] = 1$ si et seulement si $\mathrm{Stab}(x) = G$, ce qui est équivalent à $x \in X^G$, comme indiqué par les accolades ci-dessus. L'énoncé en découle via une dernière application de Lagrange. □

L'idée principale de cette sous-section est d'appliquer (II.17) à l'action d'un groupe fini G sur lui-même par conjugaison, à savoir :

$$G\times G \longrightarrow G\,, \qquad (g,x)\longmapsto g\cdot x = gxg^{-1}\,.$$

On vérifie facilement qu'il s'agit bien d'une action, ce qui justifie un peu de terminologie.

- L'orbite de $x \in G$ est

$$G\cdot x = \{g\cdot x \mid g\in G\} = \{gxg^{-1} \mid g\in G\}\,,$$

  qu'on appelle la *classe de conjugaison* de $x \in G$.
- Le stabilisateur de $x \in G$ est

$$\mathrm{Stab}(x) = \{g\in G \mid g\cdot x = x\} = \{g\in G \mid gxg^{-1} = x\} = \{g\in G \mid gx = xg\} =: Z_G(x)$$

  qu'on appelle le *centralisateur* de $x \in G$.
- L'ensemble des points fixes est

$$X^G = \{x\in X \mid g\cdot x = x \ \ \forall g\in G\} = \{x\in X \mid gx = xg \ \ \forall g\in G\} =: Z(G)\,,$$

  appelé le *centre* de G.

On obtient donc immédiatement le corollaire suivant, appelé *équation des classes*.

Corollaire II.86. *Pour tout groupe fini G et tout ensemble de représentants S des classes de conjugaison, on a*

$$|G| = |Z(G)| + \sum_{x\in S\smallsetminus Z(G)} [G:Z_G(x)]\,, \tag{II.18}$$

avec $2 \leq [G:Z_G(x)]$ un diviseur de $|G|$ pour tout $x \in S\smallsetminus Z(G)$. □

Les remarques suivantes nous seront utiles par la suite : les preuves sont élémentaires et seront discutées en exercice.

Remarques II.87.

1. L'entier $[G:Z_G(x)]$ est le cardinal de la classe de conjugaison de x.

2. Tout sous-groupe de $Z(G)$ est normal dans G.
3. Si G admet un sous-groupe $H < Z(G)$ tel que G/H est cyclique, alors G est commutatif.

Voici quelques premiers exemples faciles. D'autres suivront plus tard, et en exercices.

Exemples II.88.

1. Si le groupe G est abélien, alors $Z(G) = G$ et l'équation des classes est trivialement satisfaite via $|G| = |Z(G)|$.
2. Soit G est un groupe non-abélien d'ordre 6. Si son centre $Z(G)$ est non-trivial, alors par Lagrange, l'ordre du quotient $G/Z(G)$ est 1,2 ou 3. Mais tout groupe d'ordre ≤ 3 est cyclique, ce qui implique que G est abélien par la Remarque II.87.3. Ainsi, si G est non-abélien d'ordre 6, son centre est trivial. L'équation des classes prend donc la forme $6 = 1 + \sum_{x \in S \smallsetminus \{e\}} [G : Z_G(x)]$, avec $2 \leq [G : Z_G(x)]$ un diviseur de 6 pour tout $x \in S \smallsetminus \{x\}$. La seule solution possible est $6 = 1 + 2 + 3$.

   En conclusion : si G est un groupe non-abélien d'ordre 6, alors son centre est trivial, et il a trois classes de conjugaison de taille 1, 2, et 3.

   En fait, on montrera en exercice qu'un tel groupe est nécessairement isomorphe au groupe symétrique S_3, dans lequel les classes de conjugaison correspondantes sont $\{\mathrm{id}\}$, $\{(1,2,3),(1,3,2)\}$, et $\{(1,2),(1,3),(2,3)\}$.

II.6.2 Applications aux p-groupes

Nous allons à présent rappeler deux applications vues en ALGÈBRE I, et en présenter deux nouvelles.

Terminologie II.89. Soit p un nombre premier. Un groupe G est appelé un *p-groupe* s'il existe un entier $k \geq 0$ tel que $|G| = p^k$.

Commençons pas appliquer la Proposition II.85 aux p-groupes.

Lemme II.90. *Si un p-groupe G agit sur un ensemble fini X, alors*

$$|X^G| \equiv |X| \pmod{p}.$$

Démonstration. Soit donc G un groupe d'ordre $|G| = p^k$ avec p premier et $k \geq 0$. Comme X est fini, la Proposition II.85 donne

$$|X| = |X^G| + \sum_{x \in S \smallsetminus X^G} [G : \mathrm{Stab}(x)],$$

avec $2 \leq [G : \mathrm{Stab}(x)]$ un diviseur de $|G| = p^k$ pour tout $x \in S \smallsetminus X^G$. Ainsi, p divise $[G : \mathrm{Stab}(x)]$ pour tout $x \in S \smallsetminus X^G$, d'où $|X| \equiv |X^G| \pmod{p}$. □

A. Centre des p-groupes

Voici la première application. Comme on le verra, ce résultat nous sera très utile par la suite, en particulier pour démontrer des énoncés par récurrence sur l'ordre d'un p-groupe.

Théorème II.91

Si G est un p-groupe non-trivial, alors $Z(G)$ est non-trivial.

Démonstration. En appliquant le Lemme II.90 à l'action par conjugaison de G sur lui-même, on obtient

$$|Z(G)| \equiv |G| \equiv 0 \pmod{p},$$

où l'on a utilisé le fait que G est un p-groupe non-trivial dans la dernière congruence. Mais comme $Z(G)$ est non-vide, on a nécessairement $|Z(G)| > 1$. □

B. Théorème de Cauchy

Augustin-Louis Cauchy (1789-1857)

Voici la seconde application, une réciproque partielle au théorème de Lagrange. Ce résultat est traditionnellement attribué à Cauchy (1845), mais la preuve que nous proposons, exceptionnellement ingénieuse, est bien plus récente [22].

Théorème II.92: Théorème de Cauchy

Si G est un groupe fini, alors pour tout premier p qui divise $|G|$, il existe un élément $g \in G$ d'ordre p.

Démonstration. Soient donc G un groupe fini et p un premier qui divise $|G|$. L'idée est de considérer l'action du p-groupe $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble

$$X := \{(x_1, \dots, x_p) \in G \times \cdots \times G \mid x_1 \cdots x_p = e\}$$

par permutations cycliques des coordonnées. En d'autres termes, il s'agit de l'action déterminée par $[1] \cdot (x_1, x_2, \dots, x_p) = (x_2, \dots, x_p, x_1)$. Notons que l'égalité $x_1 x_2 \cdots x_p = e$ est équivalente à $x_2 \cdots x_p x_1 = e$, donc cette action est bien définie. Notons également que le cardinal de X est donné par $|X| = |G|^{p-1}$, puisque pour tous $x_1, \dots, x_{p-1} \in G$, il existe un unique $x_p \in G$ tel que $x_1 \cdots x_{p-1} x_p = e$ (donné par $x_p = x_{p-1}^{-1} \cdots x_1^{-1}$). Le Lemme II.90 donne donc

$$|X^{\mathbb{Z}/p\mathbb{Z}}| \equiv |X| = |G|^{p-1} \equiv 0 \pmod{p},$$

22. Due à James H. McKay, elle date de 1959.

où dans la dernière congruence, on a utilisé que p divise $|G|$ et que $p-1>0$. Mais cet ensemble de points fixes n'est autre que

$$\begin{aligned} X^{\mathbb{Z}/p\mathbb{Z}} &= \{(x_1,\dots,x_p)\in G\times\cdots\times G \mid x_1\cdots x_p = e,\ x_1=\cdots=x_p\} \\ &= \{(x,\dots,x)\in G\times\cdots\times G \mid x^p = e\}, \end{aligned}$$

en bijection avec l'ensemble $Y := \{x\in G \mid x^p = e\}$. En conclusion, cet ensemble Y a cardinal un multiple de p. Comme Y contient le neutre, ce multiple est positif. Ainsi, il existe $x\in G\setminus\{e\}$ tel que $x^p = e$. Comme p est premier, cela implique que x est d'ordre p. □

C. Les p-groupes sont résolubles

Voici la troisième application, dont le titre contient déjà toute la substance.

Théorème II.93

Les p-groupes sont résolubles.

Démonstration. Soit donc G un p-groupe. Par définition, il existe un entier $k\geq 0$ tel que $|G| = p^k$. Nous allons procéder par récurrence sur $k\geq 0$. Le départ de la récurrence est évident puisque le seul groupe d'ordre $p^0 = 1$ est le groupe trivial, qui est résoluble. Fixons à présent G d'ordre p^k avec $k\geq 1$, et supposons que tous les p-groupes d'ordre $< p^k$ sont résolubles. Puisque $k\geq 1$, le groupe G est d'ordre $p^k > 1$ et donc non-trivial. Par le Théorème II.91, son centre $Z(G)\triangleleft G$ est non-trivial. Le quotient $G/Z(G)$ est un p-groupe puisque son ordre divise p^k, mais d'ordre $< p^k$ puisque $Z(G)$ est non-trivial. Par hypothèse de récurrence, le groupe quotient $G/Z(G)$ est résoluble. Mais $Z(G)$ est également résoluble puisqu'il s'agit d'un groupe abélien. Par la Proposition II.22, on conclut que le groupe G est lui-même résoluble. □

D. Groupes d'ordre p^2

Voici la quatrième et dernière application de cette sous-section.

Théorème II.94: Classification des groupes d'ordre p^2

Si G est un groupe d'ordre p^2 avec p premier, alors G est isomorphe à exactement un des deux groupes $\mathbb{Z}/p^2\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$.

Démonstration. Soit donc G un groupe d'ordre p^2 avec p premier. Nous allons tout d'abord vérifier que G est nécessairement abélien. Par le Théorème II.91, le centre de G est non-trivial. Ainsi, le quotient $G/Z(G)$ est soit d'ordre 1 (auquel cas G est abélien), soit d'ordre p. Dans ce dernier cas, le quotient $G/Z(G)$ serait cyclique, ce qui impliquerait à nouveau G abélien par la Remarque II.87.3.

Il est à présent possible de conclure en invoquant la classification des groupes abéliens finis (Théorème II.67) appliquée aux groupes d'ordre p^2. Mais comme la preuve de ce cas particulier est tout à fait élémentaire, autant la donner en détails plutôt que d'utiliser "un canon pour tuer une mouche".

Par Lagrange, tous les éléments de G sont soit d'ordre 1 (le neutre e), soit d'ordre p, soit d'ordre p^2. S'il existe $g \in G$ d'ordre p^2, alors on a $G \simeq \langle g \rangle \simeq \mathbb{Z}/p^2\mathbb{Z}$ par la classification des groupes cycliques. Supposons donc que tout $g \in G \setminus \{e\}$ est d'ordre p : on est en présence d'un groupe abélien dont tous les éléments sont d'ordre $\leq p$. On vérifiera en exercices qu'un tel groupe abélien est muni d'une structure d'espace vectoriel sur le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Comme G est d'ordre p^2, cet espace vectoriel est de dimension 2, d'où un isomorphisme d'espaces vectoriels $G \simeq \mathbb{F}_p^2$. En particulier, on a bien un isomorphisme de groupes $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Reste à noter que les deux groupes $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ne sont pas isomorphes, puisque le premier est cyclique mais pas le deuxième. □

II.6.3 Théorèmes de Sylow

Ludvig Sylow (1832-1918)

Après avoir utilisé autant que possible l'équation des classes, il est temps d'introduire de nouveaux outils : les fameux théorèmes de Sylow, découverts par Ludvig Sylow en 1872.

Rappelons que par Lagrange, si H est un sous-groupe d'un groupe G fini, alors l'ordre de H divise celui de G. Il est donc naturel de se poser la question de la réciproque : est-il vrai que pour tout diviseur d de $|G|$, il existe un sous-groupe $H < G$ d'ordre $|H| = d$?

Il n'est pas très difficile de montrer que cela est vrai dans le cas abélien : c'est une conséquence presque immédiate de la classification des groupes abéliens finis (Théorème II.67), mais cela peut également se montrer directement. En revanche, la réponse est négative en général. Par exemple[23], le groupe $G = A_5$, qui est d'ordre 60, n'admet pas de sous-groupe d'ordre $d = 30$; en effet, un tel sous-groupe serait d'ordre 2 et donc normal, ce qui est impossible puisque A_5 est un groupe simple (Théorème II.8).

Peut-on néanmoins dire quelque chose en général, pour certaines classes de diviseurs de $|G|$? En fait, on peut dire beaucoup, et c'est l'objet de cette sous-section.

Terminologie II.95. Soient p un premier et G un groupe fini.

- Un *p-sous-groupe* de G est un sous-groupe de G qui est un p-groupe.
- Un *p-sous-groupe de Sylow* (ou *p-Sylow*) de G est un p-sous-groupe $P < G$ tel que p ne divise pas $[G : P]$.

En des termes moins élégants mais plus parlants, un p-Sylow de G est un sous-groupe $P < G$ tel que $|P| = p^r$ avec $|G| = p^r m$ et $\text{pgcd}(p, m) = 1$.

Voici le premier des trois théorèmes de Sylow.

23. Un exemple plus petit est le groupe A_4, d'ordre 12, qui n'admet pas de sous-groupe d'ordre 6 ; mais la preuve est moins directe. En fait, c'est un exemple de taille minimale, par la Proposition II.97.

Théorème II.96: Premier théorème de Sylow

Tout groupe fini contient un p-sous-groupe de Sylow pour tout premier p.

Notons que si p ne divise pas l'ordre du groupe G, alors un p-sous-groupe de Sylow de G n'est autre qu'un sous-groupe d'ordre $p^0 = 1$, donc le sous-groupe trivial $P = \{e\}$. Le premier théorème de Sylow reste bien entendu vrai dans ce cas, mais n'est véritablement intéressant que dans les cas des premiers qui divisent l'ordre du groupe.

En fait, ce théorème est un cas particulier de l'énoncé suivant [24].

Proposition II.97. *Si d est un diviseur de $|G|$ de la forme $d = p^k$ avec p premier et $k \geq 0$, alors G admet un sous-groupe d'ordre d.*

Démonstration. Fixons un premier p, et soit $d = p^k$ un diviseur de $|G|$ avec $k \geq 0$. Si $k = 0$, l'énoncé est trivial. On peut donc supposer $k \geq 1$, et l'on souhaite montrer : *si p^k divise $|G|$ avec $k \geq 1$, alors il existe un sous-groupe $P < G$ d'ordre p^k.*

Procédons par induction sur $|G| \geq p$. Si $|G| = p$, alors l'énoncé est trivialement satisfait puisque G admet le sous-groupe $P = G$ d'ordre p. Fixons donc un groupe G d'ordre $|G| > p$ divisible par p^k avec $k \geq 1$, et supposons l'énoncé démontré pour tout groupe d'ordre $< |G|$.

S'il existe un sous-groupe propre $H \subsetneq G$ tel que $p \nmid [G : H]$, alors p^k divise toujours $|H| = \frac{|G|}{[G:H]}$ et on peut appliquer l'hypothèse de récurrence à H : il existe un sous-groupe $P < H \subset G$ d'ordre $|P| = p^k$; comme c'est également un sous-groupe de G, cela conclut ce cas.

Supposons à présent que tout sous-groupe propre $H \subsetneq G$ satisfait $p \mid [G : H]$. Par l'équation des classes (Corollaire II.86), on a

$$|G| = |Z(G)| + \sum_{x \in S \setminus Z(G)} [G : Z_G(x)] .$$

Comme p^k divise $|G|$ avec $k \geq 1$, le premier p divise $|G|$. De plus, comme $Z_G(x) \subsetneq G$ pour tout $x \notin Z(G)$, on a $p \mid [G : Z_G(x)]$ par hypothèse. La conclusion est donc que p divise $|Z(G)|$. Par le Théorème de Cauchy [25], il existe un élément $a \in Z(G)$ d'ordre p. Considérons le sous-groupe $N := \langle a \rangle$ engendré par a, qui est normal dans G puisque $N \subset Z(G)$; on peut donc former le quotient G/N. Comme $|G/N| = \frac{|G|}{p}$ et $p^k \mid |G|$, on a $p^{k-1} \mid |G/N| < |G|$. Par hypothèse de récurrence, le quotient G/N contient un sous-groupe d'ordre p^{k-1}. Par la structure des sous-groupes d'un quotient (voir la première partie du Théorème II.5), ce sous-groupe est de la forme P/N avec $N \subset P < G$. Le sous-groupe $P < G$ étant d'ordre

$$|P| = |P/N| \cdot |N| = p^{k-1} \cdot p = p^k ,$$

cela conclut la preuve. □

24. À ce stade, il est légitime de se demander pourquoi se focaliser sur les p-sous-groupes maximaux, alors que toute puissance de p est réalisée ; la réponse est donnée par les autres théorèmes de Sylow.

25. Ici la version abélienne suffit, qui est plus élémentaire.

Le deuxième théorème de Sylow est relativement technique dans son énoncé, mais le preuve est concise, et les corollaires peut-être plus parlants que le théorème lui-même. Le voici.

Théorème II.98: Deuxième théorème de Sylow

Soient G un groupe fini, $P < G$ un p-sous-groupe de Sylow, et $H < G$ un p-sous-groupe. Alors, il existe $g \in G$ tel que $H \subset gPg^{-1}$.

Démonstration. Soient donc G, P et H comme dans l'énoncé. Considérons l'action du p-groupe H sur l'ensemble $X = G/P$ des classes à gauche modulo P via multiplication : $h \cdot gP = (hg)P$ pour tous $h \in H$ et $g \in G$.

Comme H est un p-groupe, le Lemme II.90 implique $|X| \equiv |X^H| \pmod{p}$. Mais comme P est un p-Sylow, le cardinal $|X| = |G/P| = [G : P]$ est premier à p. Ainsi, le cardinal de X^H n'est pas divisible par p. En particulier, cet ensemble est non-vide : il existe donc une classe à gauche $gP \in X^H$ qui est un point fixe de cette action. En d'autres termes, pour tout $h \in H$, on a $hgP = gP$. Cette égalité implique

$$hgP = gP \Leftrightarrow g^{-1}hgP = P \Rightarrow g^{-1}hg \in P \Leftrightarrow h \in gPg^{-1}$$

pour tout $h \in H$, d'où l'inclusion voulue $H \subset gPg^{-1}$. □

L'énoncé et la preuve sont courts, mais pas évidents à assimiler. En revanche, les conséquences sont immédiates et frappantes.

Corollaire II.99. *Tout p-sous-groupe d'un groupe fini est contenu dans un p-sous-groupe de Sylow.*

Démonstration. Soit H un p-sous-groupe de G. Par le premier théorème de Sylow, il existe un p-Sylow $P < G$. Par le deuxième théorème de Sylow, il existe $g \in G$ tel que $H \subset gPg^{-1}$. Comme gPg^{-1} est un p-Sylow, le corollaire est démontré. □

Corollaire II.100. *Tous les p-sous-groupes de Sylow d'un groupe fini fixé sont conjugués.*

Démonstration. Soient donc P, P' deux p-Sylow d'un groupe fini G. Comme P' est un p-sous-groupe, le deuxième théorème de Sylow nous garantit l'existence de $g \in G$ tels que $P' \subset gPg^{-1}$. Mais comme $|P'| = |P|$, on a égalité $P' = gPg^{-1}$. □

En particulier, on obtient l'énoncé tout à fait remarquable que voici : tous les p-Sylow d'un groupe donné sont isomorphes. Voyons quelques exemples pour illustrer ce théorème.

Exemples II.101.

1. Supposons G abélien. Par le Théorème II.96 et le Corollaire II.100, pour tout premier p, le groupe G admet un unique p-Sylow. Notons que ce résultat découle également du théorème de classification des groupes abéliens finis (Théorème II.67), ce que nous avons vu en exercices.

2. Soit $G = D_{2n} = \langle x, y \mid x^2, y^n, xyx = y^{-1} \rangle$ le groupe diédral d'ordre $2n$ avec $n \geq 3$, et choisissons le premier $p = 2$.
   - Si n est impair, alors un 2-Sylow de G est un sous-groupe d'ordre 2. Ces sous-groupes sont engendrés par les éléments d'ordre 2 de D_{2n}, à savoir les réflexions $y^i x y^{-i}$ avec $0 \leq i \leq n-1$. Il y en a n, et ils sont tous conjugués comme prédit par le Corollaire II.100. Le cas $n = 5$ est illustré en Figure 4.
   - Si n est pair, en revanche, les 2-Sylows ne sont pas des sous-groupes d'ordre 2. Ce derniers sont engendrés par les réflexions, et par la rotation d'un demi-tour $y^{n/2}$. Notons qu'il y a deux classes de conjugaison de réflexions : celles dont l'axe passe par des sommets du n-gone régulier (de la forme $y^i x y^{-i}$ avec $0 \leq i < n/2$), et celles dont l'axe passe par le milieu des côtés (de la forme $y^i(xy)y^{-i} = y^i x y^{1-i}$ avec $0 \leq i < n/2$). Le cas $n = 6$ est illustré en Figure 4, pour lequel il y a donc 7 sous-groupes d'ordre 2, répartis en 3 classes de conjugaison.

     En revanche, les théorèmes de Sylow nous disent par exemple que D_{12} contient des sous-groupes d'ordre 4 qui sont tous conjugués. En fait, on peut vérifier qu'il y a trois tels sous-groupes : $\langle y^i x y^{-i} \rangle \times \langle y^3 \rangle$, qui sont conjugués comme il se doit (et isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

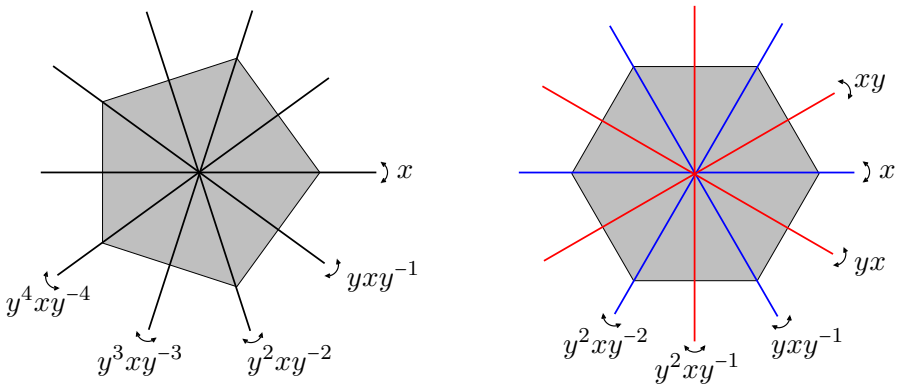


FIGURE 4 – Gauche : les n axes de réflexion du n-gone régulier correspondants aux 2-Sylow de D_{2n}, avec $n = 5$. Droite : les deux classes de conjugaison de réflexions pour $n = 6$, données par deux couleurs distinctes.

Venons-en au troisième et dernier théorème de Sylow.

Théorème II.102: Troisième théorème de Sylow

Soit G un groupe fini d'ordre $|G| = p^r m$ avec p premier et $p \nmid m$. Le nombre n_p de p-sous-groupe de Sylow de G satisfait $n_p \mid m$ et $n_p \equiv 1 \pmod{p}$.

Exemples II.103.

1. Si G est abélien, par l'Exemple II.101.1, on a $n_p = 1$ pour tout premier p. Cet entier satisfait bien $n_p \mid m$ et $n_p \equiv 1 \pmod{p}$ comme il se doit.

2. Si p ne divise pas l'ordre de G, alors le seul p-Sylow de G est le sous-groupe trivial. On a donc à nouveau $n_p = 1$, qui vérifie les conditions voulues.
3. Pour $G = D_{2n}$ avec n impair, on avait $n_2 = n$ par l'Exemple II.101.2. Il satisfait bien $n_2 \mid m = n$ et $n_2 \equiv 1 \pmod 2$.
   Pour $G = D_{12}$, on avait $n_2 = 3$, qui satisfait bien $n_2 \mid m = 3$ et $n_2 \equiv 1 \pmod 2$.
4. Pour $G = S_4$, les cas $p = 2, 3$ donnent des résultats instructifs, qu'on verra en exercice.

Comme le conjugué d'un p-sous-groupe de Sylow est encore un p-sous-groupe de Sylow, ce théorème implique immédiatement le résultat suivant.

Corollaire II.104. *Soit G un groupe fini d'ordre $|G| = p^r m$ avec p premier et $p \nmid m$. Si la seule solution $n_p \geq 1$ de $n_p \mid m$ et $n_p \equiv 1 \pmod p$ est $n_p = 1$, alors G contient un unique p-Sylow, qui est normal dans G.* □

La preuve du Théorème II.102 nécessite un peu de terminologie et quelques résultats préliminaires, qui ont leur intérêt propre.

Terminologie II.105. Soit X un sous-ensemble d'un groupe G. On appelle

$$N_G(X) := \{g \in G \mid gXg^{-1} = X\}$$

le *normalisateur* de X.

Remarques II.106.

1. On vérifie que $N_G(X)$ est un sous-groupe de G.
2. Si $X = H \subset G$ est un sous-groupe de G, alors on a $H \lhd N_G(H) < G$. De plus, le groupe $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal (d'où la terminologie).
3. En particulier, H est normal dans G si et seulement si $N_G(H) = G$. En d'autres termes, H a un unique conjugué si et seulement si $[G : N_G(H)] = 1$.

Cette dernière observation se généralise de la façon suivante.

Lemme II.107. *Soit H un sous-groupe d'un groupe fini G. Le nombre de sous-groupes de G conjugués à H est donné par l'indice $[G : N_G(H)]$.*

Démonstration. Considérons l'action par conjugaison de G sur l'ensemble des sous-groupes de G. On cherche à calculer le cardinal $|G \cdot H|$ de l'orbite de H. Par définition, on a $\mathrm{Stab}(H) = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$. Par la formule des orbites et Lagrange, on a donc bien

$$|G \cdot H| = \frac{|G|}{|\mathrm{Stab}(H)|} = \frac{|G|}{|N_G(H)|} = [G : N_G(H)]\,. \qquad \square$$

On aura besoin d'un dernier résultat préliminaire.

Lemme II.108. *Si H est un p-sous-groupe d'un groupe fini G, alors*

$$[N_G(H) : H] \equiv [G : H] \pmod p\,.$$

Démonstration. Considérons l'action de H par multiplication à gauche sur l'ensemble $X = G/H$ des classes à gauche modulo H. Comme dans la preuve du Théorème II.98, on vérifie que les points fixes de cette action sont les classes gH telles que $H = gHg^{-1}$, ce qui est équivalent à $g \in N_G(H)$. En d'autres termes, on a $X^H = N_G(H)/H$. Ainsi, le nombre de points fixes est donné par

$$|X^H| = |N_G(H)/H| = [N_G(H) : H] .$$

Comme H est un p-groupe, on peut appliquer le Lemme II.90 et obtenir

$$[G : H] = |G/H| = |X| \equiv |X^H| = [N_G(H) : H] \pmod{p} . \qquad \square$$

Nous sommes enfin en mesure de démontrer le troisième théorème de Sylow.

Démonstration du Théorème II.102. Soient donc G un groupe fini, et p un premier. Par le premier théorème de Sylow, il existe un p-Sylow P de G. Comme tous les p-Sylow de G sont conjugués (Corollaire II.100), on a

$$n_p = \#\{p\text{-Sylow de } G\} = \#\{\text{conjugués de } P\} = [G : N_G(P)]$$

par le Lemme II.107. Par conséquent, on a

$$m = [G : P] = \frac{|G|}{|P|} = \frac{|G|}{|N_G(P)|} \cdot \frac{|N_G(P)|}{|P|} = [G : N_G(P)] \cdot [N_G(P) : P] = n_p \cdot [N_G(P) : P] ,$$

ce qui montre que n_p divise m comme annoncé. Comme P est un p-groupe, on peut appliquer le Lemme II.108, d'où $m = [G : P] \equiv [N_G(P) : P] \pmod{p}$. Par l'égalité ci-dessus, on a donc

$$m = n_p \cdot [N_G(P) : P] \equiv n_p \cdot m \pmod{p} .$$

Comme p et m sont premiers entre eux, la classe de m modulo p est inversible dans $\mathbb{Z}/p\mathbb{Z}$. L'équation ci-dessus implique donc $n_p \equiv 1 \pmod{p}$. $\square$

II.6.4 Applications des théorèmes de Sylow

Venons-en à la dernière sous-section de ce chapitre : trois applications classiques des théorèmes de Sylow.

A. Non-existence de groupe simple d'ordre donné

Pour G un groupe fini et p un premier fixé, on notera $|G| = p^r m$ avec $p \nmid m$. Comme on l'a vu en Corollaire II.104, s'il existe un premier p tel que le seul diviseur d de m tel que $d \equiv 1 \pmod{p}$ est $d = 1$, alors G admet un unique p-Sylow, qui est normal. En particulier, si $m > 1$, alors le groupe G n'est pas simple [26].

Cette observation permet de conclure à la non-existence de groupe simple d'un ordre donné. Voyons quelques exemples, de complexité croissante.

26. Si $m = 1$, alors G est un p-groupe, qui n'est simple que si $r = 1$ (par le Théorème II.91 et la Proposition II.6).

Exemples II.109 (Non-simplicité de groupes)**.**

1. Il n'existe pas de groupe simple d'ordre 2024.

   ⌜ Comme $2024 = 2^3 \cdot 11 \cdot 23$, considérons $p = 23$. La liste des diviseurs de $m = 2^3 \cdot 11 = 88$ est $\{1, 2, 4, 8, 11, 22, 44, 88\}$. Parmi ces diviseurs, le seul qui satisfait $d \equiv 1 \pmod{23}$ est $d = 1$. Ainsi, tout groupe d'ordre 2024 possède un sous-groupe normal d'ordre 23, et n'est donc pas simple. ⌟

2. Il n'existe pas de groupe simple d'ordre 12.

   ⌜ Comme $12 = 2^2 \cdot 3$, le troisième théorème de Sylow implique que $n_2 \in \{1, 3\}$ et $n_3 \in \{1, 4\}$. On ne peut donc pas conclure aussi simplement que ci-dessus. Mais supposons $n_3 = 4$. Par Lagrange, les 4 sous-groupes d'ordre 3 s'intersectent en $\{e\}$, d'où 8 éléments d'ordre 3 dans G. Il reste donc $12 - 1 - 8 = 3$ éléments d'ordre 2 ou 4, seulement la place pour un seul 2-Sylow, qui est donc normal dans G. Ainsi, un groupe G possède soit un sous-groupe normal d'ordre 3 (si $n_3 = 1$), soit un sous-groupe normal d'ordre 4 (si $n_3 = 4$, auquel cas $n_2 = 1$), soit les deux (si $n_2 = 1$ et $n_3 = 1$). Dans tous les cas, il n'est pas simple. ⌟

3. Il n'existe pas de groupe simple d'ordre 24.

   ⌜ Comme $24 = 2^3 \cdot 3$, le troisième théorème de Sylow implique à nouveau $n_2 \in \{1, 3\}$ et $n_3 \in \{1, 4\}$ et ne suffit pas à conclure. De plus, il y a la place [27] dans un groupe d'ordre 24 pour $n_2 = 3$ et $n_3 = 4$. Mais dans ce cas, considérons l'action de G par conjugaison sur l'ensemble X des trois 2-Sylow. Cette action est non-triviale puisque tous ces 2-Sylow sont conjugués (Corollaire II.100). Cela définit un homomorphisme $G \to S(X) = S_3$ dont le noyau $N \triangleleft G$ satisfait $N \neq G$ (puisque cet homomorphisme est non-trivial) et $N \neq \{e\}$ (puisque $|G| = 24 > 6 = |S_3|$). Ainsi, le groupe G n'est pas simple. ⌟

En utilisant ces techniques de manière systématique, on peut montrer les résultats suivants.

- Si G est un groupe d'ordre $|G| < 60$ non-premier, alors G n'est pas simple.
- Si G est un groupe d'ordre $|G| = pq$, p^2q ou pqr avec p, q, r des premiers distincts, alors G n'est pas simple.

Notons que les deux hypothèses sont nécessaires, puisque A_5 est un groupe simple d'ordre $60 = 2^2 \cdot 3 \cdot 5$.

B. Classification des groupes d'ordre pq

Rappelons que nous avons déjà classifié les groupes d'ordre p premier (ils sont isomorphes à $\mathbb{Z}/p\mathbb{Z}$ par Lagrange), et ceux d'ordre p^2 (isomorphes à $\mathbb{Z}/p\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ par le Théorème II.94).

Grâce aux théorèmes de Sylow, nous pouvons aller plus loin.

27. Et cela arrive, par exemple dans $G = S_4$.

Théorème II.110: classification des groupes d'ordre pq

Soit G un groupe d'ordre pq avec $p < q$ deux premiers.

(i) Si $q \not\equiv 1 \pmod{p}$, alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$.

(ii) Si $q \equiv 1 \pmod{p}$, alors G est isomorphe soit au groupe cyclique $\mathbb{Z}/pq\mathbb{Z}$, soit à un unique groupe non-abélien $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Démonstration. Soit G un groupe d'ordre pq avec $p < q$ premiers. Par le troisième théorème de Sylow, le nombre n_q de q-Sylow de G satisfait $n_q \mid p$ (d'où $n_p \in \{1, p\}$ puisque p est premier) et $n_q \equiv 1 \pmod{q}$, d'où $n_q = 1$ car $p < q$. Cet unique q-Sylow est donc un sous-groupe normal $N \triangleleft G$. Comme il est d'ordre q premier, on a $N \simeq \mathbb{Z}/q\mathbb{Z}$. Par le premier théorème de Sylow, il existe un p-Sylow H de G. Comme il est d'ordre p premier, on a $H \simeq \mathbb{Z}/p\mathbb{Z}$.

Il s'agit à présent de vérifier que G est le produit semi-direct interne de N par H. On a déjà que N est normal dans G. Ensuite, comme $N \cap H$ est un sous-groupe de H et de N, Lagrange implique que son ordre divise $|H| = p$ et $|N| = q$. Comme ce sont des premiers distincts, on a $|H \cap N| = 1$, et donc $N \cap H = \{e\}$. Finalement, par le deuxième théorème d'isomorphisme (Théorème II.4), le sous-groupe $NH < G$ satisfait $NH/N \simeq H/(N \cap H)$, d'où

$$|NH| = \frac{|N| \cdot |H|}{|N \cap H|} = \frac{q \cdot p}{1} = pq = |G|,$$

ce qui implique $NH = G$.

Le groupe G étant le produit semi-direct interne de $N \simeq \mathbb{Z}/q\mathbb{Z}$ par $H \simeq \mathbb{Z}/p\mathbb{Z}$, la Proposition II.64(ii) donne un isomorphisme

$$G \simeq N \rtimes_\theta H \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\theta \mathbb{Z}/p\mathbb{Z}$$

pour un certain homomorphisme $\theta\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^*$. Comme expliqué en Exemple II.63.3, la donnée d'un tel homomorphisme est équivalente à la donnée de $\theta_{[1]} =: [k] \in (\mathbb{Z}/q\mathbb{Z})^*$ tel que $[k]^p = [1]$. Ainsi, l'ordre de $[k]$ dans $(\mathbb{Z}/q\mathbb{Z})^*$ est soit 1, soit p.

- L'ordre de $[k]$ est 1 si et seulement si $[k] = [1]$, ce qui est équivalent à avoir un produit direct $G \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Par le théorème chinois, on obtient donc le groupe cyclique $\mathbb{Z}/pq\mathbb{Z}$.
- Si l'ordre de $[k] \in (\mathbb{Z}/q\mathbb{Z})^*$ est égal à p, cela implique par Lagrange que p divise $q - 1$, i.e. la congruence $q \equiv 1 \pmod{p}$. Dans ce cas, le Lemme II.66 assure qu'à isomorphisme près, il existe un unique produit semi-direct non-abélien $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Cela conclut la preuve. □

Exemples II.111.

1. Si G est un groupe d'ordre $2q$ avec q un premier impair, alors G est isomorphe soit au groupe cyclique $\mathbb{Z}/2q\mathbb{Z}$, soit au groupe diédral $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq D_{2q}$.

2. Tous les groupes d'ordre $3 \cdot 5 = 15$ sont cycliques, de même que ceux d'ordre $3 \cdot 11 = 33$, $5 \cdot 7 = 35$, $3 \cdot 17 = 51$, $5 \cdot 13 = 65$, $7 \cdot 11 = 77$, etc.
3. Un groupe d'ordre $3 \cdot 7 = 21$ est soit cyclique, soit isomorphe à un unique groupe non-abélien $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$.

C. Classification des groupes d'ordre au plus 15

Pour conclure, nous allons énoncer la classification des groupes d'ordre au plus 15, sans en donner tous les détails. Cela constitue un bon résumé des différents résultats de classification obtenus jusqu'ici.

Cette classification est donnée dans la table ci-dessous, où l'on note C_n le groupe cyclique d'ordre n.

$\lvert G\rvert$	abéliens	non-abéliens
1	C_1	
2	C_2	
3	C_3	
4	C_4, $C_2 \times C_2$	
5	C_5	
6	C_6	D_6
7	C_7	
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$	D_8, Q
9	C_9, $C_3 \times C_3$	
10	C_{10}	D_{10}
11	C_{11}	
12	C_{12}, $C_6 \times C_2$	D_{12}, A_4, $C_3 \rtimes C_4$
13	C_{13}	
14	C_{14}	D_{14}
15	C_{15}	

Pour démontrer cette classification, soit donc G un groupe d'ordre $1 < n \leq 15$.

- Si $n = p \in \{2, 3, 5, 7, 11, 13\}$, alors $G \simeq \mathbb{Z}/p\mathbb{Z}$ par Lagrange.
- Si $n = p^2 \in \{4, 9\}$, alors $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ par le Théorème II.94.
- Si $n = 2q \in \{6, 10, 14\}$, alors $G \simeq \mathbb{Z}/2q\mathbb{Z}$ ou D_{2q} par le Théorème II.110. Notons que le groupe D_6 est isomorphe à S_3.
- Si $n = 15 = 3 \cdot 5$, on a $G \simeq \mathbb{Z}/15\mathbb{Z}$ par le Théorème II.110.

Restent les groupes d'ordre 8 et 12.

- Pour $n = 8$, on connaît la liste complète des groupes abéliens d'ordre 8 par le Théorème II.67, à savoir $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z}$. On connaît

également le groupe non-abélien D_8. Il s'avère qu'il en existe encore un, appelé le *groupe quaternionique*, dont voici une présentation :

$$Q := \langle x, y \mid x^4, x^2y^2, yxy^{-1}x \rangle .$$

Il est possible de montrer que D_8 et Q sont les seuls groupes non-abéliens d'ordre 8, et ne sont pas isomorphes.

- Finalement, pour $n = 12$, on connaît la liste complète des groupes abéliens par le Théorème II.67 : $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On connaît également les groupes[28] non-abéliens A_4, D_{12} et $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$. Il est possible de montrer que ce sont les seuls groupes non-abéliens d'ordre 12, et qu'ils ne sont pas isomorphes.

On obtient donc bien la classification énoncée dans la table ci-dessus.

Exercices

1. Soient N, H des sous-groupes d'un groupe G avec $N \triangleleft G$. Montrer les assertions suivantes, qui forment le *deuxième théorème d'isomorphisme*.
   (i) L'ensemble $NH := \{nh \mid n \in N,\ h \in H\}$ est un sous-groupe de G.
   (ii) On a $N \triangleleft NH$ et $(N \cap H) \triangleleft H$.
   (iii) On a un isomorphisme $NH/N \simeq H/(N \cap H)$.

2. Soit N un sous-groupe normal d'un groupe G. Montrer les assertions suivantes, qui forment le *troisième théorème d'isomorphisme*.
   (i) Les sous-groupes de G/N sont de la forme H/N avec $N \subset H < G$.
   (ii) Pour tout $N \subset H < G$, on a $H/N \triangleleft G/N$ si et seulement si $H \triangleleft G$.
   (iii) Pour tout $N \subset H \triangleleft G$, on a $(G/N)/(H/N) \simeq G/H$.

3. Soit G un groupe abélien. Montrer que G est simple si et seulement si $G \simeq \mathbb{Z}/p\mathbb{Z}$ avec p premier.

4. Montrer les énoncés suivants.
   (i) Si $\varphi : G \to G'$ est un homomorphisme, alors $\varphi([G,G]) = [\varphi(G), \varphi(G)]$.
   (ii) Si G, G' sont deux groupes, alors $[G \times G', G \times G'] = [G,G] \times [G',G']$.
   (iii) Si $N \triangleleft G$ est tel que G/N est abélien, alors N contient $[G,G]$.

5. Montrer que le groupe dérivé de A_4 est donné par

$$[A_4, A_4] = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\},$$

   et est isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

6. Soit K un corps, et $n \geq 1$ un entier. Pour $1 \leq i \neq j \leq n$ et $\lambda \in K^*$, soit $E_{ij}(\lambda) \in \mathrm{SL}(n,K)$ la *matrice élémentaire* définie par

$$(E_{ij}(\lambda))_{k\ell} = \begin{cases} 1 & \text{si } k = \ell; \\ \lambda & \text{si } i = k \text{ et } j = \ell; \\ 0 & \text{sinon.} \end{cases}$$

28. Le troisième provient de l'existence d'un homomorphisme $\mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z})^*$ non-trivial.

En clair, cette matrice a des 1 sur la diagonale, un (i,j)-coefficient donné par λ, et des zéros partout ailleurs.

(i) Montrer que $\mathrm{SL}(n,K)$ est engendré par les matrices élémentaires $E_{ij}(\lambda)$.

(ii) Vérifier que pour i,j,k distincts, les matrices élémentaires satisfont

$$E_{ij}(\lambda) = E_{ik}(\lambda)E_{kj}(1)E_{ik}(-\lambda)E_{kj}(-1)\,.$$

7. À l'aide de l'exercice précédent, montrer les points suivants pour tout corps K et tout entier $n \neq 2$:

(i) $[\mathrm{GL}(n,K),\mathrm{GL}(n,K)] = \mathrm{SL}(n,K)$;

(ii) $[\mathrm{SL}(n,K),\mathrm{SL}(n,K)] = \mathrm{SL}(n,K)$.

À votre avis, les groupes $\mathrm{SL}(n,K)$ avec $n \geq 3$ sont-ils simples ?

8. (i) Vérifier que les groupes $\mathrm{GL}(n,\mathbb{F}_2)$ et $\mathrm{SL}(n,\mathbb{F}_2)$ coïncident.

(ii) En étudiant l'action naturelle du groupe $\mathrm{GL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2)$ sur les trois vecteurs non-nuls de $\mathbb{F}_2^2$, montrer qu'il est isomorphe au groupe symétrique S_3.

(iii) En conclure que les assertions de l'exercice précédent sont en général fausses pour $n = 2$.

9. Montrer qu'un groupe est simple et résoluble si et seulement s'il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

10. Un groupe G est dit *parfait* si $[G,G] = G$. Montrer les assertions suivantes.

(i) Un groupe abélien non-trivial n'est pas parfait.

(ii) Un groupe G est parfait si et seulement si tout homomorphisme $\varphi\colon G \to A$ avec A abélien est trivial.

(iii) Si $\varphi\colon G \to G'$ est un homomorphisme avec G parfait, alors $\varphi(G)$ est parfait.

(iv) Tout quotient d'un groupe parfait est parfait.

(v) Tout groupe simple non-abélien est parfait.

(vi) Un groupe résoluble non-trivial n'est pas parfait.

Donner deux exemples de familles infinies de groupes parfaits.

11. Rappelons que pour tout $n \geq 3$, le *groupe diédral* D_{2n} est le groupe des isométries du plan qui fixent globalement le n-gone de sommets $\{z \in \mathbb{C} \,|\, z^n = 1\}$. Ce groupe d'ordre $2n$ est engendré par la rotation r d'angle $2\pi/n$ autour de l'origine et par la conjuguaison complexe s.

(i) Calculer le groupe dérivé du groupe diédral D_{2n}.

(ii) Déterminer l'abélianisé de D_{2n}.

12. Rappelons qu'une action d'un groupe G sur un ensemble X est équivalente à la donnée d'un homomorphisme de groupes

$$G \longrightarrow S(X) = \mathrm{Aut}_{\mathsf{Set}}(X)\,.$$

Par conséquent, on définit une *action d'un groupe G sur un objet A* d'une catégorie $\mathscr{C}$ quelconque comme la donnée d'un homomorphisme de groupes

$$G \longrightarrow \mathrm{Aut}_{\mathscr{C}}(A)\,.$$

Parmi les notions suivantes, déterminer lesquels se généralisent de la catégorie Set à une catégorie $\mathscr{C}$ arbitraire :

orbite, action transitive, point fixe, stabilisateur, action fidèle.

13. Soient $\mathscr{F}\colon \mathsf{Grp} \to \mathsf{Ab}$ le foncteur donné par l'abélianisation, et $\mathscr{G}\colon \mathsf{Ab} \to \mathsf{Grp}$ le foncteur oubli. Vérifier que pour tout groupe G et tout groupe abélien A, on a une bijection naturelle

$$\mathrm{Hom}_{\mathsf{Ab}}(\mathscr{F}(G), A) \simeq \mathrm{Hom}_{\mathsf{Grp}}(G, \mathscr{G}(A))\,.$$

Remarque. On dit que $\mathscr{F}$ et $\mathscr{G}$ sont des *foncteurs adjoints*. Plus précisément, on dit que $\mathscr{F}$ est *adjoint à gauche* de $\mathscr{G}$ et que $\mathscr{G}$ est *adjoint à droite* de $\mathscr{F}$.

14. Rappelons la catégorie Mon des monoïdes définie en exercice 2 du Chapitre I.
    (i) Vérifier que pour tout monoïde E, l'ensemble

$$\mathscr{I}(E) := \{x \in E \mid \text{il existe } y \in E \text{ tel que } xy = yx = e\}$$

    des éléments inversibles de E forme un groupe.
    (ii) Montrer que cela permet de construire un foncteur $\mathscr{I}\colon \mathsf{Mon} \to \mathsf{Grp}$.
    (iii) Vérifier que ce foncteur est adjoint à droite du foncteur oubli $\mathsf{Grp} \to \mathsf{Mon}$.

15. Montrer que pour tous groupes G et G', on a un isomorphisme

$$(G \times G')_{\mathrm{ab}} \simeq G_{\mathrm{ab}} \oplus G'_{\mathrm{ab}}\,.$$

    En déduire que le foncteur d'abélianisation $\mathscr{F}\colon \mathsf{Grp} \to \mathsf{Ab}$ préserve les produits.

16. Soit G un groupe quelconque.
    (i) Montrer que pour tout élément $g \in G$, l'application $\iota_g\colon G \to G$ définie par $\iota_g(x) = gxg^{-1}$ est un automorphisme de G,.
    (ii) Vérifier que l'application $\iota\colon G \to \mathrm{Aut}(G)$ donnée par $g \mapsto \iota_g$ est un homomorphisme de groupes. Son image, notée $\mathrm{Int}(G)$, est le groupe des *automorphismes intérieurs* de G.
    (iii) Montrer l'isomorphisme $G/Z(G) \simeq \mathrm{Int}(G)$, où $Z(G)$ est le centre de G.
    (iv) Vérifier que $\mathrm{Int}(G)$ est un sous-groupe normal de $\mathrm{Aut}(G)$. Le quotient est noté $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Int}(G)$, et appelé le groupe des *automorphismes extérieurs* de G.
    (v) Vérifier que tout automorphisme φ de G définit un automorphisme φ_{ab} de G_{ab}, et que l'application $\mathrm{Aut}(G) \to \mathrm{Aut}(G_{\mathrm{ab}})$ donnée par $\varphi \mapsto \varphi_{\mathrm{ab}}$ est un homomorphisme de groupes.
    (vi) Montrer que cela induit un homomorphisme $\mathrm{Out}(G) \to \mathrm{Aut}(G_{\mathrm{ab}})$.
    (vii) Décrire explicitement cet homomorphisme dans le cas de G abélien.

17. Étant donné un ensemble X, on a défini un groupe libre sur X comme un objet initial d'une catégorie $\mathscr{C}^X$.
    (i) Cette catégorie admet-elle des objets finaux ? Sont-ils intéressants ?
    (ii) Comme le groupe trivial $T = \{e\}$ est un objet initial dans Grp, on pourrait penser que la paire (e, T) est un objet initial dans $\mathscr{C}^X$ pour tout ensemble X, avec $e\colon X \to T$ l'application constante. En effet, pour tout groupe G, il existe un unique homomorphisme de groupes $\varphi\colon T \to G$. Expliquer pourquoi (e, T) n'est *pas* initial dans $\mathscr{C}^X$ (sauf si X est vide).

18. Redémontrer le résultat suivant sans passer par la Remarque I.11.3 :

    Soit X un ensemble. Si $j: X \to F(X)$ et $j': X \to F'(X)$ sont deux groupes libres sur X, alors il existe un unique isomorphisme de groupes $\varphi: F(X) \to F'(X)$ tel que $\varphi \circ j = j'$.

19. Montrer que le foncteur $\mathscr{F}: \mathsf{Set} \to \mathsf{Grp}$ défini par le groupe libre est adjoint à gauche du foncteur oubli $\mathscr{O}: \mathsf{Grp} \to \mathsf{Set}$.

20. En Figure 3, on a dessiné un graphe associé au groupe libre F_2. Tenter de tracer les graphes associés aux groupes libres F_n pour $n = 0, 1, 3$.

21. (i) Vérifier que pour tout ensemble X et tout groupe abélien A, l'ensemble

    $$A^{\oplus X} = \{\alpha: X \to A \mid \alpha(x) \neq 0 \text{ pour un nombre fini de } x \in X\}$$

    est un sous-groupe du groupe abélien $A^X = \{\alpha: X \to A\}$.

    (ii) Montrer que le groupe $G = \mathbb{Z}^{\oplus \mathbb{N}}$ satisfait $G \simeq G \times G$.

    (iii) Expliquer pourquoi le groupe $\mathbb{Z}^X$ (muni de l'application naturelle $j: X \to \mathbb{Z}^X$) n'est *pas* un groupe abélien libre sur X si cet ensemble est infini.

22. Soit $\mathscr{C}$ une *catégorie concrète*, c'est-à-dire une catégorie munie d'un foncteur oubli $\mathscr{G}: \mathscr{C} \to \mathsf{Set}$ tel que tout $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ est déterminé par l'application associée $\mathscr{G}(f): \mathscr{G}(A) \to \mathscr{G}(B)$.
    Un *objet de $\mathscr{C}$ libre* sur un ensemble X est un objet $F(X)$ de $\mathscr{C}$ muni d'une application $j_X: X \to \mathscr{G}(F(X))$ qui satisfait la propriété universelle suivante : pour tout objet A de $\mathscr{C}$ et toute application $f: X \to \mathscr{G}(A)$, il existe un unique morphisme $\varphi \in \mathrm{Hom}_{\mathscr{C}}(F(X), A)$ tel que $\mathscr{G}(\varphi) \circ j_X = f$.

    (i) Vérifier que dans le cas de $\mathscr{C} = \mathsf{Grp}$ et Ab, on retrouve bien la définition du groupe libre et du groupe abélien libre sur X.

    (ii) Qu'est-ce qu'un objet de $\mathscr{C}$ libre sur $X = \varnothing$?

    (iii) Montrer que s'il existe, un objet de $\mathscr{C}$ libre sur X est unique à unique isomorphisme près (dans quelle catégorie ?).

    (iv) Supposons qu'il existe un objet A de $\mathscr{C}$ tel que $|\mathscr{G}(A)| \geq 2$. Vérifier qu'alors, l'application $j_X: X \to \mathscr{G}(F(X))$ est injective pour tout ensemble X.

    (v) Montrer que si $F(X)$ existe pour tout ensemble X, cela définit un foncteur $\mathscr{F}: \mathsf{Set} \to \mathscr{C}$ adjoint à gauche du foncteur oubli $\mathscr{G}: \mathscr{C} \to \mathsf{Set}$.

    (vi) En s'inspirant des constructions vues en cours pour les catégories $\mathscr{C} = \mathsf{Grp}$ et Ab, donner une construction explicite d'un objet de $\mathscr{C}$ libre sur X pour les catégories $\mathscr{C} = \mathsf{Mon}$ et K-Vect. Identifier ces objects libres dans les cas $X = \varnothing$ et $X = \{x\}$.

    (vii) Pour la catégorie $\mathscr{C} = \mathsf{Corps}$, déterminer s'il existe un objet de $\mathscr{C}$ libre sur X.

    (viii) Et pour la catégorie Ann, dans les cas $X = \varnothing$ et $X = \{x\}$?

    (ix) Et pour la catégorie Top ?

23. On va noter $G * G'$ le coproduit des groupes G et G'.

    (i) En utilisant uniquement les propriétés universelles correspondantes, montrer que le groupe libre $F(\{x, y\})$ est isomorphe à $F(\{x\}) * F(\{y\})$.

    (ii) Plus généralement, montrer que pour tous ensembles X et Y, on a

    $$F(X \sqcup Y) \simeq F(X) * F(Y)\,.$$

(iii) Ainsi, ce foncteur $\mathsf{Set} \to \mathsf{Grp}$ préserve les coproduits. Est-ce qu'il préserve également les produits ?

Indication. Commencer par construire des homomorphismes $i_X : F(X) \to F(X \sqcup Y)$ et $i_Y : F(Y) \to F(X \sqcup Y)$ à l'aide de la propriété universelle du groupe libre sur X et sur Y, puis montrer que $F(X \sqcup Y)$ muni de ces homomorphismes satisfait la propriété universelle du coproduit de $F(X)$ et $F(Y)$.

24. (i) Montrer que tout groupe dont les éléments sont d'ordre au plus 2 est abélien, et de plus un espace vectoriel sur $\mathbb{F}_2$.
(ii) Soit A un groupe abélien, et considérons le sous-groupe $2A = \{2a \mid a \in A\}$. Vérifier que le groupe abélien quotient $A/2A$ est un espace vectoriel sur $\mathbb{F}_2$.
(iii) Montrer que cette construction définit un foncteur $\mathscr{F} : \mathsf{Ab} \to \mathbb{F}_2\text{-}\mathsf{Vect}$.
(iv) Vérifier que si A et A' sont des groupes abéliens isomorphes, alors $A/2A$ et $A'/2A'$ sont des $\mathbb{F}_2$-espaces vectoriels isomorphes.

25. Étant donné un sous-ensemble R d'un groupe G, on note

$$\langle\langle R \rangle\rangle = \bigcap_{R \subset N \lhd G} N$$

l'intersection des sous-groupes normaux de G qui contiennent R. On parle du *sous-groupe normal engendré* par $R \subset G$.
(i) Vérifier qu'il s'agit du plus petit sous-groupe normal de G qui contient R.
(ii) Montrer que $\langle\langle R \rangle\rangle = \langle X \rangle$, avec

$$X = \left\{ grg^{-1} \,|\, r \in R,\ g \in G \right\} .$$

(iii) En déduire la forme générale des éléments de $\langle\langle R \rangle\rangle$.

26. (i) Soit D_{2n} le groupe diédral d'ordre $2n$ avec $n \geq 3$ (voir exercice 11). Montrer qu'il admet la présentation

$$D_{2n} = \left\langle x, y \mid x^2, y^n, xyxy \right\rangle .$$

(ii) Pour $n = 1, 2$, quels sont les groupes donnés par les présentations correspondantes ? Peut-on les interpréter comme des groupes de symétries d'un sous-ensemble du plan ?
(iii) Interpréter le *groupe diédral infini*

$$D_\infty = \left\langle x, y \mid x^2, xyxy \right\rangle$$

comme le groupe de symétries d'un sous-ensemble du plan.
(iv) Montrer que ce groupe admet également la présentation

$$D_\infty = \left\langle a, b \mid a^2, b^2 \right\rangle .$$

27. Vérifier que le groupe symétrique S_3 admet la présentation

$$S_3 = \left\langle x, y \mid x^2, y^3, xyxy \right\rangle .$$

En déduire que D_6 et S_3 sont isomorphes.

28. Trouver deux présentations différentes du groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, et démontrer qu'il s'agit bien de présentations.

29. En utilisant les propriétés universelles correspondantes, montrer que le foncteur d'abélianisation $\mathsf{Grp} \to \mathsf{Ab}$ préserve les coproduits, dans le sens que
$$(G * G')_{\mathrm{ab}} \simeq G_{\mathrm{ab}} \oplus G'_{\mathrm{ab}}$$
pour tous groupes G, G'.

30. Vérifier que pour deux sous-groupes H_1, H_2 d'un groupe G, on a $H_1 H_2 = G$ et $H_1 \cap H_2 = \{e\}$ si et seulement si tout élément $g \in G$ s'écrit de manière unique comme $g = h_1 h_2$ avec $h_1 \in H_2$ et $h_2 \in H_2$.

31. Considérons le groupe diédral $D_4 = \langle x, y \mid x^2, y^2, xyxy \rangle$.
    (i) Montrer que D_4 est le produit direct interne des sous-groupes $\langle x \rangle$ et $\langle y \rangle$.
    (ii) En déduire (à nouveau) l'existence d'un isomorphisme $D_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

32. Soient $m, n \in \mathbb{Z}$ deux entiers premiers entre eux.
    (i) Montrer que le groupe $G = \mathbb{Z}/mn\mathbb{Z}$ est produit direct interne des sous-groupes H_1 engendré par $[m]$ et H_2 engendré par $[n]$.
    (ii) En déduire une preuve du théorème des restes chinois.

33. Soient G un groupe, et $N, H < G$ des sous-groupes. Montrer que si $NH = G$, alors N est normal dans G si et seulement si $hnh^{-1} \in N$ pour tous $n \in N$ et $h \in H$.

34. Montrer qu'un groupe G est produit direct interne de sous-groupes N, H si et seulement si G est produit semi-direct interne de N par H avec $\gamma : H \to \mathrm{Aut}(N)$ trivial.

35. Soit G un groupe fini admettant un sous-groupe normal N tel que $|N|$ et $|G/N|$ sont premiers entre eux, et un sous-groupe H d'ordre $|H| = |G/N|$. Montrer que G est produit semi-direct interne de N par H.

36. Montrer que la loi de composition dans le produit semi-direct est associative.

37. Pour tout groupe G, on définit son *holomorphe* via $\mathrm{Hol}(G) = G \rtimes_\theta \mathrm{Aut}(G)$, où l'homomorphisme $\theta : \mathrm{Aut}(G) \to \mathrm{Aut}(G)$ est l'identité.
    (i) Identifier $\mathrm{Hol}(\mathbb{Z}/n\mathbb{Z})$ pour $n = 2, 3$.
    (ii) Montrer l'isomorphisme $\mathrm{Hol}(\mathbb{Z}) \simeq D_\infty$.

38. Montrer que pour tout groupe N, tout automorphisme $\alpha \in \mathrm{Aut}(N)$ peut être réalisé comme conjuguaison : il existe un groupe G contenant N comme sous-groupe normal et $g \in G$ tels que $\alpha(n) = gng^{-1}$ pour tout $n \in N$.

39. Soit $G = N \rtimes_\theta H$ un produit semi-direct (externe) de N par H. Montrer que G est résoluble si et seulement si N et H sont résolubles.

40. Montrer que si un produit semi-direct $N \rtimes_\theta H$ est abélien, alors c'est le produit direct $N \times H$.

41. (i) Montrer qu'il existe exactement deux homomorphismes $\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z})$, et donc un unique produit semi-direct $\mathbb{Z} \rtimes \mathbb{Z}$ potentiellement non-abélien.
    (ii) Écrire explicitement la loi de composition de ce groupe, et vérifier qu'il n'est pas abélien.

(iii) Montrer qu'il admet la présentation $\mathbb{Z} \rtimes \mathbb{Z} = \langle a, b \mid aba^{-1} = b^{-1} \rangle$.

42. Étant donnés deux groupes $H = \langle X \mid R \rangle$ et $N = \langle Y \mid S \rangle$ ainsi qu'un homomorphisme $\theta : H \to \mathrm{Aut}(N)$, tenter de trouver une présentation du produit semi-direct $N \rtimes_\theta H$.

Remarque. Il ne s'agit pas de donner une preuve complète, mais de proposer une réponse intuitive qui soit cohérente avec les exemples de présentations de produits semi-directs vues jusqu'à présent, à savoir

$$\mathbb{Z} \times \mathbb{Z} = \langle x, y \mid xyx^{-1}y^{-1} \rangle, \quad \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = \langle x, y \mid x^2, y^n, xyxy \rangle,$$
$$\mathbb{Z} \rtimes \mathbb{Z} = \langle x, y \mid xyx^{-1}y \rangle, \quad \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = \langle x, y \mid x^2, xyxy \rangle .$$

On pourra ensuite donner une idée de preuve.

43. Classifier les groupes abéliens d'ordre 360 à isomorphisme près.

44. Soit G est un groupe abélien fini.
    (i) En utilisant le théorème de classification, montrer que pour tout d qui divise l'ordre de G, il existe un sous-groupe d'ordre d.
    (ii) Pour un premier p, notons $|G| = p^k m$ avec $p \nmid m$. En utilisant le théorème de classification, vérifier que G admet un unique sous-groupe d'ordre p^k.

45. Pour tout entier $m > 0$, déterminer le nombre de groupes abéliens d'ordre m à isomorphisme près.

Rappel. Une *partition* d'un entier n est une décomposition de n en somme d'entiers strictement positifs ; on notera $p(n)$ le nombre de ces partitions, considérées à l'ordre des termes près.

46. Fixons un groupe abélien G, un premier p et un entier $i \geq 0$.
    (i) Vérifier que $p^i G := \{p^i x \mid x \in G\}$ est un sous-groupe de G, avec $p^{i+1}G < p^i G$. On peut donc considérer le groupe abélien quotient $p^i G/p^{i+1}G$.
    (ii) Pour $G = \mathbb{Z}/p^n\mathbb{Z}$, montrer que $p^i G/p^{i+1}G$ est d'ordre p pour $0 \leq i < n$ et trivial pour $i \geq n$.
    (iii) Pour $G = \mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_\ell}\mathbb{Z}$, calculer l'entier d_i tel que $|p^i G/p^{i+1}G| = p^{d_i}$. En déduire que la suite d'entiers d_i permet de reconstruire les entiers $n_1, \ldots, n_\ell$ à l'ordre près.

47. (i) Si M_1, M_2 sont des A-modules, montrer que $M_1 \times M_2$ est un A-module pour les lois

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$
$$a \cdot (x_1, x_2) = (a \cdot x_1, a \cdot x_2) .$$

    Il est noté $M_1 \oplus M_2$, et appelé la *somme directe* de M_1 et M_2.
    (ii) Vérifier que le produit et le coproduit de M_1 et M_2 dans la catégorie A-Mod sont donnés par la somme directe $M_1 \oplus M_2$ (munie de quelles applications ?)

48. Montrer que dans un A-module M, on a les égalités suivantes pour tous $a \in A$ et $x \in M$:

$$a \cdot 0_M = 0_M, \quad 0_A \cdot x = 0_M .$$

A-t-on également que $a \cdot x = 0_M$ implique $a = 0_A$ ou $x = 0_M$ comme dans le cas d'un espace vectoriel ?

49. Existe-t-il un objet initial dans la catégorie A-Mod ? Et un objet final ?

50. (i) Vérifier que si $\varphi\colon A \to B$ est un homomorphisme d'anneaux, alors B est un A-module via $a \cdot b = \varphi(a)b$ pour tous $a \in A$ et $b \in B$.
    (ii) En conclure que A est un A-module pour la loi "externe" donnée par la multiplication.
    (iii) En conclure également que tout anneau de caractéristique n est un module sur $\mathbb{Z}/n\mathbb{Z}$ (et donc, que tout anneau de caractéristique p premier est un $\mathbb{F}_p$-espace vectoriel).

51. (i) Montrer que la donnée d'une structure de A-module sur un groupe abélien fixé $(M,+)$ coïncide avec la donnée d'un homomorphisme d'anneaux
$$A \longrightarrow \mathrm{End}_{\mathsf{Ab}}(M)\,.$$
    (ii) En particulier, vérifier que tout groupe abélien $(M,+)$ est un module sur l'anneau $\mathrm{End}_{\mathsf{Ab}}(M)$ via la loi $f \cdot x = f(x)$ pour $f \in \mathrm{End}_{\mathsf{Ab}}(M)$ et $x \in M$.

52. (i) Soit E un K-espace vectoriel muni d'un endomorphisme linéaire $f \in \mathrm{End}(E)$. Vérifier que cela définit une structure de $K[X]$-module sur E via la loi externe $K[X] \times E \to E, (P,v) \mapsto P \cdot v$ donnée par
$$\Big(\sum_{i\geq 0} \lambda_i X^i\Big) \cdot v = \sum_{i\geq 0} \lambda_i f^i(v)\,, \quad \text{où } f^0 = \mathrm{id} \text{ et } f^i = \overbrace{f \circ \cdots \circ f}^{i} \in \mathrm{End}(E)\,.$$
    On notera ce module par E_f.
    (ii) Réciproquement, montrer qu'un $K[X]$-module M est un K-espace vectoriel et que l'application $f\colon M \to M$ donnée par $f(x) = X \cdot x$ est un endomorphisme linéaire de M.
    (iii) Soient E, E' deux K-espaces vectoriels munis d'endomorphismes $f \in \mathrm{End}(E)$ et $f' \in \mathrm{End}(E')$. Vérifier qu'une application $\varphi\colon E_f \to E'_{f'}$ entre les $K[X]$-modules correspondants est $K[X]$-linéaire si et seulement si $\varphi\colon E \to E'$ est K-linéaire et satisfait $\varphi \circ f = f' \circ \varphi$.
    (iv) En conclure que deux $K[X]$-modules E_f et $E_{f'}$ sont isomorphes si et seulement si les endomorphismes $f, f' \in \mathrm{End}(E)$ sont conjugués par un automorphisme linéaire $\varphi \in \mathrm{Aut}(E)$.

53. Soit A un anneau quelconque.
    (i) Pour tout ensemble X, définir et construire le A-module libre sur X en s'inspirant des cas $A = \mathbb{Z}$ et $A = K$ déjà traités (voir l'exercice 22).
    (ii) Qu'obtient-on dans les cas $X = \varnothing$, et $X = \{1, \ldots, n\}$ avec $n \geq 1$ fini ?
    (iii) Montrer que si M est un A-module libre (i.e. isomorphe à un A-module libre sur un certain ensemble X) avec A intègre, alors $a \cdot \alpha = 0_M$ avec $a \in A$ et $\alpha \in M$ implique $a = 0_A$ ou $\alpha = 0_M$ (voir l'exercice 48).

54. Pour A un anneau intègre, montrer que les conditions suivantes sont équivalentes :
    (i) Chaque objet de A-Mod est libre.
    (ii) L'anneau A est un corps.

55. Soit p un premier fixé. Montrer qu'un groupe abélien dont tous les éléments sont d'ordre 1 ou p admet une structure de $\mathbb{F}_p$-espace vectoriel.

56. Le but de cet exercice est de proposer des "questions ouvertes" élémentaires.
    (i) Existe-t-il un groupe G dont l'action sur lui-même par conjugaison est transitive ?
    (ii) Le centre de tout p-groupe non-trivial est non-trivial. Est-ce vrai pour un groupe d'ordre pq avec p, q deux premiers distincts ?
    (iii) Par Cauchy, si un premier p divise l'ordre de G, alors G admet un élément d'ordre p. Est-ce que cet énoncé est vrai pour le produit pq de deux premiers divisant l'ordre de G ?
    (iv) On l'a vu, tout groupe d'ordre p^2 est abélien. Est-ce également le cas de tout groupe d'ordre pq ? Et de tout groupe d'ordre p^3 ?
    (v) Par Lagrange, l'ordre d'un sous-groupe $H < G$ divise l'ordre de G. Est-ce que réciproquement, pour tout diviseur d de $|G|$, il existe un sous-groupe $H < G$ d'ordre d ?
    (vi) Est-ce qu'une action d'un p-groupe sur un ensemble fini X tel que p ne divise pas $|X|$ admet toujours un point fixe ?
    (vii) Est-ce qu'une action d'un p-groupe sur un ensemble fini X admet toujours un point fixe ?

57. Montrer les énoncés suivants, où G est un groupe et x un élément de G.
    (i) L'indice $[G : Z_G(x)]$ est le cardinal de la classe de conjugaison de x.
    (ii) Tout sous-groupe de $Z(G)$ est normal dans G.
    (iii) Si G admet un sous-groupe $H < Z(G)$ tel que G/H est cyclique, alors G est commutatif.

58. Soit $G = D_{2n}$ le groupe diédral d'ordre $2n$, avec $3 \leq n < \infty$.
    (i) Calculer le centre de G.
    (ii) Identifier les classes de conjuguaison.
    (iii) Pour chaque classe de conjuguaison, calculer l'indice du centralisateur.
    (iv) Vérifier explicitement la validité de l'équation des classes pour D_{2n}.

59. (i) Montrer que pour le groupe A_5, l'équation des classes donne
$$60 = 1 + 15 + 20 + 12 + 12\,.$$
    (ii) À l'aide de cette equation, donner une nouvelle preuve du fait que A_5 est un groupe simple.

    Indication. Un sous-groupe normal est une union de classes de conjugaisons, contient l'identité, et a un ordre qui divise l'ordre du groupe.

60. Le but de cet exercice est de montrer à l'aide de l'équation des classes que tout groupe non-abélien d'ordre 6 est isomorphe à S_3.

    Comme on l'a vu en cours, cette équation montre qu'un tel groupe G a un centre trivial et exactement deux classes de conjuguaison non-triviales, d'ordre 2 et 3.
    (i) Montrer qu'un groupe dont tous les éléments sont d'ordre ≤ 2 est abélien ; en conclure qu'il existe $y \in G$ d'ordre 3.
    (ii) Vérifier que $\langle y \rangle$ est normal dans G.
    (iii) Montrer que $[y]$ est la classe de conjuguaison d'ordre 2, et que $[y] = \{y, y^2\}$.
    (iv) Montrer qu'il existe $x \in G$ tel que $yx = xy^2$.

(v) Vérifier que x est d'ordre 2.
(vi) Montrer que x, y engendrent G.
(vii) En utilisant l'exercice 27, en conclure que G est isomorphe à S_3.

61. Le but de cet exercice est d'explorer ce que nous dit l'équation des classes dans le cas du groupe symétrique $G = S_n$.

Comme vous l'avez vu en Algèbre I, l'identité $\tau(i_1, \dots, i_\ell)\tau^{-1} = (\tau(i_1), \dots, \tau(i_\ell))$ implique facilement le résultat suivant : deux permutations sont conjuguées dans S_n si et seulement si elles admettent toutes deux une décomposition en cycles disjoints de longueurs $\ell_1, \dots, \ell_m$ pour les même valeurs $\ell_1, \dots, \ell_m$ (avec $\ell_1 + \cdots + \ell_m = n$). Une telle partition λ de n peut être encodée par une suite d'entiers non-négatifs de la manière suivante : on notera $\lambda = (a_j)_{j\geq 1}$ si la partition λ contient a_1 fois le nombre 1, a_2 fois le nombre 2, a_3 fois le nombre 3,... (avec $\sum_j j a_j = n$).

(i) Vérifier que le centre de S_n est trivial pour $n \geq 3$.
(ii) Montrer que pour $\sigma \in S_n$ dans la classe de conjuguaison correspondant à la partition $\lambda = (a_j)_{j\geq 1}$, on a

$$|Z_G(\sigma)| = \prod_{j\geq 1} j^{a_j}(a_j!)\,.$$

(iii) En déduire la formule suivante : pour tout entier $n \geq 1$, on a

$$n! = \sum_{\lambda=(a_j)\vdash n} \frac{n!}{\prod_{j\geq 1} j^{a_j}(a_j!)}\,,$$

où la somme est sur toutes les partitions $\lambda = (a_j)_{j\geq 1}$ de l'entier n.
(iv) Expliciter les termes de cette formule pour $n = 1, 2, 3, 4$.

62. Soient p, q deux premiers, et soit G un groupe d'ordre pq. Montrer que soit G est abélien, soit son centre est trivial.

63. Soit p un premier, et soit G un groupe d'ordre p^r. Montrer que G contient un sous-groupe normal d'ordre p^k pour tout $k \leq r$.

Indication. Procéder par récurrence sur $r \geq 0$ et utiliser le troisième théorème d'isomorphisme.

64. Le premier théorème de Sylow a été démontré comme cas particulier de la Proposition II.97, qui dit que tout diviseur de G qui est une puissance d'un premier est réalisé comme ordre d'un sous-groupe de G. Montrer que réciproquement, cette proposition est elle-même une conséquence facile du premier théorème de Sylow.

65. Soit G le groupe symétrique S_4.
(i) Faire la liste de tous les p-sous-groupes de Sylow de G.
(ii) Vérifier les trois théorèmes de Sylow sur cet exemple.
(iii) Montrer que les deuxième et troisième théorèmes ne s'appliquent pas aux sous-groupes de G d'ordre 4.

66. Soient G un groupe d'ordre 12, et n_p le nombre de p-sous-groupes de Sylow de G. Comme on l'a vu, on a $n_2 \in \{1, 3\}$ et $n_3 \in \{1, 4\}$ mais $(n_2, n_3) \neq (3, 4)$ (ce qui implique que G n'est pas simple). Identifier les nombres n_2 et n_3 pour les groupes suivants :

$$\mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \quad A_4, \quad D_{12}, \quad \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}\,.$$

67. Existe-t-il un groupe simple d'ordre 2023 ?

68. En utilisant le troisième théorème de Sylow et la Proposition II.22, démontrer que tout groupe d'ordre pq, p^2q ou pqr avec p, q, r trois premiers distincts est un groupe résoluble.
Est-ce que tout groupe d'ordre p^2qr est résoluble ?

Chapitre III: Corps

Le but de ce chapitre est de présenter les bases de la théorie des *extensions de corps*, dont la formulation moderne doit beaucoup au mathématicien allemand Heinrich Weber. Outre les préparatifs nécessaires à la théorie de Galois, ce chapitre contient quelques résultats tout à fait remarquables, comme la caractérisation des points constructibles à la règle et au compas (Section III.5) et la classification des corps finis (Section III.7).

Heinrich Weber (1842-1913)

III.1 Rappels sur les anneaux et les corps

Comme le chapitre précédent, nous allons commencer ce chapitre par une section de rappels sur la théorie des anneaux, dont la formulation moderne est essentiellement due à Emmy Noether.

Emmy Noether (1882-1935)

Le but est non seulement de se remémorer les concepts fondamentaux de la théorie des anneaux vus en Algèbre I, mais également de les compléter avec quelques résultats qui nous seront utiles par la suite. En particulier, nous verrons deux sources importantes de corps : les corps de fractions, et les quotients d'anneaux par des idéaux maximaux.

Comme vous le savez, la *catégorie des anneaux*, notée Ann, est définie ainsi :

- Les objets de Ann sont les *anneaux*, i.e. les groupes abéliens $(A,+)$ munis d'une loi de composition $(a,b)\mapsto ab$ associative, admettant un neutre 1_A, et satisfaisant les relations de distributivité $a(b+c)=ab+ac$ et $(a+b)c=ab+ac$ pour tous $a,b,c\in A$.
- Les morphismes de Ann sont les *homomorphismes d'anneaux*, i.e. les applications $\varphi\colon A\to A'$ telles que $\varphi(a+b)=\varphi(a)+\varphi(b)$, $\varphi(ab)=\varphi(a)\varphi(b)$ pour tous $a,b\in A$ et $\varphi(1_A)=1_{A'}$.

Ainsi, toutes les notions vues au Chapitre I ont un sens dans Ann : en particulier, les *isomorphismes d'anneaux* (qui coïncident avec les homomorphismes bijectifs), l'objet final (qui est *l'anneau trivial* $A=0$ caractérisé par l'égalité $0_A=1_A$), et l'objet initial (qui n'est autre que l'anneau des entiers $\mathbb{Z}$). Un autre anneau intéressant est l'objet libre de la catégorie Ann sur l'ensemble réduit à un singleton : comme on l'a vu en exercices, il s'agit de l'anneau $\mathbb{Z}[X]$ des polynômes[1] à coefficients dans $\mathbb{Z}$.

1. À ce sujet, on notera habituellement $f\in A[X]$ un polynôme, mais il sera parfois plus judicieux de le noter $f(X)$.

Un sous-ensemble B d'un anneau A est un *sous-anneau* si $1_A \in B$ et si pour tous $a, b \in B$, on a $-a, a+b, ab \in B$. On vérifie que l'image d'un homomorphisme d'anneaux est un sous-anneau [2].

Rappelons qu'un anneau A est *commutatif* si $ab = ba$ pour tous $a, b \in A$. C'est un *corps* s'il est commutatif et si son *groupe des unités* [3]

$$A^* := \{a \in A \mid \text{il existe } a^{-1} \in A \text{ tel que } aa^{-1} = a^{-1}a = 1\}$$

est égal à $A \setminus \{0\}$. On vérifie facilement qu'un corps est un anneau *intègre*, c'est-à-dire commutatif, non-trivial [4], et sans diviseur de zéro ($ab = 0$ implique $a = 0$ ou $b = 0$).

Bien entendu, la *catégorie des corps*, notée Corps, a pour objets les corps, et pour morphismes les homomorphismes d'anneaux entre corps. Une propriété cruciale des homomorphismes de corps est qu'ils sont toujours injectifs. On aura tendance à parler de *plongements* pour désigner les homomorphismes d'anneaux injectifs, et à les noter par des flèches incurvées de la forme $\hookrightarrow$.

Le résultat suivant, que vous avez vu en ALGÈBRE I, nous sera utile à de multiples reprises. Il concerne les corps finis, qui seront complètement classifiés en Section III.7.

Théorème III.1

Si K est un corps fini, alors son groupe des unités $K^* = K \setminus \{0\}$ est cyclique.

Voici à présent une question (un peu vague mais) très naturelle :

Étant donné un anneau A, comment le plonger dans un corps de la façon la plus efficace possible ?

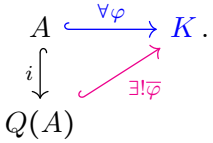
Il s'agit en particulier de construire un homomorphisme injectif $i : A \hookrightarrow Q(A)$ avec $Q(A)$ un corps. Comme $A \simeq i(A)$ est alors un sous-anneau du corps $Q(A)$, l'anneau A est nécessairement intègre. En fait, c'est toujours possible dès que cette condition est satisfaite, ce qui nous fournit une première source de corps.

Théorème III.2: Corps des fractions

Étant donné un anneau intègre A, il existe un corps $Q(A)$ et un homomorphisme injectif $i : A \hookrightarrow Q(A)$ qui satisfait la propriété universelle suivante : pour tout homomorphisme injectif $\varphi : A \hookrightarrow K$ avec K un corps, il existe un

2. Et réciproquement, tout sous-anneau $B \subset A$ est l'image d'un homomorphisme d'anneaux : l'inclusion $B \to A$.
3. Les notations $\mathscr{U}(A)$ et $A^\times$ sont parfois utilisées, mais on leur préférera A^*.
4. En effet, dans l'anneau trivial $A = \{0\}$, on a $0 = 1$ d'où $A^* = \{0\}$ et $A \setminus \{0\} = \varnothing$.

unique homomorphisme $\overline{\varphi}\colon Q(A) \hookrightarrow K$ tel que $\overline{\varphi} \circ i = \varphi$:



Démonstration. Considérons l'ensemble $A \times (A \setminus \{0\})$ muni de la relation $\sim$ définie par $(a,b) \sim (c,d)$ si $ad = bc$. On vérifie qu'il s'agit d'une relation d'équivalence. Soit $Q(A)$ l'ensemble quotient correspondant, et notons $\frac{a}{b}$ la classe d'équivalence de la paire $(a,b) \in A \times (A \setminus \{0\})$. Considérons à présent les deux lois sur $Q(A)$ définies comme suit :

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd} \quad \text{et} \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

Notons que comme A est intègre et b, d non-nuls, on a bien $bd \in A \setminus \{0\}$. On vérifiera en exercice que ces opérations sont bien définies, et font de $Q(A)$ un anneau commutatif, avec $0_{Q(A)}$ donné par la classe $\frac{0}{b}$ avec $b \in A \setminus \{0\}$, et $1_{Q(A)}$ par la classe $\frac{b}{b}$ avec $b \in A \setminus \{0\}$. Ainsi, tout élément $\frac{a}{b} \in Q(A) \setminus \{0\}$ satisfait $a \in A \setminus \{0\}$, et admet l'inverse $\frac{b}{a}$: l'anneau $Q(A)$ est donc bien un corps. On vérifie que l'application $i\colon A \to Q(A)$ donnée par $i(a) = \frac{a}{1}$ est homomorphisme injectif.

Finalement, soit $\varphi\colon A \hookrightarrow K$ un homomorphisme injectif avec K un corps. Un homomorphisme $\overline{\varphi}\colon Q(A) \hookrightarrow K$ tel que $\overline{\varphi} \circ i = \varphi$ satisfait nécessairement

$$\overline{\varphi}\left(\frac{a}{b}\right) = \overline{\varphi}\left(\frac{a}{1} \cdot \frac{1}{b}\right) = \overline{\varphi}(i(a) \cdot i(b)^{-1}) = \overline{\varphi}(i(a))\overline{\varphi}(i(b))^{-1} = \varphi(a)\varphi(b)^{-1}$$

pour tout $a \in A$ et $b \in A \setminus \{0\}$. Et l'on vérifie que cette équation définit bel et bien un homomorphisme de corps $\overline{\varphi}\colon Q(A) \hookrightarrow K$: les détails seront vus en exercices. □

Remarques III.3.

1. Le corps $Q(A)$ est appelé le *corps des fractions* de A.
2. L'homomorphisme $i\colon A \hookrightarrow Q(A)$ peut être interprété comme un objet initial dans la catégorie $\mathscr{K}^A$ dont les objets sont les homomorphismes injectifs $A \hookrightarrow K$ avec K un corps. De ce fait, par la Remarque I.11.3, le corps des fractions est uniquement déterminé à isomorphisme près par sa propriété universelle (isomorphisme unique dans $\mathscr{K}^A$).
3. Par la propriété universelle, le corps des fractions $Q(A)$ est le plus petit corps dans lequel A se plonge. Par conséquent, sa construction répond bien à la question posée ci-dessus.
4. On montre facilement que cette construction définit un foncteur de la catégorie des anneaux intègres et morphismes injectifs dans Corps. C'est un exercice.

Exemples III.4 (corps des fractions)**.**

1. Si l'anneau intègre A est un corps, alors $i = \mathrm{id}_A\colon A \hookrightarrow A$ satisfait la propriété universelle du corps des fractions : on obtient donc $Q(A) \simeq A$ dans ce cas.

2. Le corps des fractions de l'anneau des entiers $A = \mathbb{Z}$ est bien entendu le corps des rationnels $Q(\mathbb{Z}) = \mathbb{Q}$. Le preuve du Théorème III.2 n'est d'ailleurs qu'une généralisation de la construction des rationnels à partir des entiers.
3. Pour tout corps K, l'anneau des polynômes $A = K[X]$ est intègre. On peut donc considérer son corps des fractions
$$K(X) := Q(K[X]) = \left\{ \frac{f}{g} \;\middle|\; f \in K[X],\, g \in K[X] \setminus \{0\} \right\},$$
appelé le corps des *fractions rationnelles* à coefficients dans K.

Passons à présent aux anneaux quotients, qui nous fournissent une seconde vaste source de corps.

Rappelons que les quotients de groupes se font par des sous-groupes normaux, qui coïncident avec les noyaux d'homomorphismes de groupes. Similairement, les quotients d'anneaux se font par des "idéaux", qui coïncident avec les noyaux d'homomorphismes d'anneaux : un *idéal* d'un anneau commutatif[5] A est un sous-ensemble $I \subset A$ tel que $(I, +)$ est un sous-groupe de $(A, +)$ et tel que $ax \in I$ pour tous $a \in A$ et $x \in I$. En effet, les lois sur A passent au quotient et induisent des lois bien définies sur A/I, faisant de A/I anneau. De plus, la projection canonique $\pi : A \to A/I$ est un homomorphisme d'anneaux de noyau $\mathrm{Ker}(\pi) = I$ satisfaisant la propriété universelle du quotient : pour tout homomorphisme d'anneaux $\varphi : A \to A'$ avec $I \subset \mathrm{Ker}(\varphi)$, il existe un unique homomorphisme d'anneaux $\overline{\varphi} : A/I \to A'$ tel que $\overline{\varphi} \circ \pi = \varphi$:

$$\begin{array}{ccc} A & \xrightarrow{\forall \varphi} & A' \,. \\ {\scriptstyle \pi}\downarrow & \nearrow_{\exists ! \overline{\varphi}} & \\ A/I & & \end{array}$$

Comme dans la catégorie des groupes, cela implique facilement le résultat fondamental suivant.

Théorème III.5: Théorème d'isomorphisme dans Ann

Tout homomorphisme d'anneaux $\varphi : A \to A'$ induit un isomorphisme
$$\overline{\varphi} : A/\mathrm{Ker}(\varphi) \longrightarrow \mathsf{Im}(\varphi)\,.$$

Exemples III.6 (idéaux et quotients)**.**

1. Tout anneau A possède les idéaux $I = \{0\}$ et $I = A$, dits *idéaux triviaux*. Les quotients correspondants sont $A/\{0\} \simeq A$ et $A/A = 0$, et ne donnent donc rien de nouveau.
2. Un anneau commutatif non-trivial est un corps si et seulement s'il ne possède que des idéaux triviaux. Ainsi, les quotients de corps ne sont pas intéressants.
3. Si $\varphi : A \to A'$ est un homomorphisme d'anneaux, alors $\mathrm{Ker}(\varphi)$ est un idéal[6]

5. Comme vous le savez, il est possible de définir les idéaux et les anneaux quotient dans le cadre général des anneux non-commutatifs, mais nous n'en aurons pas besoin dans ce chapitre.
6. Réciproquement, tout idéal I de A est un noyau : celui de la projection $\pi : A \to A/I$.

de A. Le quotient correspondant est $A/\mathrm{Ker}(\varphi) \simeq \mathsf{Im}(\varphi)$ par le Théorème III.5. Les cas de $\varphi = \mathrm{id}_A$ et de l'homomorphisme trivial redonnent les deux exemples vu ci-dessus en 1.

4. Si $x_1, \ldots, x_n \in A$ sont des éléments quelconques d'un anneau commutatif, alors

$$(x_1, \ldots, x_n) := \{a_1x_1 + \cdots + a_nx_n \mid a_1, \ldots, a_n \in A\}$$

est le plus petit idéal de A contenant[7] $x_1, \ldots, x_n$. Dans le cas d'un unique élément $x \in A$, l'idéal

$$(x) := \{ax \mid a \in A\} = Ax = xA$$

est appelé *l'idéal principal* engendré par x. Un anneau intègre est dit *principal* si tous ses idéaux sont principaux.

5. L'anneau des entiers $\mathbb{Z}$ est un anneau principal[8] : tous ses idéaux sont de la forme $(n) = n\mathbb{Z}$ pour un certain $n \geq 0$, et les quotients correspondants sont les anneaux $\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$ des entiers modulo n.
6. Pour tout corps K, l'anneau des polynômes $K[X]$ est un anneau principal : tous ses idéaux sont de la forme (f) pour un certain $f \in K[X]$, et les quotients correspondants sont une source inépuisable de nouveaux anneaux intéressants.

La notion de *caractéristique* d'un anneau A admet maintenant une définition très élégante : comme $\mathbb{Z}$ est un objet initial de Ann, il existe un unique homomorphisme d'anneaux $\epsilon : \mathbb{Z} \to A$. Son noyau étant un idéal de $\mathbb{Z}$ principal, il existe un unique entier $n \geq 0$ tel que $\mathrm{Ker}(\epsilon) = n\mathbb{Z}$: cet entier n'est autre que $\mathrm{car}(A)$. Dans ce contexte, rappelons que les anneaux intègres (et donc en particulier les corps) ont nécessairement caractéristique nulle ou égale à un premier.

Supposons à présent que A est un anneau commutatif, et que $I \subset A$ est un idéal *propre*, i.e. différent de A ; nous noterons ce fait par le symbole $I \subsetneq A$. Un tel idéal I est dit *maximal* si pour tout idéal J avec $I \subset J \subset A$, on a $J = I$ ou $J = A$. Par ailleurs, un idéal $I \subsetneq A$ est dit *premier* si pour tous $a, b \in A$ avec $ab \in I$, on a $a \in I$ ou $b \in I$. Ces concepts sont motivés par les implications suivantes :

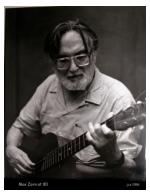
$$I \text{ maximal } \Leftrightarrow A/I \text{ corps } \Rightarrow A/I \text{ intègre } \Leftrightarrow I \text{ premier}. \tag{III.1}$$

Wolfgang Krull (1899-1971)

Puisque notre but affiché est de trouver une source de corps, il nous reste à construire des idéaux maximaux dans des anneaux commutatifs. Le théorème suivant, dû à Wolfgang Krull, est donc potentiellement très utile.

Théorème III.7: Théorème de Krull

Pour tout idéal propre I d'un anneau commutatif A, il existe un idéal maximal $\mathfrak{m}$ de A avec $I \subset \mathfrak{m} \subset A$.



MAX ZORN
(1906-1993)

Malheureusement, la démonstration [9] est non-constructive : elle repose en effet sur le fameux *lemme de Zorn*, qui est équivalent à l'*axiome du choix*. Si l'énoncé du théorème de Krull est utile, la nature de sa démonstration est donc un peu décevante. Pour construire explicitement des corps, il nous faut une méthode systématique pour construire explicitement des idéaux maximaux dans un anneau commutatif.

Soit donc A un anneau intègre, et fixons $p \in A \setminus \{0\}$ avec $p \notin A^*$. Un tel élément p est dit *irréductible* dans A si pour tous $a, b \in A$ avec $p = ab$, on a $a \in A^*$ ou $b \in A^*$. De plus, un tel élément p est dit *premier* dans A si pour tous $a, b \in A$ avec $p \mid ab$, on a $p \mid a$ ou $p \mid b$ dans A. Pour $p \in A \setminus (\{0\} \cup A^*)$, on montre facilement les implications suivantes :

$$(p) \text{ maximal } \overset{\text{(III.1)}}{\Rightarrow} (p) \text{ premier } \Leftrightarrow p \text{ premier } \Rightarrow p \text{ irréductible}. \qquad \text{(III.2)}$$

De plus, si A est un anneau principal, alors on a également que p irréductible implique (p) maximal, et toutes les conditions ci-dessus sont donc équivalentes [10]. Par conséquent, nous avons à présent une seconde vaste source de corps : "il suffit" de trouver un élément irréductible p dans un anneau principal A pour obtenir un corps $K = A/(p)$.

Exemples III.8 (corps quotients)**.**

1. Comme $\mathbb{Z}$ est un anneau principal, on obtient les équivalences suivantes pour tout entier $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$:

   $$\mathbb{Z}/p\mathbb{Z} \text{ corps } \Leftrightarrow \mathbb{Z}/p\mathbb{Z} \text{ intègre } \Leftrightarrow p \text{ premier } \Leftrightarrow p \text{ irréductible}.$$

   Le corps correspondant est noté $\mathbb{F}_p$.

2. Comme le polynôme $1+X^2 \in \mathbb{R}[X]$ n'admet pas de racine dans $\mathbb{R}$, il est irréductible dans l'anneau principal $\mathbb{R}[X]$. Par conséquent, le quotient $\mathbb{R}[X]/(1+X^2)$ est un corps. Comme vous l'avez vu, il s'agit en fait d'une des constructions possibles du corps des complexes. En effet, l'homomorphisme $\mathbb{R}[X] \to \mathbb{C}$ donné par $f \mapsto f(i)$ est surjectif de noyau $(1 + X^2)$ (ce dernier point nécessite un peu de travail), et induit donc un isomorphisme $\mathbb{R}[X]/(1 + X^2) \simeq \mathbb{C}$ par le Théorème III.5.

LEOPOLD
KRONECKER
(1823-1891)

Dans l'exemple 2 ci-dessus, nous avons construit un corps $\mathbb{R}[X]/(1+X^2) \simeq \mathbb{C}$ contenant $\mathbb{R}$ comme sous-corps, et tel que le polynôme $1 + X^2$ admet une racine dans $\mathbb{C}$. Cette construction se généralise de la façon suivante : c'est ce qu'on appelle parfois la *construction de Kronecker*.

Proposition III.9. *Soient K un corps et $f \in K[X]$ un élément irréductible. Alors, le quotient $L := K[X]/(f)$ est un corps, muni d'un plongement naturel $\varphi : K \hookrightarrow L$. De plus, le polynôme f admet une racine dans L.*

7. En fait, l'intersection de tous les idéaux de A contenant $x_1, \ldots, x_n$.
8. En fait, un anneau euclidien.
9. Que nous ne verrons pas.
10. C'est faux pour $p = 0$, puisque l'idéal (0) est premier dans $\mathbb{Z}$ mais pas maximal.

Démonstration. Comme K est un corps, l'anneau $K[X]$ est principal, ce qui implique que (f) est un idéal maximal puisque f est irréductible. Ainsi, le quotient $L = K[X]/(f)$ est un corps par (III.1). De plus, comme l'inclusion naturelle $K \hookrightarrow K[X]$ et la projection canonique $\pi\colon K[X] \to L$ sont des homomorphismes d'anneaux, leur composition $\varphi\colon K \hookrightarrow L$ en est un également.

Ce plongement $\varphi\colon K \hookrightarrow L$ définit [11] un plongement $\varphi\colon K[X] \hookrightarrow L[X]$, ce qui permet de considérer $\varphi(f)$ comme un polynôme à coefficients dans L. Notons que si $f = \sum_i \lambda_i X^i \in K[X]$, alors on a $\varphi(f) = \sum_i \pi(\lambda_i) X^i \in L[X]$. Considérons à présent $a := \pi(X) \in L$ la classe d'équivalence du polynôme $X \in K[X]$. Comme $\pi\colon K[X] \to L$ est un homomorphisme d'anneaux de noyau (f), le polynôme $\varphi(f) \in L[X]$ satisfait

$$\varphi(f)(a) = \sum_i \pi(\lambda_i)\pi(X)^i = \pi\Big(\sum_i \lambda_i X^i\Big) = \pi(f) = 0\,,$$

et admet donc bien la racine $a \in L$. □

Au vu de la puissance de la construction de Kronecker, il serait très utile d'avoir à disposition des critères pour déterminer si un polynôme $f \in K[X]$ est irréductible. Pour des raisons évidentes, tout polynôme $f \in K[X]$ de degré 1 est irréductible, mais le quotient $K[X]/(f)$ est isomorphe à K et ne donne donc rien de nouveau (c'est un exercice). On cherche donc des polynômes $f \in K[X]$ irréductibles avec $\deg(f) > 1$.

Pour $K = \mathbb{C}$, les seuls polynômes $f \in \mathbb{C}[X]$ irréductibles sont de degré 1 : c'est une conséquence triviale du résultat classique suivant que vous connaissez. Notons que cet énoncé porte bien mal ses deux noms usuels, à savoir *Théorème fondamental de l'algèbre* et *Théorème de d'Alembert*, puisqu'il s'agit d'un résultat d'analyse, et que D'ALEMBERT n'en a donné qu'une preuve incomplète. Nous en verrons une nouvelle preuve, presque exclusivement algébrique, en Section IV.4.

JEAN LE ROND D'ALEMBERT (1717-1783)

Théorème III.10: Théorème fondamental de l'algèbre

Tout polynôme $f \in \mathbb{C}[X]$ non-constant admet une racine dans $\mathbb{C}$.

La réponse est également facile pour $K = \mathbb{R}$: un polynôme $f = aX^2 + bX + c \in \mathbb{R}[X]$ est irréductible si et seulement si $b^2 - 4ac < 0$. Dans ce cas, on montre que $\mathbb{R}[X]/(f) \simeq \mathbb{C}$, ce qui généralise le cas $f = X^2 + 1$.

Il existe également certaines méthodes pour $K = \mathbb{Q}$, que nous rappelons ici.

GOTTHOLD EISENSTEIN (1823-1852)

Proposition III.11 (critère d'Eisenstein)**.** *Soit $f = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$ un polynôme de degré $n \geq 1$. S'il existe un premier $p \in \mathbb{N}$ tel que $p \mid a_i$ pour $i = 0, \ldots, n-1$, $p \nmid a_n$, et $p^2 \nmid a_0$, alors $f \in \mathbb{Q}[X]$ est irréductible.*

Rappelons qu'un polynôme $f \in \mathbb{Z}[X]$ (ou plus généralement $f \in A[X]$ avec A factoriel) est dit *primitif* si le plus grand commun diviseur de ses coefficients est 1 (resp. est une unité de A).

11. En général, un homomorphisme d'anneaux $\varphi\colon A \to B$ induit un unique homomorphisme d'anneaux $A[X] \to B[X]$ via $\sum_i \lambda_i X^i \mapsto \sum_i \varphi(\lambda_i) X^i$, qu'on notera par le même symbole via un léger abus de notation.

Proposition III.12 (critère de réduction). *Soit $p \in \mathbb{N}$ un premier, et notons $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ l'homomorphisme d'anneaux induit par la projection canonique. Si $f \in \mathbb{Z}[X]$ est primitif, si $\deg(\pi(f)) = \deg(f)$ et si $\pi(f) \in \mathbb{F}_p[X]$ est irréductible*[12]*, alors $f \in \mathbb{Q}[X]$ est irréductible.*

Nous terminerons cette section avec le rappel d'un dernier résultat qui, dans le cas de l'anneau des entiers $A = \mathbb{Z}$, n'est autre que le *théorème fondamental de l'arithmétique*.

Théorème III.13

Un anneau principal A est *factoriel* : pour tout élément $a \in A \setminus (A^* \cup \{0\})$, il existe des éléments irréductibles $p_1, \dots, p_m \in A$ (pas forcéments distincts) tels que $a = p_1 \cdots p_m$, et cette décomposition est unique à l'ordre près et à multiplication par des unités près.

Ainsi, on peut exposer une "hiérarchie" des anneaux de la façon suivante :

$$\text{corps} \Rightarrow \text{euclidien} \Rightarrow \text{principal} \Rightarrow \text{factoriel} \Rightarrow \text{intègre} \Rightarrow \text{commutatif}.$$

Dans ce chapitre, nous allons donc nous concentrer sur les anneaux les plus "favorables", à savoir les corps.

III.2 Extensions de corps

Rappelons qu'un *sous-corps* K d'un corps L est un sous-anneau $K \subset L$ qui est un corps. En d'autres termes, le sous-ensemble $K \subset L$ contient 1_L, il satisfait que pour tous $a, b \in K$, on a $-a, a+b, ab \in K$ et il contient l'inverse a^{-1} de tout $a \in K \setminus \{0\}$.

Cela mène à la définition du concept central de ce chapitre.

Définition III.14

Une **extension de corps** est une paire $K \subset L$ avec K un sous-corps de L.

Cette définition appelle un certain nombre de remarques.

Remarques III.15.

1. De façon légèrement plus commode, un sous-ensemble K d'un corps L est un sous-corps si et seulement si $1_L \in K$ et on a $a - b \in K$ et $ab^{-1} \in K$ pour tous $a \in K$ et $b \in K \setminus \{0\}$. C'est un exercice.

12. Vérifier qu'un polynôme est irréductible dans $\mathbb{F}_p[X]$ peut se révéler pénible, mais à l'inverse de $\mathbb{Q}[X]$, cela ne demande qu'un temps fini.

2. De manière équivalente, une extension de corps peut être définie comme une paire de corps $K \subset L$ telle que les opérations sur K sont les restrictions des opérations sur L. C'est aussi un exercice.
3. Toute extension $K \subset L$ définit un homomorphisme de corps $K \hookrightarrow L$, à savoir l'inclusion. Réciproquement, tout homomorphisme de corps $\varphi : K \to L$ est injectif, et définit donc un isomorphisme entre K et $\varphi(K)$, qui est un sous-corps de L. On peut donc identifier K et $\varphi(K)$, et considérer tout homomorphisme de corps $\varphi : K \hookrightarrow L$ comme une extension de corps $K \subset L$.

   On aura donc tendance à identifier les extensions de corps $K \subset L$ et les homomorphismes de corps $K \to L$.
4. On utilisera parfois la notation [13] $\begin{array}{c} L \\ \vert \\ K \end{array}$ pour une extension de corps $K \subset L$.

Exemples III.16 (extensions de corps)**.**

1. La suite $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ est une suite d'extensions de corps : on parle de *tour d'extensions*.
2. Pour un corps K quelconque, considérons le corps des fractions rationnelles à coefficients dans K défini en Exemple III.4.3 :

$$K(X) \coloneqq Q(K[X]) = \left\{ \frac{f}{g} \;\middle|\; f \in K[X],\, g \in K[X] \setminus \{0\} \right\}.$$

   Le corps K est un sous-corps de $K(X)$ via $\lambda \mapsto \frac{\lambda}{1}$ (puisqu'il s'agit de la composition des homomorphismes $K \hookrightarrow K[X]$ et $K[X] \overset{i}{\hookrightarrow} Q(K[X]) = K(X)$). On obtient donc une extension de corps $K \subset K(X)$.
3. Si L est un corps de caractéristique nulle, alors il existe un unique homomorphisme de corps $\mathbb{Q} \hookrightarrow L$. Ainsi, tout corps de caractéristique nulle est une extension des rationnels.

   ⌜ Comme $\mathbb{Z}$ est un objet initial dans Ann, il existe un unique homomorphisme d'anneaux $\epsilon : \mathbb{Z} \to L$, qui est injectif puisque $\mathrm{car}(L) = 0$. Par la propriété universelle du corps des fractions, il existe un unique homomorphisme de corps $\overline{\epsilon} : \mathbb{Q} \to L$ tel que $\overline{\epsilon} \circ i = \epsilon$. De plus, comme tout homomorphisme de corps $\varphi : \mathbb{Q} \to L$ se retreint à un homomorphisme d'anneaux $\varphi \circ i : \mathbb{Z} \to L$, on a nécessairement $\varphi \circ i = \epsilon$, d'où $\varphi = \overline{\epsilon}$ par unicité. ⌟
4. Si L est un corps de caractéristique p, alors il existe un unique homomorphisme de corps $\mathbb{F}_p \hookrightarrow L$. En particulier, tout corps de caractéristique p est une extension de $\mathbb{F}_p$.

   ⌜ Il existe un unique homomorphisme d'anneaux $\epsilon : \mathbb{Z} \to L$, qui par définition de la caractéristique, a noyau $\mathrm{Ker}(\epsilon) = p\mathbb{Z}$. Par la propriété universelle du quotient, il

13. La notation L/K est aussi commune, mais ressemble trop à un quotient pour être utilisée sans source de confusion.

induit un unique homomorphisme $\overline{\epsilon}\colon \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \to L$ tel que $\overline{\epsilon} \circ \pi = \epsilon$. Le fait que tout homomorphisme $\varphi\colon \mathbb{F}_p \to L$ coïncide avec $\overline{\epsilon}$ se démontre comme ci-dessus. ⌟

5. Tout $f \in K[X]$ irréductible définit une extension de corps $K \subset L := K[X]/(f)$: c'est une reformulation de la Proposition III.9.

Il est temps de faire une remarque presque triviale (la vérification est laissée en exercice), mais de la plus haute importance.

Remarque III.17. Si $K \subset L$ est une extension de corps, alors L est un espace vectoriel sur K via $\lambda \cdot v = \lambda v$ pour tout $\lambda \in K$ et $v \in L$. (Si l'extension est obtenue par un homomorphisme de corps $\varphi\colon K \hookrightarrow L$, alors cette structure est donnée par $\lambda \cdot v = \varphi(\lambda)v$.)

Cela permet d'introduire une terminologie très naturelle.

Terminologie III.18. Le *degré* d'une extension $K \subset L$, noté $[L : K]$, est la dimension de L comme espace vectoriel sur K. Une extension $K \subset L$ est dite *finie* si son degré est fini, et *infinie* sinon.

Voici quelques exemples.

Exemples III.19 (degré d'extensions)**.**

1. Une extension $K \subset L$ n'est jamais de degré 0, puisque L contient $1_L = 1_K \neq 0_K$.
2. Une extension $K \subset L$ est de degré 1 si et seulement si $K = L$: on parle d'*extension triviale*.

   ⌜ Si $K = L$, alors $[L : K] = \dim_K(L) = \dim_K(K) = 1$. Supposons réciproquement que $[L : K] = 1$. Puisque $\lambda \cdot 1_L = 0$ avec $\lambda \in K$ implique $\lambda = 0$, la famille $\{1_L\}$ est linéairement indépendante sur K ; comme $\dim_K(L) = [L : K] = 1$, c'est une K-base de L. On a donc bien $L = \{\lambda \cdot 1_L \mid \lambda \in K\} = K$. ⌟
3. L'extension $\mathbb{R} \subset \mathbb{C}$ est de degré 2, puisque $\{1, i\}$ est une $\mathbb{R}$-base de $\mathbb{C}$.
4. L'extension $\mathbb{Q} \subset \mathbb{R}$ est infinie : c'est un exercice.
5. Pour tout corps K, l'extension $K \subset K(X)$ est infinie : cela découle du fait que la famille infinie $\{1, X, X^2, \dots\} \subset K(X)$ est libre sur K.
6. Soient $f \in K[X]$ irréductible et $K \subset L := K[X]/(f)$ l'extension de corps correspondante (Proposition III.9). Alors, le degré $[L : K]$ de l'extension est égal au degré[14] du polynôme $f \in K[X]$.

   ⌜ L'extension $K \subset L$ est donnée par la composition $K \hookrightarrow K[X] \xrightarrow{\pi} K[X]/(f)$. Ainsi, si l'on note $\pi(g) = \overline{g}$ pour $g \in K[X]$, la structure de K-espace vectoriel sur L est donnée par $\lambda \cdot \overline{g} = \overline{\lambda g}$. Nous allons vérifier que si f est de degré n, alors la famille $\{\overline{1}, \overline{X}, \overline{X}^2, \dots, \overline{X}^{n-1}\}$ est une K-base de L, ce qui montre l'affirmation.
   Commençons par l'indépendance linéaire : soient $\lambda_0, \lambda_1, \dots, \lambda_{n-1} \in K$ tels que

$$\lambda_0 \cdot \overline{1} + \lambda_1 \cdot \overline{X} + \cdots + \lambda_{n-1} \cdot \overline{X}^{n-1} = \overline{0} \in L\,.$$

14. Notons que comme f est irréductible, on a forcément $\deg(f) \geq 1$.

Cela implique que la classe de $h = \lambda_0 + \lambda_1 X + \cdots + \lambda_{n-1}X^{n-1} \in K[X]$ est nulle dans le quotient L, et donc que h est un élément de l'idéal (f) : il existe $g \in K[X]$ tel que $h = gf$. Comme $n-1 \geq \deg(h) = \deg(g)+\deg(f) = \deg(g)+n$, on a forcément $g = 0$, d'où $h = 0$, et $\lambda_i = 0$ pour tous i.

Pour montrer que cette famille est génératrice, prenons un élément quelconque $\overline{g} \in L$ avec $g \in K[X]$. Comme K est un corps et f non-nul, on peut appliquer la division euclidienne et obtenir $q, r \in K[X]$ avec $g = qf + r$ et $\deg(r) < \deg(f) = n$. Si l'on note $r = r_0 + r_1 X + \cdots + r_{n-1}X^{n-1}$, on a donc

$$\overline{g} = \overline{r} = r_0 \cdot \overline{1} + r_1 \cdot \overline{X} + \cdots + r_{n-1} \cdot \overline{X}^{n-1} \in L$$

avec $r_i \in K$, ce qui conclut la preuve. ⌟

Le cas de $f = 1 + X^2 \in \mathbb{R}[X]$ redonne bien entendu l'exemple 3 ci-dessus. On verra d'autres exemples plus tard.

Voici le premier énoncé de cette section.

Proposition III.20. *Soit $K \subset L \subset M$ une tour d'extensions. L'extension $K \subset M$ est finie si et seulement si $K \subset L$ et $L \subset M$ sont finies, auquel cas on a l'égalité*

$$[M : K] = [M : L][L : K] .$$

Démonstration. Supposons d'abord que les extensions $K \subset L$ et $L \subset M$ sont finies. Soient $\{v_1, \ldots, v_\ell\} \subset L$ une K-base de L et $\{w_1, \ldots, w_m\} \subset M$ une L-base de M. Nous allons montrer que la famille

$$\{v_i w_j \mid i = 1, \ldots, \ell,\ j = 1 \ldots, m\}$$

est une K-base de M : cela impliquera que l'extension $K \subset M$ est également finie, de degré $[M : K] = m\ell = [M : L][L : K]$.

Pour vérifier que cette famille est génératrice, prenons $x \in M$ arbitraire. Comme la famille $\{w_j\}_j$ engendre M sur L, il existe $\lambda_j \in L$ tels que $x = \sum_{j=1}^m \lambda_j w_j$. Comme la famille $\{v_i\}_i$ engendre L sur K, il existe $\mu_{ij} \in K$ tels que $\lambda_j = \sum_{i=1}^\ell \mu_{ij} v_i$ pour tout j. On obtient donc $x = \sum_{j=1}^m \sum_{i=1}^\ell \mu_{ij} v_i w_j$: cette famille engendre bien M sur K. Pour vérifier qu'elle est libre, prenons $\mu_{ij} \in K$ tels que

$$0 = \sum_{i,j} \mu_{ij} v_i w_j = \sum_{i=1}^{\ell} \underbrace{\left(\sum_{j=1}^{m} \mu_{ij} v_i \right)}_{\in L} w_j .$$

Comme la famille $\{w_j\}_j$ est libre sur L, cela implique $\sum_{j=1}^m \mu_{ij} v_i = 0$ pour tout j. Comme la famille $\{w_j\}_j$ est libre sur K, on obtient donc bien $\mu_{ij} = 0$ pour tous i, j.

Il reste à montrer que si $K \subset M$ est finie, alors $K \subset L$ et $L \subset M$ sont finies. Supposons par la contraposée que $L \subset M$ est infinie. Alors, il existe des familles libres sur L de taille finie arbitraire dans M ; comme ces familles sont également libres sur K, on aurait $K \subset M$ infinie. Similairement, si $K \subset L$ est infinie, il existe des familles libres sur K de taille finie arbitraire dans L et donc dans M, d'où $K \subset M$ infinie. □

Notation et terminologie III.21.

- Pour $K \subset L$ une extension et $S \subset L$ un sous-ensemble quelconque, posons

$$K[S] := \bigcap_{\substack{K \cup S \subset A \\ A \text{ sous-anneau de } L}} A\,, \qquad K(S) := \bigcap_{\substack{K \cup S \subset M \\ M \text{ sous-corps de } L}} M\,.$$

  Notons que $K[S]$ est le plus petit sous-anneau de L contenant $K \cup S$, tandis que $K(S)$ est le plus petit sous-corps de L contenant $K \cup S$. On appelle $K[S]$ (resp. $K(S)$) le sous-anneau (resp. sous-corps) de $K \subset L$ *engendré par* S.
- S'il existe $S \subset L$ fini tel que $L = K(S)$, l'extension $K \subset L$ est dite *de génération finie*. Si $S = \{a_1, \ldots, a_n\}$, on notera [15] $L = K(a_1, \ldots, a_n)$.
- S'il existe $S = \{a\} \subset L$ tel que $L = K(S)$, l'extension $K \subset L$ est dite *simple*, et l'on notera $L = K(a)$.

Avant de donner quelques exemples, un certain nombre de remarques s'imposent. Les vérifications des quatre premières sont laissées en exercice.

Remarques III.22. Soit $K \subset L$ une extension de corps.

1. Pour tout $S \subset L$, on a $K(S) = Q(K[S])$.
2. Pour tous $S, T \subset L$, on a $K(S)(T) = K(S \cup T)$.
3. Pour tous $a_1, \ldots, a_n \in L$,

$$K[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) \mid f \in K[X_1, \ldots, X_n]\}\,,$$

   ce qui justifie la notation. En particulier, on a l'égalité

$$K[a] = \{f(a) \mid f \in K[X]\}\,. \tag{III.3}$$

4. Pour tous $a_1, \ldots, a_n \in L$,

$$K(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \;\middle|\; f, g \in K[X_1, \ldots, X_n],\ g(a_1, \ldots, a_n) \neq 0 \right\},$$

   ce qui justifie la notation. En particulier, on a l'égalité

$$K(a) = \left\{ \frac{f(a)}{g(a)} \;\middle|\; f, g \in K[X],\ g(a) \neq 0 \right\}. \tag{III.4}$$

5. Toute extension finie est de génération finie.

   ⌜ Nous allons procéder par récurrence sur le degré $n := [L : K] \geq 1$ de l'extension finie $K \subset L$. Le départ de récurrence est trivial, puisque $n = 1$ correspond à l'extension triviale $L = K$ (Exemple III.19.2) qui est de génération finie puisque $K = K(\varnothing)$. Supposons donc $n > 1$ et l'énoncé vrai pour toute extension de degré $< n$. Comme $n = [L : K] > 1$, on a $K \subsetneq L$ par l'Exemple III.19.2 : il existe donc $a \in L \smallsetminus K$. Ainsi, l'extension $K \subset K(a)$ est non-triviale, d'où $[K(a) : K] > 1$. Par la Proposition III.20, on a donc $[L : K(a)] = \frac{n}{[K(a):K]} < n$. Par hypothèse de récurrence, il existe $S \subset L$ fini tel que $L = K(a)(S)$, qui coïncide avec $K(\{a\} \cup S)$ par la remarque 2 ci-dessus. Ainsi, l'extension $K \subset L$ est bien de génération finie. ⌟

15. au lieu de $L = K(\{a_1, \ldots, a_n\})$.

Voici enfin quelques exemples concrets de cette construction.

Exemples III.23 (Extensions simples)**.**

1. Pour $S = \varnothing$, on a trivialement $K[S] = K(S) = K$ (soit par définition, soit en utilisant (III.3) et (III.4)). De même, pour tout $S \subset K$, on a $K[S] = K(S) = K$. En particulier, l'extension triviale est (trivialement) une extension simple.
2. L'extension $\mathbb{R} \subset \mathbb{C}$ est simple, car $\mathbb{C} = \mathbb{R}(i)$. En effet, on a
$$\mathbb{R}[i] \overset{\text{(III.3)}}{=} \{f(i) \mid f \in \mathbb{R}[X]\} = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}\,,$$
d'où $\mathbb{R}(i) = Q(\mathbb{R}[i]) = Q(\mathbb{C}) = \mathbb{C}$ par la remarque 1 ci-dessus.
3. Pour tout corps K, l'extension $K \subset K(X)$ est simple. En effet, si l'on pose $S = \{X\} \subset K(X)$, les équations (III.3) et (III.4) impliquent
$$K[S] = \{f(X) \mid f \in K[X]\} = K[X]$$
et
$$K(S) = \left\{ \frac{f(X)}{g(X)} \;\middle|\; f, g \in K[X],\ g(X) \neq 0 \right\} = K(X)\,,$$
ce qui justifie également les notations.
4. Toute extension finie d'un corps fini est simple.

   ⌜ En effet, si $K \subset L$ est une extension finie (disons $[L : K] = d$) d'un corps fini K (d'ordre q), alors L est un espace vectoriel de dimension d sur K. Ainsi, l'espace vectoriel L isomorphe à K^q et donc d'ordre q^d ; en particulier, le corps L est fini. Par le Théorème III.1, le groupe L^* est cyclique : si on note $a \in L^*$ un générateur, on a $L \subset K[a] \subset K(a)$, d'où $L = K(a)$ une extension simple de K. ⌟
5. Pour tous corps K et $f \in K[X]$ irréductible, l'extension $K \subset L = K[X]/(f)$ est simple, car $L = K(a)$ avec $a \in K[X]/(f)$ la classe d'équivalence du polynôme $X \in K[X]$.

   ⌜ Rappelons qu'en Exemple III.19.6, on a montré que $L = K[X]/(f)$ est un K-espace vectoriel de base $\{1, a, a^2, \ldots, a^{n-1}\}$, avec $n = \deg(f)$. On obtient donc les inclusions
$$L \subset \{g(a) \mid g \in K[X]\} \overset{\text{(III.3)}}{=} K[a] \subset K(a)\,,$$
   d'où $L = K(a)$ comme annoncé. ⌟

   Notons qu'on a également montré en Proposition III.9 que $a \in L$ est une racine du polynôme f. Ainsi, la construction de l'extension $L = K[X]/(f)$ peut (et doit) être vue comme *l'adjonction à K d'une racine de f*. Bien entendu, cette grande classe d'exemples généralise l'exemple 2 ci-dessus.
6. Dans $\mathbb{Q} \subset \mathbb{R}$, considérons l'extension simple $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$. Nous allons maintenant montrer que
$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}\}\,.$$

⌜ Comme la seconde égalité découle de (III.3), il nous suffit de montrer que l'anneau $\mathbb{Q}[\sqrt{2}] = \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}\}$ est un corps : on aura alors bien $\mathbb{Q}(\sqrt{2}) = Q(\mathbb{Q}[\sqrt{2}]) = \mathbb{Q}[\sqrt{2}]$. Pour ce faire, considérons un élément non-nul $\alpha + \beta\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, et vérifions qu'il possède un inverse multiplicatif dans $\mathbb{Q}[\sqrt{2}]$. Un calcul direct montre que

$$\frac{\alpha}{\alpha^2 - 2\beta^2} - \frac{\beta}{\alpha^2 - 2\beta^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

fait l'affaire ; notons qu'on a bien $\alpha^2 - 2\beta^2 \neq 0$ car $(\alpha, \beta) \neq (0, 0)$ par hypothèse, et $\sqrt{2}$ est irrationnel. ⌟

Il semble à première vue étonnant que l'anneau $\mathbb{Q}[\sqrt{2}]$ soit un corps : c'est en réalité un cas particulier d'un phénomène très fréquent (voir Corollaire III.27). Notons également que l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ est obtenue en adjoignant à $\mathbb{Q}$ une racine du polynôme irréductible $f = X^2 - 2 \in \mathbb{Q}[X]$. Ainsi, cet exemple devrait se comprendre comme un nouveau cas particulier de l'exemple 5 ci-dessus. Et effectivement, l'homomorphisme $\mathbb{Q}[X] \to \mathbb{Q}[\sqrt{2}]$, $g \mapsto g(\sqrt{2})$ induit un isomorphisme $\mathbb{Q}[X]/(X^2 - 2) \simeq \mathbb{Q}(\sqrt{2})$: cela découlera de résultats plus généraux (Proposition III.25), voir Exemple III.28.3.

7. L'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ est simple, car $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$: c'est un exercice.
8. L'extension $\mathbb{Q} \subset \mathbb{R}$ n'est pas de génération finie (et donc pas simple) : c'est un autre exercice.

Nous terminons cette section avec une dernière remarque.

Remarque III.24. Comme vous l'aurez remarqué, le seul exemple d'extension non-simple que nous avons donné est une extension infinie. Il est en fait difficile de construire des extensions finies qui ne sont pas simple, en raison du *théorème de l'élément primitif* : si K est un corps de caractéristique nulle ou un corps fini, alors toute extension finie de K est simple. Nous verrons une preuve de ce résultat en Section IV.4.

III.3 Extensions simples

Comme on l'a vu ci-dessus, les extensions simples sont légion. De plus, toute extension de génération finie $K \subset K(a_1, a_2, \ldots, a_n)$ peut être exprimée comme une tour d'extensions simples via la Remarque III.22.1 :

$$K \subset K(a_1) \subset K(a_1)(a_2) \subset \cdots \subset K(a_1)(a_2)\cdots(a_n) = K(a_1, a_2, \ldots, a_n). \quad \text{(III.5)}$$

Nous allons donc nous intéresser aux extensions simples, qui sont en réalité faciles à classifier : elles sont toutes de la forme des Exemples III.23.3 ou III.23.5. Voici l'énoncé précis.

Proposition III.25. *Soit $K \subset K(a)$ une extension simple.*

- *Si $K \subset K(a)$ est infinie, alors $K(a)$ est isomorphe au corps des fractions rationnelles $K(X)$.*
- *Si $K \subset K(a)$ est finie, alors il existe un unique polynôme irréductible unitaire $f \in K[X]$ tel que $K(a) \simeq K[X]/(f)$. De plus, le polynôme f est de degré $[K(a) : K]$, et c'est le polynôme unitaire de degré minimal dans $K[X]$ tel que $f(a) = 0$.*

Démonstration. Soit $K \subset K(a)$ une extension simple, et soit $\epsilon : K[X] \to K(a)$ l'homomorphisme d'évaluation donné par $\epsilon(g) = g(a)$. Par le théorème d'isomorphisme et (III.3), il induit un isomorphisme

$$K[X]/\mathrm{Ker}(\epsilon) \xrightarrow{\simeq} K[a] \subset K(a)\,.$$

Comme $K(a)$ est intègre, l'anneau $K[a]$ l'est aussi, de même que $K[X]/\mathrm{Ker}(\epsilon)$ par l'isomorphisme ci-dessus. Par (III.1), l'idéal $\mathrm{Ker}(\epsilon)$ est premier.

Supposons tout d'abord que $\mathrm{Ker}(\epsilon) = \{0\}$. Dans ce cas, on a un isomorphisme $\epsilon : K[X] \xrightarrow{\simeq} K[a]$. Par fonctorialité (Remarque III.3.4), cela induit un isomorphisme entre les corps des fractions correspondants, à savoir

$$K(X) = Q(K[X]) \simeq Q(K[a]) = K(a)$$

par la Remarque III.22.1. Puisque l'extension $K \subset K(X)$ est infinie (comme montré en Exemple III.19.5), il en va de même [16] pour l'extension $K \subset K(a)$.

Supposons à présent $\mathrm{Ker}(\epsilon) \neq \{0\}$. Comme $K[X]$ est un anneau principal, il existe $f \in K[X]$ tel que $\mathrm{Ker}(\epsilon) = (f)$; de plus, ce polynôme est uniquement déterminé si on le suppose unitaire. Comme cet idéal est premier et non-nul, les implications (III.2) nous garantissent que f est irréductible. Comme $K[X]$ est principal, l'idéal (f) est maximal, et le quotient $K[X]/(f) \simeq K[a]$ est donc un corps. Ainsi, on a bien un isomorphisme $K[X]/(f) \simeq K[a] = K(a)$. L'égalité $\deg(f) = [K(a) : K]$ découle maintenant de l'Exemple III.19.6. Finalement, le fait que f est le polynôme unitaire de degré minimal dans $K[X]$ tel que $f(a) = 0$ découle de sa définition. □

Terminologie III.26. Dans le cas de $K \subset K(a)$ finie, l'unique polynôme irréductible unitaire $f \in K[X]$ tel que $f(a) = 0$ est appelé le *polynôme minimal* de a sur K.

Corollaire III.27. *Une extension simple $K \subset K(a)$ est finie si et seulement si $K[a] = K(a)$.*

Démonstration. Si l'extension $K \subset K(a)$ est finie, alors nous sommes dans le second cas de la Proposition III.25, dont la preuve montre que $K[a]$ est un corps, d'où $K[a] = K(a)$. Si l'extension $K \subset K(a)$ est infinie, alors nous sommes dans le premier cas de la Proposition III.25, dont la preuve montre $K[a] \simeq K[X]$. Comme $K[X] \subsetneq K(X)$, on a donc $K[a] \subsetneq K(a)$. □

16. Ou simplement : la famille infinie $\{1, a, a^2, \dots\} \subset K(a)$ est linéairement indépendante sur K puisque $\mathrm{Ker}(\epsilon) = 0$.

Exemples III.28 (extensions simples et polynômes minimaux)**.**

1. Un élément $a \in K$ a polynôme minimal $f = X - a \in K[X]$ sur K.
2. Le polynôme minimal de $i \in \mathbb{C}$ sur $\mathbb{R}$ est $X^2 + 1 \in \mathbb{R}[X]$, et l'on retrouve l'isomorphisme bien connu
$$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i] \simeq \mathbb{R}[X]/(X^2 + 1)\,.$$
(Par contre, le polynôme minimal de i sur $\mathbb{C}$ est $X - i$.)
3. Dans $\mathbb{Q} \subset \mathbb{R}$, l'élément $\sqrt{2} \in \mathbb{R}$ a polynôme minimal $f = X^2 - 2 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$. En effet, ce polynôme est bien irréductible dans $\mathbb{Q}[X]$ puisqu'il n'a pas de racine rationnelle. On obtient l'isomorphisme promis
$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] \simeq \mathbb{Q}[X]/(X^2 - 2)\,.$$
(Par contre, le polynôme minimal de $\sqrt{2}$ sur $\mathbb{R}$ est $X - \sqrt{2} \in \mathbb{R}[X]$.)
4. Plus généralement, si p est un premier et $n \geq 1$ un entier, alors $a := \sqrt[n]{p} \in \mathbb{R}$ a polynôme minimal $f = X^n - p \in \mathbb{Q}[X]$. En effet, on a clairement $f(a) = 0$, et $f \in \mathbb{Q}[X]$ est irréductible par le critère d'Eisenstein (Proposition III.11). Cela implique l'isomorphisme
$$\mathbb{Q}(\sqrt[n]{p}) = \mathbb{Q}[\sqrt[n]{p}] \simeq \mathbb{Q}[X]/(X^n - p)\,.$$
On obtient donc en particulier que le sous-anneau
$$\mathbb{Q}[\sqrt[n]{p}] = \{\alpha_0 + \alpha_1 \sqrt[n]{p} + \alpha_1(\sqrt[n]{p})^2 + \cdots + \alpha_{n-1}(\sqrt[n]{p})^{n-1} \mid \alpha_0, \ldots, \alpha_{n-1} \in \mathbb{Q}\}$$
des réels est en fait en corps. On l'avait démontré "à la main" dans le cas $n = 2$ (et $p = 2$) en Exemple III.23.6, ce qui n'était pas si difficile. Mais tenter de démontrer directement le cas $n = 3$ (et $p = 2$) sera laissé en exercice.

Nous terminons cette section avec un corollaire qui nous sera extrêmement utile par la suite, tout particulièrement en théorie de Galois.

Corollaire III.29. *Soit $K \subset L$ une extension, et soient $a, a' \in L$ deux racines d'un polynôme irréductible $f \in K[X]$. Alors, il existe un unique isomorphisme $\varphi\colon K(a) \to K(a')$ tel que $\varphi|_K = \mathrm{id}_K$ et $\varphi(a) = a'$.*

Démonstration. Soient donc $f \in K[X]$ irréductible, et a, a' deux racines de f dans une extension L de K. Par la Proposition III.25, on a des isomorphismes de corps
$$K[X]/(f) \xrightarrow{\bar{\epsilon}} K(a) \quad \text{et} \quad K[X]/(f) \xrightarrow{\bar{\epsilon}'} K(a')\,.$$
Si l'on note $\pi\colon K[X] \to K[X]/(f)$ la projection canonique, ces isomorphismes satisfont $\bar{\epsilon}(\pi(\lambda)) = \lambda = \bar{\epsilon}'(\pi(\lambda))$ pour tout $\lambda \in K$, de même que $\bar{\epsilon}(\pi(X)) = a$ et $\bar{\epsilon}'(\pi(X)) = a'$. Ainsi, l'isomorphisme $\varphi := \bar{\epsilon}' \circ (\bar{\epsilon})^{-1}\colon K(a) \to K(a')$ satisfait bien $\varphi|_K = \mathrm{id}_K$ et $\varphi(a) = a'$. L'unicité découle de (III.4) : par cette égalité, tout homomorphisme de corps φ défini sur $K(a)$ est uniquement déterminé par $\varphi|_K$ et par $\varphi(a)$. □

III.4 Extensions algébriques

La dichotomie dans la Proposition III.25 nous amène naturellement à formuler l'une des définitions les plus importantes de ce chapitre.

Définition III.30

Soit $K \subset L$ une extension. Un élément $a \in L$ est dit **algébrique** sur K si $K \subset K(a)$ est finie. Sinon, a est dit **transcendant** sur K.
Une extension $K \subset L$ est une **extension algébrique** si tout $a \in L$ est algébrique sur K.

Remarques III.31.

1. Par la Proposition III.25, un élément $a \in L$ est algébrique sur K si et seulement s'il existe $f \in K[X] \setminus \{0\}$ tel que $f(a) = 0$. Ainsi, l'élément $a \in L$ est transcendant sur K et seulement si le seul polynôme $f \in K[X]$ tel que $f(a) = 0$ est $f = 0$.
2. Si $a \in L$ est algébrique sur K (de polynôme minimal $f \in K[X]$), alors l'entier $[K(a) : K] = \deg(f) \geq 1$ est appelé le *degré* de a sur K, noté $\deg_K(a)$.
3. Par construction, si un polynôme $g \in K[X]$ satisfait $g(a) = 0$, alors g est un multiple du polynôme minimal f (i.e. f divise g dans $K[X]$).
4. Dans une tour d'extensions $K \subset L \subset M$, tout $a \in M$ algébrique sur K est également algébrique sur L, de degré $\deg_L(a) \leq \deg_K(a)$: c'est un exercice.

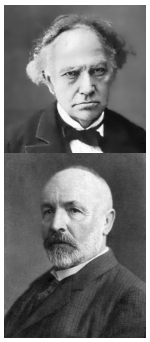
Exemples III.32 (éléments algébriques)**.**

1. Tout élément $a \in K$ est algébrique sur K, de degré 1.
   Réciproquement, si $K \subset L$ est une extension, un élément $a \in L$ algébrique sur K avec $\deg_K(a) = 1$ est racine d'un polynôme unitaire de degré 1 dans $K[X]$, donc forcément de $X - a \in K[X]$, d'où $a \in K$.
2. L'élément $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$, de degré 2.
3. Plus généralement, si p est un premier et $n \geq 1$ un entier, alors $a := \sqrt[n]{p} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$, de degré n (voir Exemple III.28.4).
4. Le nombre complexe i est algébrique sur $\mathbb{R}$, de degré 2.
5. Pour tout corps K, l'élément $X \in K(X)$ est transcendant sur K.
6. L'extension $\mathbb{Q} \subset \mathbb{R}$ est-elle algébrique ? Le premier à avoir démontré l'existence de nombres transcendants[17] fut Liouville en 1844 : plus précisément, il montra que le nombre réel

Joseph Liouville (1822-1901)

$$\sum_{j \geq 1} 10^{-j!} = 0,110001000000000000000001000...$$

est transcendant (et donc, que $\mathbb{Q} \subset \mathbb{R}$ n'est pas une extension algébrique). Le premier nombre "naturel" dont la transcendance fut établie est le nombre d'Euler $e = 2,718...$, par Hermite en 1873. (Quant à la transcendance de π,



GEORG CANTOR (1845-1918)

nous y reviendrons en Section III.5). L'année suivante, en 1874, CANTOR utilisa sa toute jeune théorie des ensembles pour démontrer l'existence d'un nombre non-dénombrable de nombres transcendants. Ce fut l'un des succès initiaux de cette théorie, devenue maintenant si classique que la preuve de ce fait peut être laissée en exercice. Notons que si e^π est transcendant, on ne sait toujours pas si les nombres $e+\pi, e\pi, \pi^e$ ou e^e sont transcendants.

Le lemme suivant nous sera utile à de multiples reprises, à commencer par la caractérisation des extensions algébriques de génération finie qui le suit immédiatement.

Lemme III.33. *Toute extension finie est algébrique. Plus précisément, si $K \subset L$ est finie, alors tout $a \in L$ est algébrique sur K, de degré $\deg_K(a) \leq [L:K]$.*

Démonstration. Soient donc $K \subset L$ une extension finie, et $a \in L$. Par la Proposition III.20 appliquée à la tour d'extensions $K \subset K(a) \subset L$, on a

$$[K(a):K] = \frac{[L:K]}{[L:K(a)]} \leq [L:K] < \infty\,,$$

ce qui démontre le lemme. □

Proposition III.34. *Soit $K \subset L = K(a_1,\ldots,a_n)$ une extension de génération finie. Sont équivalents :*

(i) $K \subset L$ est finie.

(ii) $K \subset L$ est algébrique.

(iii) Chaque a_i est algébrique sur K.

Si tel est le cas, alors on a $[L:K] \leq \prod_{i=1}^n \deg_K(a_i)$.

Démonstration. L'implication (i) ⇒ (ii) découle du Lemme III.33 (et est valide sans l'hypothèse de génération finie), tandis que (ii) ⇒ (iii) est triviale. Reste donc à montrer que si $K \subset L = K(a_1,\ldots,a_n)$ est telle que chaque a_i est algébrique sur K, alors on a $[L:K] \leq \prod_{i=1}^n \deg_K(a_i)$. Par la Proposition III.20 appliquée à (III.5), on a

$$\begin{aligned}[L:K] = [K(a_1,\ldots,a_n):K] &= \prod_{i=1}^n [K(a_1,\ldots,a_{i-1})(a_i) : K(a_1,\ldots,a_{i-1})] \\ &= \prod_{i=1}^n \deg_{K(a_1,\ldots,a_{i-1})}(a_i) \leq \prod_{i=1}^n \deg_K(a_i)\,,\end{aligned}$$

où l'inégalité finale découle de la Remarque III.31.4. □

Ce résultat n'était pas très difficile à démontrer, mais il implique le résultat tout à fait remarquable que voici : pour toute extension $K \subset L$, l'ensemble des éléments de L algébriques sur K est un corps. En particulier, si $a, b \in L$ sont algébriques sur K (i.e. sont racines de polynômes non-nuls à coefficients dans K),

17. Quand on parle d'un nombre réel, on utilise simplement la terminologie *algébrique* et *transcendant* sans préciser "sur $\mathbb{Q}$".

alors il en va de même pour $a \pm b$ et ab (pour quels polynômes ?). Grâce à la théorie patiemment développée ci-dessus, démontrer ce fait est maintenant un jeu d'enfants.

Corollaire III.35. *Pour toute extension $K \subset L$, l'ensemble*

$$\mathscr{A}_L(K) := \{a \in L \mid a \text{ est algébrique sur } K\}$$

est un sous-corps de L qui contient K.

Démonstration. On a bien entendu $\mathscr{A}_L(K) \subset L$ par définition, et $K \subset \mathscr{A}_L(K)$ puisque tout $a \in K$ est algébrique sur K. Reste donc à démontrer que $\mathscr{A}_L(K)$ est un sous-corps, i.e. que pour tous $a, b \in \mathscr{A}_L(K)$ avec $b \neq 0$, on a $a-b, ab^{-1} \in \mathscr{A}_L(K)$. Comme l'extension $K \subset K(a,b)$ est telle que a, b sont algébriques sur K, la Proposition III.34 implique qu'il s'agit d'une extension algébrique : tout élement de $K(a,b)$ est algébrique sur K. Comme $K(a,b)$ est un corps qui contient a, b il contient également $a-b$ et ab^{-1}, ce qui conclut la preuve. □

Exemple III.36 (nombres algébriques)**.** On note souvent $\overline{\mathbb{Q}}$ le corps $\mathscr{A}_{\mathbb{C}}(\mathbb{Q})$ des nombres complexes algébriques (sur $\mathbb{Q}$). Par définition, l'extension $\mathbb{Q} \subset \overline{\mathbb{Q}}$ est algébrique. Néanmoins, elle n'est pas finie, ce qui montre que la Proposition III.34 est fausse sans l'hypothèse de génération finie. En effet, le corps $\overline{\mathbb{Q}}$ contient $\sqrt[n]{2}$ pour tout $n \geq 1$, d'où $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ pour tout $n \geq 1$ (voir Exemple III.28.4)

Voici une dernière conséquence de la Proposition III.34 : la composition d'extensions algébriques est algébrique (qu'elles soient de génération finie ou pas).

Corollaire III.37. *Soient $K \subset L \subset M$ une tour d'extensions. L'extension $K \subset M$ est algébrique si et seulement si $K \subset L$ et $L \subset M$ sont algébriques.*

Démonstration. Si $K \subset M$ est algébrique, alors tout élément de M est algébrique sur K. Il suit trivialement que tout élément de M est algébrique sur L, et que tout élément de L est algébrique sur K. Ainsi, les extensions $K \subset L$ et $L \subset M$ sont également algébriques.

Supposons réciproquement que $K \subset L$ et $L \subset M$ sont algébriques, et fixons un élément $a \in M$ quelconque. Comme a est algébrique sur L, il existe un polynôme

$$f = \alpha_0 + \alpha_1 X + \cdots + \alpha_{n-1} X^{n-1} + X^n \in L[X] \setminus \{0\}$$

tel que $f(a) = 0$. Il suit que a est déjà algébrique sur le sous-corps $K(\alpha_0, \ldots, \alpha_{n-1})$ de L, puisque f a coefficients dans ce corps ; ainsi, l'extension

$$K(\alpha_0, \ldots, \alpha_{n-1}) \subset K(\alpha_0, \ldots, \alpha_{n-1}, a)$$

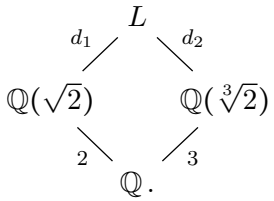
est finie. D'autre part, comme $\alpha_i \in L$ et $K \subset L$ est algébrique, chaque α_i est algébrique sur K. Par la Proposition III.34, l'extension $K \subset K(\alpha_0, \ldots, \alpha_{n-1})$ est donc finie. Par la Proposition III.20, l'extension

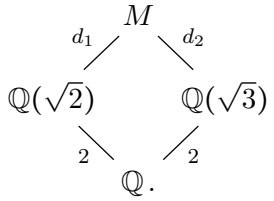
$$K \subset K(\alpha_0, \ldots, \alpha_{n-1}, a)$$

est également finie, et donc algébrique par le Lemme III.33. Par conséquent, on a bien que a est algébrique sur K, ce qui conclut la preuve. □

Nous terminons cette section avec quelques calculs explicites de degrés d'extensions algébriques. Vous en trouverez d'autres en exercices.

Exemples III.38 (degré d'extensions algébriques)**.**

1. Dans $\mathbb{Q} \subset \mathbb{C}$, considérons le corps intermédiaire $K = \mathbb{Q}(\sqrt{2}, i)$, et tentons de calculer $[K : \mathbb{Q}]$.
   Notons tout d'abord que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ puisque $X^2 - 2 \in \mathbb{Q}[X]$ est irréductible [18] et est donc le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$. Notons ensuite que $i \in K$ est de degré au plus 2 sur $\mathbb{Q}(\sqrt{2})$ puisqu'il est racine de $X^2 + 1 \in \mathbb{Q}(\sqrt{2})[X]$, mais n'est pas de degré 1 puisque $i \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. Ainsi, il est de degré 2, et l'on obtient par la Proposition III.20
   $$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4\,.$$
2. Dans $\mathbb{Q} \subset \mathbb{R}$, considérons le corps intermédiaire $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, et tentons de calculer $[L : \mathbb{Q}]$.
   Cette fois, il est judicieux de considérer les deux tours d'extensions ci-dessous :
   

   Comme illustré dans ce diagramme, on connait les degrés $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (via l'Exemple III.32.3), mais les degrés $d_1 := [L : \mathbb{Q}(\sqrt{2})]$ et $d_2 := [L : \mathbb{Q}(\sqrt[3]{2})]$ demeurent inconnus. Néanmoins, on sait que $d_1 \leq 3$ puisque $\sqrt[3]{2}$ est racine de $X^3 - 2 \in \mathbb{Q}(\sqrt{2})[X]$, et que $d_2 \leq 2$ pour une raison analogue. Comme la Proposition III.20 implique $2d_1 = [L : \mathbb{Q}] = 3d_2$, la seule solution possible est $d_1 = 3$ et $d_2 = 2$, d'où $[L : \mathbb{Q}] = 6$.
   Notons que ce résultat implique que $X^3 - 2 \in \mathbb{Q}(\sqrt{2})[X]$ est irréductible. En effet, il s'agit d'un polynôme unitaire avec racine $\sqrt[3]{2}$ et degré égal au degré $[\mathbb{Q}(\sqrt{2})(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] = 3$: c'est donc le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}(\sqrt{2})$, et il est donc irréductible. Pour une raison analogue, le polynôme $X^2 - 2 \in \mathbb{Q}(\sqrt[3]{2})[X]$ est irréductible.
3. Dans $\mathbb{Q} \subset \mathbb{R}$, considérons le corps intermédiaire $M = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, et calculons $[M : \mathbb{Q}]$.
   Cette fois, même l'étude des deux tours d'extension ci-dessous ne suffit pas :
   

18. Soit par Eisenstein avec $p = 2$, soit parce que $\sqrt{2}$ est irrationnel.

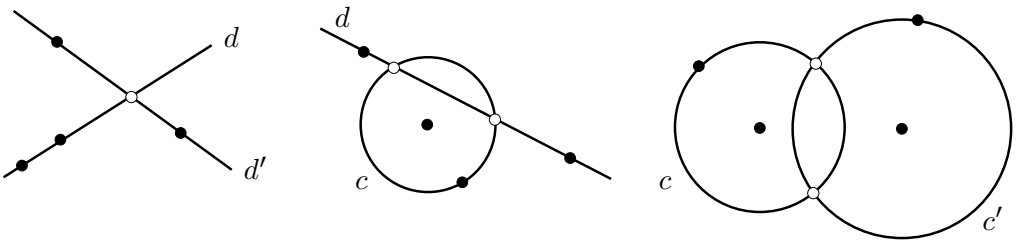


FIGURE 5 – Les éléments de S_{DD} (resp. S_{DC}, S_{CC}) obtenus comme intersection de deux droites (resp. d'une droite et d'un cercle, de deux cercles). Les points de S sont en noir, ceux de $S^+ \setminus S$ en blanc.

En effet, on calcule $[\mathbb{Q}(\sqrt{2})\mathbb{Q}] = [\mathbb{Q}(\sqrt{3})\mathbb{Q}] = 2$ et $d_1 := [M : \mathbb{Q}(\sqrt{2})] \leq 2$, $d_2 := [M : \mathbb{Q}(\sqrt{3})] \leq 2$ avec $2d_1 = 2d_2$, ce qui ne suffit pas à conclure : on peut avoir $d_1 = d_2 = 2$ ou $d_1 = d_2 = 1$. Nous allons à présent exclure ce dernier cas, ce qui impliquera donc $[M : \mathbb{Q}] = 4$ (et le fait que $X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$ et $X^2 - 2 \in \mathbb{Q}(\sqrt{3})[X]$ sont irréductibles).

⌜ Supposons par l'absurde que $d_1 = 1$, ce qui implique $\sqrt{3} \in \mathbb{Q}[\sqrt{2}]$. Il existerait donc $\alpha, \beta \in \mathbb{Q}$ tels que $\sqrt{3} = \alpha + \beta\sqrt{2}$, d'où $3 = \alpha^2 + 2\beta^2 + 2\alpha\beta\sqrt{2}$. Si $\alpha\beta \neq 0$, on aurait $\sqrt{2} = \frac{3-\alpha^2-2\beta^2}{2\alpha\beta} \in \mathbb{Q}$, une contradiction. Ainsi, soit $\beta = 0$, soit $\alpha = 0$. Le premier cas mène à $\sqrt{3} = \alpha \in \mathbb{Q}$, et le second à $\sqrt{3/2} = \beta \in \mathbb{Q}$: tous deux sont impossibles, puisqu'Eisenstein appliqué à $X^2 - 3 \in \mathbb{Q}[X]$ et à $2X^2 - 3 \in \mathbb{Q}[X]$ montre que ces polynômes de degré 2 sont irréductibles, et donc que leurs racines $\sqrt{3}$ et $\sqrt{3/2}$ sont irrationnelles. ⌟

III.5 Constructions à la règle et au compas

Le but de cette section est de donner une application spectaculaire de la théorie des extensions de corps : une caractérisation algébrique des points constructibles à la règle et au compas à partir d'un sous-ensemble donnés de points. Une conséquence immédiate en sera l'impossibilité de trois grands problèmes de l'Antiquité. Nous en verrons une autre, moins directe, en Section IV.3 : la caractérisation des polygones réguliers constructibles à la règle et au compas.

Bien évidemment, il s'agit dans un premier temps de formaliser la notion de *constructible à la règle et au compas*. Pour S un sous-ensemble quelconque du plan, posons

$$S^+ := S \cup S_{DD} \cup S_{DC} \cup S_{CC} ,$$

avec les notations suivantes, illustrées en Figure 5 :

- S_{DD} est l'ensemble des points de la forme $z \in d \cap d'$ avec d, d' deux droites non-parallèles contenant chacune au moins deux points de S ;
- S_{DC} l'ensemble des points de la forme $z \in d \cap c$ avec d une droite contenant au moins deux points de S et c un cercle de centre dans S et contenant au moins un point de S ;

- S_{CC} l'ensemble des points de la forme $z \in c \cap c'$ avec c, c' deux cercles de centres distincts dans S et contenant chacun au moins un point de S.

Posons encore $S(0) \coloneqq S$, $S(n+1) \coloneqq S(n)^+$ pour tout $n \geq 0$: l'ensemble $S(n)$ est constitué des points du plan constructibles à la règle et au compas à partir de S en au plus n pas. Finalement, on pose

$$\mathscr{C}(S) \coloneqq \bigcup_{n \geq 0} S(n)\,,$$

l'ensemble des points du plan constructibles à la règle et au compas (en un nombre fini de pas) à partir de S.

Remarques III.39.

1. Si S compte au plus 1 point, alors $\mathscr{C}(S) = S$: en effet, on a besoin d'au moins 2 points pour pouvoir construire quoi que ce soit. On supposera donc $|S| \geq 2$ dans la suite de cette section.
2. À l'aide de deux points distincts $\{A, B\} \subset S$, on construit facilement à la règle et au compas un repère orthonormé dans lequel $A = (0,0)$ et $B = (1,0)$. On peut donc identifier le plan avec le plan complexe $\mathbb{C}$ et supposer $\{0,1\} \subset S$.
3. Pour un sous-ensemble $S \subset \mathbb{C}$, on notera $\overline{S} = \{\overline{z} \mid z \in S\}$.

La preuve du lemme suivant repose sur des constructions explicites vues en GÉOMÉTRIE I : elle est laissée en exercice.

Lemme III.40. *Pour tout $S \subset \mathbb{C}$ contenant $\{0,1\}$, l'ensemble $\mathscr{C}(S)$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}(S \cup \overline{S})$: en d'autres termes, on a une tour d'extensions*

$$\mathbb{Q}(S \cup \overline{S}) \subset \mathscr{C}(S) \subset \mathbb{C}\,.$$

De plus, $z \in \mathscr{C}(S)$ implique[19] *$\overline{z}, \sqrt{z} \in \mathscr{C}(S)$.* □

Voici une première caractérisation de $\mathscr{C}(S)$.

Proposition III.41. *Si $S \subset \mathbb{C}$ contient $\{0,1\}$, alors $\mathscr{C}(S)$ est le plus petit sous-corps K de $\mathbb{C}$ tel que :*

(i) $S \subset K$,

(ii) $z \in K \Rightarrow \sqrt{z} \in K$,

(iii) $z \in K \Rightarrow \overline{z} \in K$.

Démonstration. Par le Lemme III.40, on sait que $\mathscr{C}(S)$ est un sous-corps de $\mathbb{C}$ qui satisfait ces trois conditions ; reste à voir que c'est le plus petit. Soit donc $K \subset \mathbb{C}$ un sous-corps satisfaisant (i), (ii) et (iii) : montrons l'inclusion $\mathscr{C}(S) \subset K$.

Commençons par trois observations. Premièrement, pour $z = x + iy \in \mathbb{C}$ avec $x, y \in \mathbb{R}$, on a

$$z = x + iy \in K \Leftrightarrow x, y \in K\,. \qquad (*)$$

19. Formellement, la racine carrée n'est définie qu'au signe près, mais si un corps contient une racine $\sqrt{z}$, il contient également l'autre $-\sqrt{z}$.

⌜ En effet, comme K est un corps, il contient -1, et donc $i = \sqrt{-1}$ par la condition (ii). Ainsi, si K contient x et y, il contiendra alors $x + iy$. Supposons réciproquement que K contient z ; par la condition (iii), il contient alors $\overline{z}$, et donc $\frac{1}{2}(z+\overline{z}) = x$ et $\frac{1}{2i}(z-\overline{z}) = y$ puisque K est un corps. ⌟

Voici la deuxième observation : si d est une droite contenant au moins deux points de K, alors son équation est de la forme $ax + by + c = 0$ avec $a, b, c \in K$ et $(a, b) \neq (0, 0)$.

⌜ Si d contient les points distincts $z_0 = x_0 + iy_0$ et $z_1 = x_1 + iy_1$ de K, alors son équation est $(x - x_0)(y_1 - y_0) = (x_1 - x_0)(y - y_0)$, avec $x_0, x_1, y_0, y_1 \in K$ par $(*)$. Il s'agit donc bien d'une équation de la forme $ax + by + c = 0$ avec $a, b, c \in K$ puisque K est un corps, et $(a, b) = (y_1 - y_0, x_0 - x_1) \neq (0, 0)$ puisque z_0 et z_1 sont distincts. ⌟

Voici la troisième observation : si c est un cercle de centre dans K contenant au moins un point de K, alors son équation est de la forme $x^2 + y^2 + dx + ey + f = 0$ avec $d, e, f \in K$ et (d, e) déterminé par le centre du cercle.

⌜ Si c est de centre $z_0 = x_0 + iy_0 \in K$ et contient $z_1 = x_1 + iy_1 \in K$, alors son équation est $(x - x_0)^2 + (y - y_0)^2 = (x_1 - x_0)^2 + (y_1 - y_0)^2$, avec $x_0, x_1, y_0, y_1 \in K$ par $(*)$. Il s'agit d'une équation de la forme $x^2 + y^2 + dx + ey + f = 0$ avec $d, e, f \in K$ puisque K est un corps, et $(d, e) = -2(x_0, y_0)$ déterminé par z_0. ⌟

À l'aide de ces observations, nous allons montrer l'inclusion $S(n) \subset K$ pour tout $n \geq 0$; on aura alors $\mathscr{C}(S) = \bigcup_{n\geq 0} S(n) \subset K$, ce qui terminera la démonstration. Procédons par récurrence sur $n \geq 0$, la condition (i) donnant le départ de la récurrence $S(0) = S \subset K$. Supposons donc $S(n) \subset K$ pour un certain $n \geq 0$, et soit $z \in S(n+1) = S(n)^+ = S(n) \cup S(n)_{DD} \cup S(n)_{DC} \cup S(n)_{CC}$. Il s'agit de vérifier que $z \in K$.

- Si $z \in S(n)$, alors $z \in K$ par l'hypothèse de récurrence $S(n) \subset K$.
- Si $z \in S(n)_{DD}$, alors par définition $z \in d \cap d'$ avec d, d' deux droites non-parallèles contenant chacune au moins deux points de $S(n) \subset K$. Ainsi, par la deuxième observation ci-dessus, le point $z = x + iy$ est l'unique solution d'un système d'équations (linéaires) de la forme

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases}$$

  avec $a, b, c, a', b', c' \in K$. Par l'algèbre linéaire, on a $\left|\begin{smallmatrix} a & b \\ a' & b' \end{smallmatrix}\right| = ab' - a'b \neq 0$ et les réels x, y appartiennent à K puisque c'est un corps, d'où $z \in K$ par $(*)$.
- Si $z \in S(n)_{DC}$, alors $z \in d \cap c$ avec d une droite contenant au moins deux points de $S(n) \subset K$ et c un cercle de centre en $S(n) \subset K$ contenant au moins un point de $S(n) \subset K$. Par les deuxième et troisième observations ci-dessus, le point $z = x + iy$ est une solution d'un système d'équations de la forme

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + dx + ey + f = 0 \end{cases} \qquad (**)$$

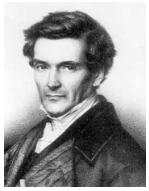
avec $a, b, c, d, e, f \in K$ et $(a, b) \neq (0, 0)$. Si $b \neq 0$, alors on a $y = -b^{-1}(ax+c)$; dans ce cas, x est solution d'une équation quadratique à coefficients dans K ; par la formule de Viète et la condition (ii), on a $x \in K$, d'où $y = -b^{-1}(ax + c) \in K$ et $z \in K$ par $(*)$. Si $b = 0$, alors $a \neq 0$ et l'on obtient la même conclusion en échangeant les rôles de x et de y.

- Finalement, si $z \in S(n)_{CC}$, alors $z \in c \cap c'$ avec c, c' deux cercles distincts avec centres dans S et contenant chacun au moins un point de $S(n) \subset K$. Par la troisième observation, $z = x + iy$ est une solution d'un système d'équations de la forme
$$\begin{cases} x^2 + y^2 + dx + ey + f = 0 \\ x^2 + y^2 + d'x + e'y + f' = 0 \end{cases}$$
avec $d, e, f, d', e', f' \in K$. Ce système est équivalent [20] au système
$$\begin{cases} x^2 + y^2 + dx + ey + f = 0 \\ (d - d')x + (e - e')y + (f - f') = 0 \end{cases}$$
avec $(d - d', e - e') \neq (0, 0)$ car les centres des cercles sont distincts. On se retrouve donc dans la même situation qu'en $(**)$ ci-dessus, d'où $z \in K$.

On a donc bien $S(n+1) \subset K$, ce qui conclut la preuve. □

Nous aurons encore besoin d'un petit résultat, dont la preuve est un exercice.

Lemme III.42. *Si $K \subset L$ est une extension de degré 2 avec $\mathrm{car}(K) \neq 2$, alors il existe $a \in L$ avec $L = K(a)$ et $a^2 \in K$.* □



Pierre-Laurent Wantzel (1814-1848)

Voici enfin le théorème principal de cette section, traditionnellement attribué à Pierre-Laurent Wantzel.

Théorème III.43: Théorème de Wantzel

Soit $S \subset \mathbb{C}$ contenant $\{0, 1\}$. Alors, un point $z \in \mathbb{C}$ appartient à $\mathscr{C}(S)$ si et seulement s'il existe un entier $n \geq 0$ et une tour d'extensions
$$\mathbb{Q}(S \cup \overline{S}) =: K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$$
avec $[K_i : K_{i-1}] = 2$ pour tout $i = 1, \ldots, n$ et $z \in K_n$.

Démonstration. Supposons dans un premier temps qu'il existe une tour d'extensions comme dans l'énoncé, et montrons l'inclusion $K_n \subset \mathscr{C}(S)$ par récurrence sur $n \geq 0$. Le départ de la récurrence est clair, puisque $K_0 = \mathbb{Q}(S \cup \overline{S}) \subset \mathscr{C}(S)$ par le Lemme III.40. Supposons donc $K_i \subset \mathscr{C}(S)$ pour un certain $i \geq 0$, et considérons K_{i+1}. Comme $[K_{i+1} : K_i] = 2$, le Lemme III.42 nous assure qu'il

20. Cette transformation correspond géométriquement à remplacer l'un des deux cercles par l'unique droite passant par les points d'intersection des deux cercles.

existe $a \in K_{i+1}$ avec $K_{i+1} = K_i(a)$ et $a^2 \in K_i \subset \mathscr{C}(S)$. Par le Lemme III.40 appliqué à $z = a^2 \in \mathscr{C}(S)$, on a $\sqrt{z} = a \in \mathscr{C}(S)$. Comme $K_i \subset \mathscr{C}(S)$ et $a \in \mathscr{C}(S)$, on a bien $K_{i+1} = K_i(a) \subset \mathscr{C}(S)$, ce qui conclut la preuve de cette implication.

Pour montrer l'autre implication, notons Ω l'ensemble des $z \in \mathbb{C}$ tels qu'il existe une tour d'extensions $K_0 \subset \cdots \subset K_n$ avec $[K_i : K_{i-1}] = 2$ pour $i = 1, \ldots, n$ et $z \in K_n$. Il nous faut vérifier que $\Omega \subset \mathbb{C}$ est un sous-corps qui satisfait aux propriétés (i), (ii) et (iii) de la Proposition III.41 ; en effet, cette même proposition impliquera alors l'inclusion $\mathscr{C}(S) \subset \Omega$.

Vérifions tout d'abord que Ω est bien un sous-corps de $\mathbb{C}$. On a bien $1 \in \Omega$, puisque $1 \in K_0 \subset \Omega$ (via la tour avec $n = 0$). Soient donc $a, b \in \Omega$ avec $b \neq 0$. Par définition de Ω et le Lemme III.42 (appliqué n fois), il existe $a_1, \ldots, a_n$ tels que

$$K_0 \subset K_0(a_1) \subset K_0(a_1, a_2) \subset \cdots \subset K_0(a_1, \ldots, a_n) \ni a$$

avec $a_i^2 \in K_0(a_1, \ldots, a_{i-1})$ pour tout $i = 1, \ldots, n$. De même, il existe $b_1, \ldots, b_m$ tels que

$$K_0 \subset K_0(b_1) \subset K_0(b_1, b_2) \subset \cdots \subset K_0(b_1, \ldots, b_m) \ni b$$

avec $b_j^2 \in K_0(b_1, \ldots, b_{j-1})$ pour tout $j = 1, \ldots, m$. Considérons la tour d'extensions

$$K_0 \subset K_0(a_1) \subset \cdots \subset K_0(a_1, \ldots, a_n) \subset K_0(a_1, \ldots, a_n, b_1) \subset \ldots$$
$$\ldots \subset K_0(a_1, \ldots, a_n, b_1, \ldots, b_m) =: L \ni a, b\,.$$

Notons que chaque extension de cette tour est de degré 1 ou 2, puisqu'on adjoint un élément dont le carré est dans le corps précédent. Il en résulte l'inclusion $L \subset \Omega$. Comme $a, b \in L$ qui est un corps, on a $a - b \in L$ et $ab^{-1} \in L$. Le sous-ensemble $\Omega \subset \mathbb{C}$ est donc bien un sous-corps.

Reste à montrer que Ω vérifie les trois conditions de la Proposition III.41.

(i) On a les inclusions $S \subset \mathbb{Q}(S \cup \overline{S}) = K_0 \subset \Omega$, d'où $S \subset \Omega$.

(ii) Soit $z \in \Omega$, d'où $K_0 \subset \cdots \subset K_n$ avec $z \in K_n$ et $[K_i : K_{i-1}] = 2$ pour tout i. Posons $K_{n+1} = K_n(\sqrt{z})$. Comme $[K_{n+1} : K_n] \leq 2$, on a bien $\sqrt{z} \in \Omega$.

(iii) Soit $z \in \Omega$, d'où $K_0 \subset \cdots \subset K_n$ avec $z \in K_n$ et $[K_i : K_{i-1}] = 2$ pour tout i. Notons τ la conjugaison complexe. Comme $\tau(K_0) = K_0$, on a la tour d'extensions

$$K_0 = \tau(K_0) \subset \tau(K_1) \subset \cdots \subset \tau(K_n) \ni \tau(z) = \overline{z}$$

avec $[\tau(K_i) : \tau(K_{i-1})] = [K_i : K_{i-1}] = 2$ pour tout i, d'où $\overline{z} \in \Omega$.

Par la Proposition III.41, on a l'inclusion $\mathscr{C}(S) \subset \Omega$, ce qui conclut la preuve. □

Le corollaire suivant sera suffisant pour la plupart de nos applications (mais pas pour toutes).

Corollaire III.44. *Si $z \in \mathbb{C}$ est constructible à la règle et au compas à partir de $S \subset \mathbb{C}$, alors z est algébrique sur $K_0 = \mathbb{Q}(S \cup \overline{S})$, de degré une puissance de 2.*

Démonstration. Si $z \in \mathscr{C}(S)$, alors par le Théorème III.43, il existe une tour d'extensions $K_0 \subset \cdots \subset K_n \ni z$ avec $[K_i : K_{i-1}] = 2$ pour $i = 1, \ldots, n$. Ainsi, le degré

$$\deg_{K_0}(z) = [K_0(z) : K_0] = \frac{[K_n : K_0]}{[K_n : K_0(z)]} = \frac{2^n}{[K_n : K_0(z)]}$$

est une puissance de 2. □

Remarques III.45.

1. Attention, la réciproque de ce corollaire est fausse : il existe des nombres algébriques $z \in \mathbb{C}$ avec $\deg_{\mathbb{Q}}(z)$ une puissance de 2, mais qui ne sont pas constructibles à la règle et au compas à partir de $S = \{0, 1\}$.
2. En GÉOMÉTRIE I, vous aviez vu un lemme de la forme suivante : *Si $x \in \mathbb{R}$ est racine d'un polynôme de degré 3 dans $\mathbb{Q}[X]$ sans racine dans $\mathbb{Q}$, alors $x \notin \mathscr{C}(\{0, 1\})$*. Cet énoncé est maintenant évident : si ce polynôme n'a pas de racine rationnelle, alors il est irréductible, et donc le polynôme minimal de x. Ainsi, on a $\deg_{\mathbb{Q}}(x) = 3$, d'où $x \notin \mathscr{C}(\{0, 1\})$ par le Corollaire III.44.

Il est maintenant possible de montrer l'impossibilité des trois grands problèmes des mathématiques antiques. Pour illustrer la fascination que ces trois problèmes ont exercé sur des générations de mathématiciens, rien ne vaut ce communiqué de l'Académie des sciences de Paris datant de 1775 :

« L'Académie a pris, cette année, la résolution de ne plus examiner aucune solution des problèmes de la duplication du cube, de la trisection de l'angle ou de la quadrature du cercle, ni aucune machine annoncée comme un mouvement perpétuel. »

La duplication du cube

D'après la légende, les habitants de Délos furent victimes d'une épidémie de peste au V^e siècle avant notre ère. Ils s'en furent consulter l'oracle de Delphes pour demander le secours d'Apollon : la Pythie leur recommanda de doubler le volume de l'autel (cubique) qui était consacré à ce dieu sur l'île de Delos, d'où le nom *problème de Delos*. En termes plus prosaïques, il nous est donc donné un cube, et il s'agit de construire (à la règle et au compas, puisque les Grecs n'envisageaient pas d'autres méthodes) un cube de volume double : c'est la *duplication du cube*.

On a donc deux points $S = \{A, B\}$ à distance réciproque d (la longueur du côté du cube), et il s'agit de construire deux points à distance z tel que $z^3 = 2d^3$, i.e. $z = d\sqrt[3]{2}$. Via l'identification du plan avec $\mathbb{C}$, on a $S = \{0, 1\}$ et $d = 1$; il s'agit donc de construire $z = \sqrt[3]{2}$ (qui porte le nom de *constante de Delos* ou *constante délienne*).

Comme $S = \{0, 1\}$, on obtient $K_0 = \mathbb{Q}(S \cup \overline{S}) = \mathbb{Q}$. On sait que $\deg_{\mathbb{Q}}(z) = 3$ car $X^3 - 2 \in \mathbb{Q}[X]$ est irréductible par Eisenstein. Par le Corollaire III.44, la constante de Délos n'est pas constructible à la règle et au compas à partir de $\{0, 1\}$, et le problème de Délos n'admet pas de solution.

La trisection de l'angle

Il est extrêmement facile de bissecter un angle quelconque à la règle et au compas : c'est le sujet d'une des premières propositions du Livre I des *Éléments d'Euclide*. En revanche, de nombreux mathématiciens grecs se sont cassé les dents sur la question de la *trisection de l'angle*, à savoir de couper un angle α quelconque en trois angles $\alpha/3$. C'est bien entendu possible pour certains angles, comme par

EUCLIDE

exemple $\alpha = \pi$: la construction d'un angle $\pi/3$ constitue d'ailleurs le sujet de la Proposition I du Livre I des *Éléments*. Mais comme nous allons le voir, c'est impossible pour d'autres angles, comme $\alpha = \pi/3$.

Supposons données deux droites qui se coupent en un angle $\alpha = \pi/3$. Comme on l'a dit, deux telles droites se construisent très facilement à partir de deux points : on peut donc poser $S = \{0, 1\}$, d'où $K_0 = \mathbb{Q}$ à nouveau. On veut construire une droite passant par l'origine, d'angle $\alpha/3 = \pi/9$ avec la droite réelle. Une telle droite permettrait de construire facilement $z := \cos(\alpha/3)$. Il nous reste donc à vérifier que $z \notin \mathscr{C}(S)$.

Pour ce faire, il faut trouver son polynôme minimal sur $\mathbb{Q}$. En appliquant les formules d'addition du cosinus et du sinus, on trouve

$$1/2 = \cos(\alpha) = \cos(\alpha/3 + \alpha/3 + \alpha/3) = 4\cos^3(\alpha/3) - 3\cos(\alpha/3) = 4z^3 - 3z\,.$$

Ainsi, z est racine du polynôme $f = 8X^3 - 6X - 1 \in \mathbb{Q}[X]$. Ce polynôme est irréductible dans $\mathbb{Q}[X]$. En effet, on peut l'écrire

$$f(X) = (2X-1)^3 + 3(2X-1)^2 - 3 = g(2X-1)$$

avec $g(X) = X^3+3X^2-3$, qui est irréductible dans $\mathbb{Q}[X]$ par Eisenstein avec $p = 3$. Ainsi, on a $\deg_{\mathbb{Q}}(z) = 3$. Par le Corollaire III.44, on a bien $z \notin \mathscr{C}(S)$, et il est impossible de trisecter l'angle $\alpha = \pi/3$ à la règle et au compas.

Remarques III.46.

1. En général, on peut montrer que la trisection de l'angle α est possible à la règle et au compas si et seulement si le polynôme $4X^3 - 3X - \cos(\alpha)$ est réductible dans $\mathbb{Q}(\cos(\alpha))[X]$. C'est l'objet d'un exercice.
2. Si la trisection de l'angle est en général impossible à la règle et au compas, elle est en revanche possible avec un compas et une *règle graduée*. C'est l'objet d'un autre exercice.

La quadrature du cercle

Le troisième problème est celui qui résista le plus longtemps, à tel point qu'il donna son nom à des expressions dans de nombreuses langues [21] : étant donné un cercle, il s'agit de construire un carré de même aire.

On a deux points donné $\{A, B\}$ à distance réciproque r (le rayon du cercle), et il faut construire des points à distance z (le côté du carré) avec $z^2 = \pi r^2$. Via l'identification du plan avec $\mathbb{C}$, on a $S = \{0, 1\}$ et $r = 1$; il s'agit donc de construire $z = \sqrt{\pi}$.

Si c'était possible, on aurait $z = \sqrt{\pi} \in \mathscr{C}(S)$, d'où $z^2 = \pi \in \mathscr{C}(S)$. Par le Corollaire III.44, le nombre π serait algébrique sur $\mathbb{Q}$ (de degré une puissance de 2). Mais π est transcendant sur $\mathbb{Q}$, un résultat qui fit passer von Lindemann à la postérité en 1882, mais dont nous ne verrons pas la preuve dans ce cours. En conclusion, la quadrature du cercle est impossible.

Ferdinand von Lindemann (1852-1939)

21. "C'est la quadrature du cercle.", "To square the circle", "Jemand versucht die Quadratur des Kreises", "Cercare la quadratura del cerchio", etc.

III.6 Corps des racines

Comme on l'avait vu en Proposition III.9, tout $f \in K[X]$ irréductible définit une extension $K \subset K[X]/(f)$ telle que f admet une racine dans L. Le but de cette section est de montrer qu'en fait, tout $f \in K[X]$ admet une extension $K \subset L$ dans laquelle f se décompose complètement (en produit de facteurs linéaires) ; de plus, il existe à isomorphisme près une unique telle extension minimale. La preuve de ce résultat est assez technique, mais le jeu en vaut la chandelle, comme on le verra par la suite.

Voici la définition formelle de cette extension.

Définition III.47

Soit $f \in K[X]$. Un **corps des racines** de f sur K est une extension $K \subset L$ telle que

$$f = c(X - a_1)\cdots(X - a_d) \in L[X] \tag{III.6}$$

avec $a_1, \ldots, a_d \in L$ (pas forcément distincts), et telle que $L = K(a_1, \ldots, a_d)$.

Remarques III.48.

1. Si la condition (III.6) est satisfaite dans $L[X]$, on dit que f est *scindée* sur L.
2. Notons que comme c est le coefficient dominant de $f \in K[X]$, on a forcément $c \in K$ (et donc $c \in L$).
3. La condition $L = K(a_1, \ldots, a_d)$ est équivalente à la condition que $K \subset L$ est minimale avec la propriété (III.6), i.e. que si on a une extension intermédiaire $K \subset L' \subset L$ avec f scindée sur L', alors $L' = L$.

   ⌜ En effet, si on a $f = c(X-a_1)\cdots(X-a_d) \in L[X]$ et $f = c'(X-a'_1)\cdots(X-a'_d) \in L'[X]$ avec $L'[X] \subset L[X]$, le fait que $L[X]$ est factoriel (par le Théorème III.13) implique (que $c = c'$ et) que $a_1, \ldots, a_d$ et $a'_1, \ldots, a'_d$ coïncident à l'ordre près. Par conséquent, le corps L' contient $K \cup \{a_1, \ldots, a_d\}$ et donc $K(a_1, \ldots, a_d) = L$. Comme $L' \subset L$, on a bien l'égalité $L' = L$. Pour vérifier la réciproque, observons que $L' := K(a_1, \ldots, a_d)$ satisfait $K \subset L' \subset L$ et la propriété (III.6) (car $c \in K$) ; par hypothèse, on a donc bien $L = L' = K(a_1, \ldots, a_d)$. ⌟

Voici le résultat principal de cette section.

Théorème III.49

Tout $f \in K[X]$ admet un corps des racines sur K. De plus, ce corps est unique dans le sens suivant : si $K \subset L$ et $K \subset L'$ sont deux corps des racines de f sur K, alors il existe un isomorphisme $\Phi : L \to L'$ tel que $\Phi|_K = \mathrm{id}_K$.

Avant de montrer ce théorème, voici d'abord quelques remarques à son sujet, suivies de quelques exemples.

Remarques III.50.

1. Comme $f \in K[X]$ admet un corps des racines unique à isomorphisme près, on dira volontiers "*le* corps des racines" de f, et on le notera souvent L_f.
2. Pour $f \in K[X]$ de degré d, on verra en exercices que $[L_f : K]$ divise $d!$.
3. Pour K un sous-corps de $\mathbb{C}$, le corps des racines de $f \in K[X]$ admet une description explicite : par le théorème fondamental de l'algèbre (Théorème III.10), c'est simplement l'extension $L_f = K(a_1, \ldots, a_d)$ avec $a_1, \ldots, a_d \in \mathbb{C}$ les racines complexes de f. Mais dans le cas général (e.g. $K = \mathbb{F}_p$, $K = \mathbb{Q}(X)$,...) une telle description explicite n'est pas toujours disponible.
4. Si $f \in K[X]$ admet un corps des racines $K \subset L_f$ et $g \in K[X]$ divise f dans $K[X]$, alors on a une tour d'extensions $K \subset L_g \subset L_f$ avec L_g un corps des racines de g sur K. C'est un exercice.
5. L'isomorphisme entre deux corps des racines de f n'est en général *pas* unique. D'ailleurs, toute la théorie de Galois repose sur cette non-unicité !

Voici quelques exemples de corps des racines. Ils illustrent à quel point le corps des racines peut varier selon le polynôme et le corps de base.

Exemples III.51 (corps des racines)**.**

1. Le corps des racines d'un polynôme $f \in K[X]$ de degré ≤ 1 est l'extension trivial $K \subset K$, puisqu'un tel polynôme s'écrit $f = c$ ou $f = c(X - a_1)$ dans $K[X]$.
2. Le corps des racines de $X^2 + 1 \in \mathbb{R}[X]$ sur $\mathbb{R}$ est $\mathbb{R} \subset \mathbb{R}(i, -i) = \mathbb{R}(i) = \mathbb{C}$, extension de degré 2.
3. Plus généralement, soit $f \in K[X]$ est un polynôme de degré 2. Si $f \in K[X]$ est réductible, alors $L_f = K$; si $f \in K[X]$ est irréductible, alors $K \subset L_f$ est une extension de degré 2.

   ⌜ Posons $f = a + bX + cX^2 \in K[X]$, et notons $a_1, a_2 \in L_f$ ses deux racines (possiblement identiques). On a alors $a_1 + a_2 = -bc^{-1} \in K$, ce qui implique que si l'une des racines est dans K, alors les deux y sont. Cela correspond au cas où f est réductible, et implique $L_f = K(a_1, a_2) = K$. A l'inverse, si le polynôme $f \in K[X]$ est irréductible, alors $L_f = K(a_1, a_2) = K(a_1)$, extension de degré $[K(a_1) : K] = \deg(f) = 2$. ⌟
4. Le corps des racines de $X^4 + 1 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$ est $\mathbb{Q} \subset \mathbb{Q}(\omega)$ avec $\omega = \exp(i\pi/4)$, extension de degré 4.

   ⌜ Comme les quatre racines complexes du polynôme $f = X^4 + 1$ sont $\omega, \omega^3, \omega^5$ et ω^7, on a bien $L_f = \mathbb{Q}(\omega, \omega^3, \omega^5, \omega^7) = \mathbb{Q}(\omega)$. Pour montrer que cette extension est de degré 4, il suffit de vérifier que f est irréductible, puisqu'on a alors que f est le polynôme minimal de ω, d'où $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\omega) = \deg(f) = 4$. Cette vérification peut se faire "à la main"[22] ou en notant que $g(X) := f(X + 1) = X^4 + 6X^3 + 10X^2 + 6X + 2$ est irréductible par Eiseinstein avec $p = 2$. ⌟

22. En vérifiant que f ne se décompose pas en un produit de deux facteurs quadratiques dans $\mathbb{Q}[X]$. Notons que cela découlera également d'un résutat plus général en Section IV.3.

5. Le corps des racines de $X^3 - 2 \in \mathbb{Q}[X]$ est $\mathbb{Q} \subset \mathbb{Q}(\lambda, \mu)$ avec $\lambda = \sqrt[3]{2}$ et $\mu = \exp(2i\pi/3)$, une extension de degré 6.

   ⌜ Comme les trois racines complexes de $f = X^3 - 2$ sont $\lambda, \mu\lambda, \mu^2\lambda$, on a

   $$L_f = \mathbb{Q}(\lambda, \mu\lambda, \mu^2\lambda) = \mathbb{Q}(\lambda, \mu)\,;$$

   l'inclusion de gauche à droite est immédiate, tandis que celle de droite à gauche découle de $\mu = \frac{\mu^2\lambda}{\mu\lambda}$. Pour calculer le degré, on note que

   $$[L_f : \mathbb{Q}] = [\mathbb{Q}(\lambda)(\mu) : \mathbb{Q}(\lambda)][\mathbb{Q}(\lambda) : \mathbb{Q}] = 2 \cdot 3 = 6$$

   car $X^3 - 2 \in \mathbb{Q}[X]$ est le polynôme minimal de λ sur $\mathbb{Q}$ tandis que $X^2 + X + 1 \in \mathbb{Q}(\lambda)[X]$ est le polynôme minimal de μ sur $\mathbb{Q}(\lambda)$. En effet, ce polynôme est irréductible dans $\mathbb{Q}(\lambda)[X]$ puisque $\mathbb{Q}(\lambda) \subset \mathbb{R}$ et il n'admet pas de racine réelle. ⌟

6. Le corps des racines de $X^4 + 2 \in \mathbb{Q}[X]$ est $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt[4]{2})$, une extension de degré 8. C'est un exercice.
7. Le corps des racines de $X^3 + X^2 + 1 \in \mathbb{Q}[X]$ est une extension de degré 6 de $\mathbb{Q}$, tandis que le corps des racines de $X^3 + X^2 + 1 \in \mathbb{F}_2[X]$ est une extension de degré 3 de $\mathbb{F}_2$. C'est un autre exercice.

Nous allons finalement nous atteler à la preuve du Théorème III.49. Dans un premier temps, montrons l'existence d'un corps des racines.

Démonstration du Théorème III.49 : existence. Soit donc $f \in K[X]$; procédons par récurrence sur $d = \deg(f)$. Pour $d \leq 1$, le corps $L = K$ est un corps des racines de f sur K (voir Exemple III.51.1), ce qui vérifie le départ de récurrence. Soit donc $d = \deg(f) > 1$, et supposons l'existence d'un corps des racines établie pour tout polynôme de degré $< d$. Comme $K[X]$ est un anneau principal, il est factoriel (Théorème III.13) ; ainsi, $f \in K[X]$ se décompose en produit de facteurs irréductibles : soit p l'un de ces facteurs, et posons $M := K[X]/(p)$. Par la Proposition III.9, cela définit une extension $K \subset M$ telle que p admet une racine $a \in M$. Comme f est un multiple de p, cet élément $a \in M$ est également une racine de f, ce qui signifie que $(X - a)$ divise f dans $M[X]$. On peut donc décomposer $f = (X - a)g$ avec $g \in M[X]$ de degré $\deg(g) = \deg(f) - 1 < d$. Par hypothèse de récurrence, il existe un corps des racines $M \subset L$ de $g \in M[X]$ sur M. Comme $f = (X - a)g$, cela implique immédiatement que $K \subset L$ est un corps des racines de f sur K. □

Dans un second temps, montrons le lemme technique suivant, qui nous sera utile à de multiples occasions.

Lemme III.52. *Soient $f \in K[X]$ et $K \subset L$ un corps des racines de f sur K. Soit encore $\varphi : K \hookrightarrow L'$ un homomorphisme tel que $\varphi(f)$ est scindée sur L'. Alors, il existe un homomorphisme $\Phi : L \hookrightarrow L'$ tel que $\Phi|_K = \varphi$, i.e. tel que le diagramme suivant commute :*

$$\begin{array}{ccc} L & & \\ \cup & \searrow^{\Phi} & \\ K & \xrightarrow[\varphi]{} & L'\,. \end{array}$$

Démonstration. Soient $K \subset L$ un corps des racines de $f \in K[X]$ et $\varphi\colon K \hookrightarrow L'$ tel que $\varphi(f) \in L'[X]$ est scindée sur L'. Nous allons procéder par récurrence sur $d = \deg(f)$. Pour $d \leq 1$, on a nécessairement $L = K$: on peut alors poser $\Phi = \varphi$, et le départ de la récurrence est vérifié.

Soit donc $d = \deg(f) > 1$, et supposons l'énoncé établi pour tout polynôme de degré $< d$. Comme $K \subset L$ est un corps des racines de f, on a en particulier $f = c\prod_{i=1}^{d}(X - a_i) \in L[X]$ avec $a_i \in L$. Considérons $a_1 \in L$, qui est algébrique sur K puisque racine de $f \in K[X]$. Soit $p \in K[X]$ son polynôme minimal, qui est irréductible et donc de degré $\deg(p) \geq 1$, et divise f dans $K[X]$. Comme $\varphi\colon K \hookrightarrow L'$ induit un homomorphisme d'anneaux $\varphi\colon K[X] \hookrightarrow L'[X]$, cela implique que $\varphi(p) =: p'$ divise $\varphi(f) =: f'$ dans $L'[X]$. Par hypothèse, on a également $f' = c'\prod_{i=1}^{d}(X - a_i') \in L'[X]$ avec $a_i' \in L'$. Comme p' divise f' dans $L'[X]$ et $\deg(p') = \deg(p) \geq 1$, l'un [23] de ces a_i' est une racine de p' : via renumérotation, on peut supposer que $a_1' \in L'$ est racine de $p' \in L'[X]$.

Considérons à présent l'isomorphisme $\varphi\colon K \to \varphi(K) =: K' \subset L'$, qui induit des isomorphismes d'anneaux $\varphi\colon K[X] \to K'[X]$ et $\overline{\varphi}\colon K[X]/(p) \to K'[X]/(p')$. En composant ce dernier avec les isomorphismes de la Proposition III.25, on obtient un isomorphisme de corps

$$K(a_1) \xleftarrow{\simeq} K[X]/(p) \xrightarrow{\overline{\varphi}} K'[X]/(p') \xrightarrow{\simeq} K'(a_1') \qquad \text{(III.7)}$$

$$\widetilde{\varphi}$$

qui satisfait $\widetilde{\varphi}|_K = \varphi$ et $\widetilde{\varphi}(a_1) = a_1'$. En particulier, on a construit un isomorphisme $\widetilde{\varphi}\colon K(a_1) \to K'(a_1')$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} L & & L' \\ \cup & & \cup \\ K(a_1) & \xrightarrow{\widetilde{\varphi}} & K'(a_1') \\ \cup & & \cup \\ K & \xrightarrow[\varphi]{} & K'. \end{array}$$

Notons à présent que $K(a_1) \subset L$ est un corps des racines du polynôme $g \in K(a_1)[X]$ tel que $f = (X - a_1)g$, qui est de degré $\deg(g) = \deg(f) - 1 < d$. De plus, l'image de g via la composition $K(a_1) \xrightarrow{\widetilde{\varphi}} K'(a_1') \subset L'$ est scindée sur L'. Par hypothèse de récurrence, il existe donc un homomorphisme $\Phi\colon L \hookrightarrow L'$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} L & \xrightarrow{\Phi} & L' \\ \cup & & \cup \\ K(a_1) & \xrightarrow{\widetilde{\varphi}} & K'(a_1'). \end{array}$$

Les deux diagrammes commutatifs ci-dessus montrent que $\Phi\colon L \to L'$ satisfait bien $\Phi|_K = \varphi$. □

23. C'est dans ce choix d'une des racines de p' que réside la non-unicité de l'extension Φ.

Nous sommes à présent en mesure de conclure la preuve du Théorème III.49.

Démonstration du Théorème III.49 : unicité. Soient donc $K \subset L$ et $K \subset L'$ sont deux corps des racines de f sur K. Comme $K \subset L$ est un corps des racines et f est scindée sur L' (puisque $K \subset L'$ est également un corps des racines de f), le Lemme III.52 nous fournit un homomorphisme $\Phi\colon L \hookrightarrow L'$ tel que $\Phi|_K = \mathrm{id}_K$. Considérons l'extension intermédiaire $K \subset \Phi(L) \subset L'$: comme $f \in K[X]$ est scindée sur L, il en va de même pour $\Phi(f) = f$ sur $\Phi(L)$. Mais comme $K \subset L'$ est un corps des racines de f, on a forcément $\Phi(L) = L'$ par minimalité (Remarque III.50). Ainsi, l'homomorphisme $\Phi\colon L \hookrightarrow L'$ est surjectif, et donc bien un isomorphisme. □

Le Lemme III.52 a une autre conséquence intéressante, que voici.

Corollaire III.53. *Soit $K \subset L$ un corps des racines d'un polynôme irréductible $f \in K[X]$, et soient $a, a' \in L$ des racines de f. Alors il existe un automorphisme $\Phi\colon L \to L$ tel que $\Phi|_K = \mathrm{id}_K$ et $\Phi(a) = a'$.*

Démonstration. Fixons donc $f \in K[X]$ irréductible, et soient $a, a' \in L$ deux racines de f dans un corps des racines L. Par le Corollaire III.29, il existe un isomorphisme $\varphi\colon K(a) \to K(a')$ tel que $\varphi|_K = \mathrm{id}_K$ et $\varphi(a) = a'$. Comme L est un corps des racines de f sur $K(a)$ et comme $\varphi(f) = f$ est scindée sur L, on peut appliquer le Lemme III.52 : le plongement $K(a) \overset{\varphi}{\hookrightarrow} K(a') \subset L$ s'étend en un homomorphisme $\Phi\colon L \to L$, qui satisfait donc toujours $\Phi|_K = \mathrm{id}_K$ et $\Phi(a) = a'$. Finalement, comme Φ est injectif, il envoie l'extension finie $K \subset L$ sur l'extension finie $K = \Phi(K) \subset \Phi(L)$ de même degré ; l'inclusion $\Phi(L) \subset L$ ne peut donc pas être stricte, et on a bien $\Phi(L) = L$. □

Nous terminons cette section avec une remarque "pour votre culture".

Remarque III.54. Un corps K est dit *algébriquement clos* si tout $f \in K[X]$ de degré au moins 1 admet une racine dans K. Par exemple, les corps $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos (puisque le polynôme $f = 1 + X^2$ n'admet pas de racine réelle), tandis que le théorème fondamental de l'algèbre garantit que $\mathbb{C}$ l'est. On montre facilement que K est algébriquement clos si et seulement si tout $f \in K[X]$ est scindée sur K.

En utilisant des techniques analogues à celles de cette section, il est possible de montrer que tout corps fixé K se plonge dans un corps algébriquement clos ; de plus, il existe à isomorphisme près un unique corps minimal avec cette propriété, appelé la *clôture algébrique* de K, et habituellement noté $\overline{K}$. Par exemple, la clôture algébrique de $\mathbb{Q}$ est donnée par le corps $\overline{\mathbb{Q}} = \mathscr{A}_{\mathbb{C}}(\mathbb{Q})$ des nombres complexes algébriques[24] sur $\mathbb{Q}$, tandis que $\overline{\mathbb{R}} = \mathbb{C}$.

Néanmoins, la preuve générale de l'existence de la clôture algébrique repose sur le *théorème de Krull* (Théorème III.7), et celle de l'unicité sur le *lemme de Zorn* : elles ne sont donc pas constructives, et nous ne les verrons pas dans ce cours.

24. Ce qui justifie la notation de l'Exemple III.36.

III.7 Corps finis

Voici une application inattendue de la théorie des corps des racines développée à la section précédente : la classification des corps finis.

Commençons par un petit rappel.

Remarque III.55. Le nombre d'éléments d'un corps fini K est toujours une puissance d'un premier. En effet, on a $\mathrm{car}(K) = p$ un premier, puisque tout corps de caractéristique nulle contient le corps infini $\mathbb{Q}$ (voir Exemple III.16.3). Comme on l'a vu en Exemple III.16.4, le corps K est une extension de $\mathbb{F}_p$, et donc un $\mathbb{F}_p$-espace vectoriel. Comme K est fini, sa dimension $d := [K : \mathbb{F}_p] \geq 1$ est finie. Par la classification des espaces vectoriels de dimension finie, on a l'isomorphisme d'espaces vectoriels $K \simeq (\mathbb{F}_p)^d$, d'où en particulier $|K| = |(\mathbb{F}_p)^d| = p^d$.

La classification ne saurait donc être plus simple que ceci.

Théorème III.56: Classification des corps finis

Si K est un corps fini, alors il existe un nombre premier p et un entier $d \geq 1$ tels que $|K| = p^d$. Réciproquement, si p est un nombre premier et $d \geq 1$ un entier, alors il existe un corps à $q = p^d$ éléments, corps unique à isomorphisme près.

La démonstration de ce théorème repose sur les résultats suivants ; la preuve du premier est laissée en exercices.

Lemme III.57. *Si x, y sont deux éléments d'un corps K caractéristique p, alors $(x+y)^p = x^p + y^p \in K$.* □

La proposition suivante implique facilement le théorème de classification.

Proposition III.58. *Soit $q = p^d$ une puissance d'un nombre premier. Le corps des racines de $X^q - X \in \mathbb{F}_p[X]$ sur $\mathbb{F}_p$ est un corps à q éléments. De plus, tout corps à q éléments est un corps des racines de $X^q - X \in \mathbb{F}_p[X]$ sur $\mathbb{F}_p$.*

Démonstration du Théorème III.56. La première phrase de l'énoncé a été vérifiée en Remarque III.55. La Proposition III.58 et le Théorème III.49 assurent que pour toute puissance de premier q, il existe un corps à q éléments. Finalement, ces mêmes énoncés impliquent que ce corps est unique à isomorphisme près. □

Démonstration de la Proposition III.58. Fixons un premier p et un entier $d \geq 1$, et posons $q := p^d$. Soit L un corps des racines du polynôme $f = X^q - X \in \mathbb{F}_p[X]$ sur $\mathbb{F}_p$, qui existe par le Théorème III.49. Il s'agit de vérifier que $|L| = q$. Pour ce faire, notons

$$R := \{x \in L \mid x^q = x\} \subset L$$

l'ensemble des racines de f dans L. La dérivée de f est $f' = qX^{q-1} - 1 = -1 \in \mathbb{F}_p[X]$, sans racine dans $\mathbb{F}_p$. Cela implique [25] que toutes les racines de f sont simples,

25. Par un résultat que vous avez vu en Algèbre I, et que l'on reverra en exercices.

d'où $|R| = \deg(f) = q$. Nous allons maintenant vérifier que $R \subset L$ est un sous-corps de L. Notons tout d'abord que R contient trivialement 1_L. De plus, pour tous $x, y \in R$, une utilisation itérative du Lemme III.57 implique

$$(x-y)^q = x^q + (-1)^q y^q = x - y \in L\,,$$

en notant que $(-1)^q = -1$ pour p impair et $(-1)^q = +1 = -1$ pour $p = 2$; on a donc bien $x - y \in R$. Finalement, pour $x \in R$ et $y \in R \smallsetminus \{0\}$, on calcule

$$(xy^{-1})^q = x^q (y^q)^{-1} = xy^{-1} \in L\,,$$

d'où $xy^{-1} \in R$. Cela montre que $R \subset L$ est un sous-corps. Comme il est de caractéristique p, il contient $\mathbb{F}_p$ par l'Exemple III.16.4 ; on est donc en présence d'une extension intermédiaire $\mathbb{F}_p \subset R \subset L$ qui contient par construction toutes les racines de f dans L. Par minimalité du corps des racines, on a $R = L$, d'où $|L| = |R| = q$.

Réciproquement, soit K un corps quelconque à $q = p^d$ élements. Par la Remarque III.55, on sait que $\mathrm{car}(K) = p$, et donc que K est une extension de $\mathbb{F}_p$ (de degré d). On va vérifier que K est un corps des racines de $f = X^q - X \in \mathbb{F}_p[X]$ sur $\mathbb{F}_p$. Pour ce faire, notons que $x = 0_K \in K$ est racine de f, de même que tout $x \in K^* = K \smallsetminus \{0_K\}$: en effet, comme K^* est un groupe d'ordre $q-1$, tout $x \in K^*$ satisfait $x^{q-1} = 1_K$. Comme $|K| = q = \deg(f)$ et f est unitaire, cela implique l'égalité

$$f = \prod_{x \in K} (X - x) \in K[X]\,,$$

donc f est scindée sur K. De plus, toute extension intermédiaire $\mathbb{F}_p \subset L \subset K$ contenant les racines de f dans K contient K tout entier, et satisfait donc $L = K$. Cela implique que K est un corps des racines de f sur $\mathbb{F}_p$, et conclut la preuve. □

Remarques III.59.

1. Ainsi, pour tout q puissance de premier, il existe à isomorphisme près un unique corps à q éléments : il est noté $\mathbb{F}_q$, et appelé *le* corps à q éléments.
2. Pour $q = p$, on a bien entendu $\mathbb{F}_q = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Néanmoins, pour $q = p^d$ avec $d > 1$, il n'existe pas de représentation commode et naturelle des éléments du corps $\mathbb{F}_q$. En particulier, le corps $\mathbb{F}_q$ n'est *pas* isomorphe à l'anneau $(\mathbb{F}_p)^d$, ni à l'anneau $\mathbb{Z}/q\mathbb{Z}$, deux anneaux non-intègres.
3. Pour tout $f \in \mathbb{F}_p[X]$ irréductible, on a $\mathbb{F}_p[X]/(f) \simeq \mathbb{F}_q$ avec $q = p^{\deg(f)}$.

   ⌜ En effet, ce quotient est bien un corps (puisque f est irréductible), et une extension de degré $\deg(f)$ de $\mathbb{F}_p$ par l'Exemple III.19.6. L'isomorphisme découle donc du Théorème III.56. ⌟

   Cela permet de faire des calculs dans $\mathbb{F}_q$ en procédant via le quotient $\mathbb{F}_p[X]/(f)$. Des exemples seront traités en exercices.

Voici encore quelques conséquences du théorème de classification.

Corollaire III.60. *Soient p un nombre premier, et $d \leq e$ deux entiers positifs. Il existe une extension $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^e}$ si et seulement si d divise e.*

Démonstration. S'il existe une extension $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^e}$, alors on a une tour d'extensions $\mathbb{F}_p \subset \mathbb{F}_{p^d} \subset \mathbb{F}_{p^e}$, et la Proposition III.20 implique que $d = [\mathbb{F}_{p^d} : \mathbb{F}_p]$ divise $[\mathbb{F}_{p^e} : \mathbb{F}_p] = e$. Supposons réciproquement que $d \leq e$ sont deux entiers positifs tels que $d \mid e$. On vérifie facilement qu'alors, l'entier $p^d - 1$ divise $p^e - 1$, ce qui implique que $X^{p^d-1} - 1$ divise $X^{p^e-1} - 1$ dans $\mathbb{F}_p[X]$. Par conséquent, on a

$$(X^{p^d} - X) \mid (X^{p^e} - X)$$

dans $\mathbb{F}_p[X]$. Comme $\mathbb{F}_{p^e}$ est un corps des racines sur $\mathbb{F}_p$ du second polynôme, et $\mathbb{F}_{p^d}$ du premier (Proposition III.58), la Remarque III.50.4 implique qu'on a une tour d'extensions $\mathbb{F}_p \subset \mathbb{F}_{p^d} \subset \mathbb{F}_{p^e}$. □

Corollaire III.61. *Soit K un corps fini. Pour tout entier $n \geq 1$, il existe des polynômes irréductibles de degré n dans $K[X]$.*

Démonstration. Soit donc K un corps fini. Par le Théorème III.56, il existe un premier p et un entier $d \geq 1$ tels que $K = \mathbb{F}_{p^d}$. Pour tout entier $n \geq 1$, posons $e = dn$. Comme d divise e, le Corollaire III.60 nous garantit l'existence d'une extension $K = \mathbb{F}_{p^d} \subset \mathbb{F}_{p^e}$, de degré $\frac{e}{d} = n$. Comme il s'agit d'une extension finie d'un corps fini, on sait que c'est une extension simple (voir Exemple III.23.4) : il existe donc $a \in \mathbb{F}_{p^e}$ tel que $\mathbb{F}_{p^e} = K(a)$. Le polynôme minimal $f \in K[X]$ de a sur K est un polynôme irréductible de degré $\deg(f) = [K(a) : K] = [\mathbb{F}_{p^e} : \mathbb{F}_{p^d}] = n$. □

III.8 Extensions normales, extensions séparables

Avec comme but la théorie de Galois, il est utile de se focaliser un instant sur des extensions particulières.

La première famille est celle des extensions *normales*, dont voici la définition.

Terminologie III.62. Une extension algébrique[26] $K \subset L$ est dite *normale* si pour tout polynôme irréductible $f \in K[X]$, si f possède une racine dans L, alors f est scindée sur L.

Remarque III.63. En d'autres termes, une extension $K \subset L$ est normale si tout polynôme irréductible $f \in K[X]$ qui a une racine dans L a toutes ses racines dans L.

Exemples III.64 (extensions normales)**.**

1. Une extension triviale $K \subset K$ est normale. En effet, si $f \in K[X]$ est irréductible et admet une racine dans K, alors f est de degré 1.

26. Cette condition n'est pas unanimement retenue selon les sources, mais cela ne change presque rien à la théorie.

2. Toute extension $K \subset L$ de degré 2 est normale.

   ⌜ Soit en effet $f \in K[X]$ irréductible avec une racine $a \in L$. Il existe donc $g \in L[X]$ tel que $f = (X-a)g \in L[X]$. On a de plus $\deg(f) = [K(a) : K] \leq [L : K] = 2$, d'où $\deg(g) \leq 1$. On a donc bien une décomposition de f dans $L[X]$ en produit de (un ou deux) facteurs linéaires. ⌟

3. L'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ n'est *pas* normale, puisque le polynôme irréductible $f = X^3 - 2 \in \mathbb{Q}[X]$ possède une seule racine dans $\mathbb{Q}(\sqrt[3]{2})$.

Voici le résultat principal de cette section : une caractérisation des extensions normales, qui nous sera très utile au Chapitre IV.

Proposition III.65. *Pour $K \subset L$ une extension finie, sont équivalents :*

(i) L'extension $K \subset L$ est normale.

(ii) Il existe $f \in K[X]$ tel que L est le corps des racines de f sur K.

(iii) Si L' est un corps contenant L comme sous-corps, alors tout homomorphisme $\varphi : L \hookrightarrow L'$ tel que $\varphi|_K = \mathrm{id}_K$ satisfait $\varphi(L) = L$.

La troisième condition n'est pas facile à assimiler, et se comprend mieux à la lumière d'un exemple où elle n'est *pas* satisfaite.

Exemple III.66. Considérons à nouveau l'extension $K = \mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) = L$, qui n'est pas normale. Le polynôme irréductible $X^3 - 2 \in \mathbb{Q}[X]$ admet les trois racines $\sqrt[3]{2}, \mu\sqrt[3]{2}, \mu^2\sqrt[3]{2}$, où $\mu = \exp(2i\pi/3)$. Par le Corollaire III.29, il existe un isomorphisme

$$L = \mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\varphi} \mathbb{Q}(\mu\sqrt[3]{2}) \subset \mathbb{C} =: L'$$

tel que $\varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. On voit bien sur cet exemple que $\varphi(L) \neq L$.

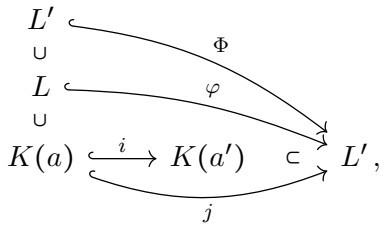
Démonstration de la Proposition III.65. Pour montrer que le premier point implique le second, supposons que $K \subset L$ est une extension finie normale. Comme c'est une extension finie, elle est de génération finie (Remarque III.22.5) et algébrique (Lemme III.33) : il existe donc $a_1, \ldots, a_n \in L$ algébriques sur K tels que $L = K(a_1, \ldots, a_n)$. Soient $f_1, \ldots f_n \in K[X]$ les polynômes minimaux de $a_1, \ldots, a_n$ sur K, respectivement, et soit $f := f_1 \cdots f_n \in K[X]$. L'extension $K \subset L$ est alors le corps des racines de f sur K. En effet, comme chaque $f_i \in K[X]$ est irréductible et $K \subset L$ normale, chaque f_i est scindé sur L, et donc $f = f_1 \cdots f_n$ également ; de plus, un corps intermédiaire $K \subset M \subset L$ sur lequel f est scindé contient nécessairement $a_1, \ldots, a_n$, d'où $M \supset K(a_1, \ldots, a_n) = L$.

Vérifions à présent que le second point implique le troisième. Soit $f \in K[X]$ tel que L est le corps des racines de f sur K. Soient L' un corps contenant L comme sous-corps, et $\varphi : L \hookrightarrow L'$ un homomorphisme tel que $\varphi|_K = \mathrm{id}_K$. Écrivons $f(X) = \sum_{i=0}^{d} \lambda_i X^i$ avec $\lambda_i \in K$, et soit $a \in L$ une racine de f. Comme $\varphi(\lambda_i) = \lambda_i$ pour tout i, on a

$$f(\varphi(a)) = \sum_{i=0}^{d} \lambda_i \varphi(a)^i = \sum_{i=0}^{d} \varphi(\lambda_i)\varphi(a)^i = \varphi\Big(\sum_{i=0}^{d} \lambda_i a^i\Big) = \varphi(f(a)) = \varphi(0) = 0\,.$$

Ainsi, l'homomorphisme $\varphi\colon L \hookrightarrow L'$ envoie toute racine de f dans L sur une racine de f dans L'. Comme $K \subset L$ est engendré par les racines de f et $\varphi(K) = K$, on a nécessairement $\varphi(L) \subset L$. Mais comme φ est injectif, il envoie l'extension finie $K \subset L$ sur l'extension finie $K = \varphi(K) \subset \varphi(L)$ de même degré. L'inclusion $\varphi(L) \subset L$ ne peut donc pas être stricte, et on a bien $\varphi(L) = L$.

Il reste à montrer que le troisième point implique le premier. Soit $f \in K[X]$ irréductible, admettant une racine $a \in L$; il faut vérifier que toutes les racines de f sont dans L. Comme observé dans la preuve de (i)⇒(ii), il existe des éléments algébriques $a_1, \dots, a_n \in L$ tels que $L = K(a_1, \dots, a_n)$; soient $f_1, \dots, f_n \in K[X]$ leurs polynômes minimaux, et soit $K \subset L'$ le corps des racines de $g := f \cdot f_1 \cdots f_n \in K[X]$. Notons l'inclusion $L \subset L'$, puisque L' contient K ainsi que les racines $a_1, \dots, a_n$ de g. Notons également que L' est corps des racines de $g \in K[X]$ sur K par définition, mais également sur $K(a)$ puisque $a \in L \subset L'$ est une racine de g. Fixons à présent une racine quelconque $a' \in L'$ de f : il reste à voir que $a' \in L$. Pour ce faire, rappelons que le Corollaire III.29 fournit un isomophisme $i\colon K(a) \to K(a')$ tel que $i|_K = \mathrm{id}_K$ et $i(a) = a'$. La composition $K(a) \overset{i}{\hookrightarrow} K(a') \subset L'$ définit donc un homomorphisme $j\colon K(a) \hookrightarrow L'$ tel que $j|_K = \mathrm{id}_K$ et $j(a) = a'$. Comme $j(g) = g$ est scindé sur L' (puisque L' est un corps des racines de $g \in K[X]$), et comme $K(a) \subset L'$ est un corps des racines de g sur $K(a)$, le Lemme III.52 implique que $j\colon K(a) \hookrightarrow L'$ s'étend en un plongement $\Phi\colon L' \hookrightarrow L'$. Soit $\varphi\colon L \hookrightarrow L'$ la restriction de Φ à L. On a donc le diagramme commutatif suivant :



avec $\varphi\colon L \hookrightarrow L'$ tel que $\varphi|_K = j|_K = \mathrm{id}_K$ et $\varphi(a) = j(a) = a'$. Par hypothèse (le troisième point), on a $\varphi(L) = L$, d'où en particulier $a' = \varphi(a) \in \varphi(L) = L$, ce qui conclut la preuve. □

Venons-en à la seconde famille d'extensions.

Terminologie III.67. • Un polynôme irréductible $f \in K[X]$ est dit *séparable* s'il n'a que des racines simples (dans un corps des racines de f sur K).

- Une extension algébrique $K \subset L$ est dite *séparable* si pour tout $a \in L$, son polynôme minimal sur K est séparable.
- Un polynôme quelconque $f \in K[X]$ est dit *séparable* si tous ses facteurs irréductibles le sont [27].

27. À ce stade, on peut légitimement se demander la raison de cette dernière définition, puisque la notion d'extension séparable n'y fait appel ; on le comprendra dans l'énoncé du Théorème IV.10.

Remarque III.68. Comme le corps des racines de f sur K est unique à isomorphisme près (Théorème III.49), la notion de séparabilité ne dépend pas du choix de ce corps des racines.

Il n'est pas évident de donner un exemple d'extension qui n'est pas séparable (on dit "inséparable"). La raison est à trouver dans le résultat suivant, qui implique immédiatement que toute extension algébrique $K \subset L$ est séparable si K est un corps de caractéristique nulle ou un corps fini.

Proposition III.69. *Si K est un corps de caractéristique nulle ou un corps fini, alors tout $f \in K[X]$ est séparable.*

Démonstration. Soit donc $f \in K[X]$ irréductible, soient $K \subset L$ son corps des racines et $a \in L$ une racine de f. Comme f est irréductible, il s'agit (à multiplication près par un élément de K^*) du polynôme minimal de a sur K.

Si a était une racine multiple de f alors[28] l'élément $a \in L$ serait également une racine de la dérivée formelle $f' \in K[X]$ de f. Comme $\deg(f') < \deg(f)$, la minimalité de f implique que $f' = 0$, ce qui est impossible en caractéristique nulle puisque $\deg(f) \geq 1$.

Supposons à présent que K est un corps fini. Par le Théorème III.56, l'extension $K \subset L$ est isomorphe à $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ pour une certaine puissance de premier $q = p^d$ et $n = [L : K]$; on peut donc identifier $K \subset L$ à $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ dans la suite. De plus, tous les éléments de $\mathbb{F}_{q^n}$ sont des racines de $g := X^{q^n} - X \in \mathbb{F}_p[X] \subset \mathbb{F}_q[X]$ (voir la preuve de la Proposition III.58). Comme a est un élément de $\mathbb{F}_{q^n}$, c'est une racine de g. Par minimalité de f, on a donc que f divise g dans $\mathbb{F}_q[X]$. Comme $g' = -1 \in \mathbb{F}_q[X]$ n'a aucune racine, le polynôme g n'a aucune racine double ; comme f divise g, le polynôme f lui non plus n'a aucune racine double. Il est donc bien séparable. □

Exemples et remarques III.70 (extensions séparables)**.**

1. Ainsi, pour trouver un polynôme inséparable $f \in K[X]$, il faut nécessairement que K soit un corps infini de caractéristique p. L'exemple le plus simple est le corps des fractions rationnelles $K = \mathbb{F}_p(Y)$.
2. On vérifiera en exercices que $f = X^p - Y \in \mathbb{F}_p(Y)[X]$ est irréductible. Comme $f' = 0$, c'est bien un polynôme inséparable.
3. Un exemple d'extension inséparable est donnée par $\mathbb{F}_p(Y^p) \subset \mathbb{F}_p(Y)$. Les détails seront vus en exercices.
4. Le *théorème de l'élément primitif*, dont il avait déjà été fait mention en Remarque III.24, peut maintenant être formulé de manière plus générale et naturelle : toute extension séparable finie est simple. Nous en verrons une preuve en Section IV.4.

28. Par un résultat que vous avez vu en Algèbre I, et que l'on a revu en exercices.

Exercices

1. Soit X un ensemble quelconque.
   (i) Vérifier que l'ensemble $\mathscr{P}(X)$ des parties de X est un anneau pour les opérations définies par
   $$X_1 + X_2 := (X_1 \cup X_2) \setminus (X_1 \cap X_2), \qquad X_1 \cdot X_2 := X_1 \cap X_2$$
   pour tous $X_1, X_2 \in \mathscr{P}(X)$.
   (ii) Montrer qu'on a un isomorphisme d'anneaux
   $$\mathscr{P}(X) \simeq (\mathbb{Z}/2\mathbb{Z})^X := \{X \xrightarrow{f} \mathbb{Z}/2\mathbb{Z}\},$$
   où la structure d'anneau sur $(\mathbb{Z}/2\mathbb{Z})^X$ est induite par celle de $\mathbb{Z}/2\mathbb{Z}$.

2. Soient A un anneau et E un monoïde. Considérons l'ensemble $A[E]$ formé des expressions de la forme
   $$\sum_{x \in E} a_x \cdot x$$
   avec $a_x \in A$ pour tout $x \in E$, et $a_x \neq 0$ pour un nombre fini de $x \in E$. Définissons des opérations sur $A[E]$ via
   $$\Big(\sum_{x\in E} a_x \cdot x\Big) + \Big(\sum_{x\in E} b_x \cdot x\Big) = \sum_{x\in E} (a_x + b_x) \cdot x$$
   $$\Big(\sum_{x\in E} a_x \cdot x\Big)\Big(\sum_{x\in E} b_x \cdot x\Big) = \sum_{x\in E} \Big(\sum_{x_1 x_2 = x} (a_{x_1} b_{x_2})\Big) \cdot x\,.$$
   (i) Montrer que cela définit une structure d'anneau sur $A[E]$.
   (ii) Pour le monoïde $\mathbb{N} = \{0, 1, 2, \dots\}$ muni de l'addition, quel est l'anneau $A[\mathbb{N}]$?

3. Vous savez que si K est un corps, alors l'anneau $K[X]$ est principal. Montrer réciproquement que si A est un anneau tel que $A[X]$ est principal, alors A est un nécessairement un corps.

4. Soit A un anneau qui contient $\mathbb{C}$ comme sous-anneau. Montrer qu'il n'existe pas d'homomorphisme d'anneaux $A \to \mathbb{R}$.

5. (i) Vérifier les détails de la preuve du Théorème III.2 : construction du corps des fractions d'un anneau intègre, et vérification de la propriété universelle correspondante.
   (ii) Montrer que cette construction définit un foncteur $\mathscr{Q}\colon \mathsf{Int} \to \mathsf{Corps}$, où Int est la catégorie des anneaux intègres et des homomorphismes d'anneaux *injectifs*.
   (iii) Vérifier qu'il existe un foncteur oubli $\mathscr{F}\colon \mathsf{Corps} \to \mathsf{Int}$, et que les foncteurs $\mathscr{Q}$ et $\mathscr{F}$ sont adjoints : pour tout anneau intègre A et tout corps K, on a une bijection naturelle
   $$\mathrm{Hom}_{\mathsf{Int}}(A, \mathscr{F}(K)) \simeq \mathrm{Hom}_{\mathsf{Corps}}(\mathscr{Q}(A), K)\,.$$

6. Vérifier que pour tout anneau A intègre, on a
   $$Q(A[X]) = Q(A)(X)\,,$$
   où $K(X)$ est le corps des fractions rationnelles à coefficients dans K.

7. Pour K un corps, vérifier qu'un polynôme de degré 2 ou 3 dans $K[X]$ est irréductible si et seulement s'il n'a pas de racine dans K.

8. (i) Montrer que si $f \in K[X]$ est de degré 1 et K un corps, alors $K[X]/(f) \simeq K$.
   (ii) Montrer que si $f \in \mathbb{R}[X]$ est irréductible de degré 2, alors $\mathbb{R}[X]/(f) \simeq \mathbb{C}$.

9. Étant donné un sous-ensemble K d'un corps L, montrer que les conditions suivantes sont équivalentes :
   (i) K est un sous-corps de L ;
   (ii) K contient 1_L et $a \in K,\ b \in K \setminus \{0\}$ implique $a - b \in K$ et $ab^{-1} \in K$;
   (iii) la restriction des deux opérations de $L \times L$ à $K \times K$ fait de K un corps.

10. (i) La catégorie Corps admet-elle un objet initial ?
    (ii) Même question pour la catégorie Corps_0 des corps de caractéristique 0.
    (iii) Même question pour la catégorie Corps_p des corps de caractéristique p.

11. Soit K un corps fixé.
    (i) Définir la catégorie Corps_K des extensions de K.
    (ii) Qu'obtient-on pour $K = \mathbb{Q}$? et pour $K = \mathbb{F}_p$?
    (iii) La catégorie Corps_K admet-elle un objet initial ?

12. Vérifier que si $K \subset L$ est une extension de corps, alors L est un espace vectoriel sur K via $\lambda \cdot v = \lambda v$ pour tout $\lambda \in K$ et $v \in L$.

13. Étant donnée une extension $K \subset L$, vérifier les énoncés suivants.
    (i) $K(S) = Q(K[S])$ pour tout $S \subset L$.
    (ii) $K(S)(T) = K(S \cup T)$ pour tous $S, T \subset L$.
    (iii) Pour tous $a_1, \ldots, a_n \in L$,
    $$K[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) \mid f \in K[X_1, \ldots, X_n]\} .$$
    (iv) Pour tous $a_1, \ldots, a_n \in L$,
    $$K(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \;\middle|\; f, g \in K[X_1, \ldots, X_n],\ g(a_1, \ldots, a_n) \neq 0 \right\} .$$

14. Montrer que toute extension de degré premier est simple.

15. (i) Montrer que si K est un corps dénombrable, alors toute extension simple de K est également dénombrable.
    (ii) Vérifier que toute extension de génération finie d'un corps dénombrable est dénombrable.
    (iii) En conclure que l'extension $\mathbb{Q} \subset \mathbb{R}$ n'est pas de génération finie.
    (iv) En déduire également que $\mathbb{Q} \subset \mathbb{R}$ n'est pas une extension finie.

16. Considérons l'extension intermédiaire de $\mathbb{Q} \subset \mathbb{R}$ donnée par $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Montrer que $\mathbb{Q} \subset L$ est en fait simple, puisque $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

17. Trouver les polynômes minimaux de :
    (i) $(\sqrt{5} + 1)/2$ dans $\mathbb{Q} \subset \mathbb{R}$, dans $\mathbb{Q} \subset \mathbb{C}$ et dans $\mathbb{R} \subset \mathbb{C}$.

(ii) $(i\sqrt{3}-1)/2$ dans $\mathbb{Q} \subset \mathbb{C}$.
(iii) $\sqrt{2}+\sqrt{3}$ dans $\mathbb{Q} \subset \mathbb{R}$.
(iv) $i\sqrt{(9+\sqrt{69})/2}$ dans $\mathbb{Q} \subset \mathbb{C}$.
(v) π dans $\mathbb{R} \subset \mathbb{C}$.

18. (i) Utiliser la théorie générale pour démontrer que pour tous entiers $m, n \geq 1$, l'anneau $\mathbb{Q}[\sqrt[n]{m}]$ est un corps.
(ii) Pour se convaincre de la puissance de cette théorie, tenter de démontrer ce fait "à la main" dans le cas particulier $m = 2$ et $n = 3$. En d'autres termes, il s'agit de montrer que l'anneau

$$\mathbb{Q}[\sqrt[3]{2}] = \{\alpha_0 + \alpha_1 \sqrt[3]{2} + \alpha_2 (\sqrt[3]{2})^2 \mid \alpha_0, \alpha_1, \alpha_2 \in \mathbb{Q}\}$$

est un corps.

19. Soient $K \subset L \subset M$ une tour d'extensions, et $a \in M$ algébrique sur K. Montrer qu'alors, a est également algébrique sur L, avec $\deg_L(a) \leq \deg_K(a)$.

20. Montrer qu'il existe un nombre non dénombrable de réels transcendants.

21. Donner deux preuves du fait que tout nombre complexe $z \in \mathbb{C}$ est algébrique sur $\mathbb{R}$: la première "à la main", la seconde en utilisant les résultats du cours.

22. (i) Montrer que si $\mathbb{C} \subset L$ est une extension algébrique, alors $L = \mathbb{C}$.
(ii) Montrer que si $\mathbb{R} \subset L$ est une extension algébrique, alors $L = \mathbb{R}$ ou L est isomorphe à $\mathbb{C}$.

23. Montrer qu'une extension $K \subset L$ est algébrique si et seulement si tout anneau A avec $K \subset A \subset L$ est un corps.

24. Soit $K \subset L$ une extension.
(i) Montrer "à la main" que si $a \in L$ est algébrique de degré n sur K (c'est-à-dire est racine d'un polynôme irréductible $f \in K[X]$ de degré n), alors $-a \in L$ est également algébrique de degré n sur K, de même que $a^{-1} \in L$ si $a \neq 0$.
(ii) Tenter de montrer "à la main" que si a et $b \in L$ sont algébriques de degré n et m sur K, respectivement, alors $a+b$ et $ab \in L$ sont également algébriques sur K, de degré au plus nm. Ensuite, démontrer ce fait en une ligne en utilisant les résultats du cours.

25. Un corps est dit *algébriquement clos* si toute extension algébrique $K \subset L$ est triviale. Vérifier que les conditions suivantes sont équivalentes.
(i) Le corps K est algébriquement clos.
(ii) Toute extension finie $K \subset L$ est triviale.
(iii) Les seuls polynômes irréductibles dans $K[X]$ sont ceux de degré 1.
(iv) Tout polynôme $f \in K[X]$ non-constant admet une racine dans K.
(v) Tout $f \in K[X]$ peut s'écrire $f = c(X-a_1)\cdots(X-a_d)$ avec $c, a_1, \ldots, a_d \in K$.

26. Vérifier qu'un corps algébriquement clos est toujours infini.

Indication. S'inspirer de la preuve d'Euclide de l'infinité des nombres premiers.

27. Soient p, q deux nombres premiers distincts.

(i) Calculer $[\mathbb{Q}(\sqrt[p]{q}, \sqrt[q]{p}) : \mathbb{Q}]$, et en conclure l'irréducibilité de $X^p - q$ dans $\mathbb{Q}(\sqrt[q]{p})[X]$.
(ii) Donner une $\mathbb{Q}$-base explicite de $\mathbb{Q}(\sqrt[p]{q}, \sqrt[q]{p})$.
(iii) Montrer que $\mathbb{Q}(\sqrt[q]{p}) \cap \mathbb{Q}(\sqrt[p]{q}) = \mathbb{Q}$.

28. Calculer les degrés des extensions suivantes de $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}), \quad \mathbb{Q}(\sqrt{6}, \sqrt{10}), \quad \mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}).$$

29. Démontrer le Lemme III.40 : pour tout sous-ensemble S du plan contenant $\{0, 1\}$, on a des extensions

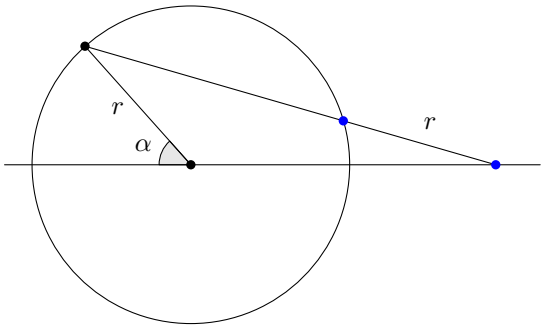
$$\mathbb{Q}(S \cup \overline{S}) \subset \mathscr{C}(S) \subset \mathbb{C}$$

telles que $z \in \mathscr{C}(S)$ implique $\overline{z}, \sqrt{z} \in \mathscr{C}(S)$.

30. Démontrer le Lemme III.42 : si $K \subset L$ est une extension de degré 2 avec $\mathrm{car}(K) \neq 2$, alors il existe $a \in L$ tel que $L = K(a)$ et $a^2 \in K$.

31. Démontrer que l'on peut trisecter n'importe quel angle à l'aide d'un compas et d'une *règle graduée* (c'est à dire, une règle avec deux points marqués dessus).

Indication. S'inspirer du dessin suivant.



32. Des extraterrestres vivant dans un monde à d dimensions souhaitent dupliquer un hypercube à la règle et au compas. Quand est-ce possible ?

33. (i) Montrer que la trisection de l'angle α est possible à la règle et au compas si et seulement si le polynôme

$$4X^3 - 3X - \cos(\alpha) \in \mathbb{Q}(\cos(\alpha))[X]$$

n'est pas irréductible.
(ii) Déterminer si les angles suivants sont trisectables ou pas : $\pi, \pi/2, \pi/3, \pi/4$.

34. Montrer que pour tout entier n tel que $\mathrm{pgcd}(3, n) = 1$, l'angle $\frac{2\pi}{n}$ est trisectable à la règle et au compas.

Indication. Utiliser le théorème de Bézout pour montrer l'existence d'entiers a, b tels que $\frac{2\pi}{3n} = a \cdot \frac{2\pi}{n} + b \cdot \frac{2\pi}{3}$.

35. Montrer que le corps des racines de $X^4 + 2 \in \mathbb{Q}[X]$ est $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt[4]{2})$, qui est une extension de degré 8.

36. Expliciter le corps des racines de $X^6 - 1 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$, ainsi que le degré de cette extension.

37. Soit $K \subset L_f$ un corps des racines de $f \in K[X]$ sur K, et soit $g \in K[X]$ qui divise f dans $K[X]$. Montrer qu'on a une tour d'extensions $K \subset L_g \subset L_f$ avec L_g un corps des racines de g sur K.

38. Soit $f \in K[X]$ de degré $d \geq 1$, et $K \subset L_f$ son corps des racines.
    (i) Montrer que $[L_f : K]$ divise $d!$.
    (ii) Vérifer que si $[L_f : K] = d!$, alors $f \in K[X]$ est irréductible.

    Indication. Énumérer les racines $a_1, \ldots, a_d \in L_f$ de f et considérer les extensions intermédiaires $L_k = K(a_1, \ldots, a_k)$.

39. Soit $\tau : L \to L$ un automorphisme d'un corps L.
    (i) Vérifier que pour tout sous-corps $K \subset L$, le sous-ensemble $\tau(K) \subset L$ est également un sous-corps de L.
    (ii) Montrer que pour toute tour $K \subset K' \subset L$, on a $[\tau(K') : \tau(K)] = [K' : K]$.

40. Considérons le polynôme $f = X^3 + X^2 + 1 \in \mathbb{Z}[X]$ et sa projection $\overline{f} \in \mathbb{F}_2[X]$.
    (i) Vérifier que $\overline{f}$ est irréductible dans $\mathbb{F}_2[X]$, et donc que f est irréductible dans $\mathbb{Q}[X]$.
    (ii) En étudiant la fonction $x \mapsto x^3 + x^2 + 1$, montrer que f possède une unique racine réelle, qui n'est pas entière.
    (iii) À l'aide des deux points précédents, déterminer le degré du corps des racines de f sur $\mathbb{Q}$.
    (iv) Montrer que si a est une racine de $\overline{f} \in \mathbb{F}_2[X]$ dans un corps de racines, alors $\{a, a^2, a^4\}$ sont des racines distinctes de $\overline{f}$.
    (v) Déterminer le degré du corps des racines de $\overline{f}$ sur $\mathbb{F}_2$, et comparer avec le point (iii).

41. Soit A un anneau intègre et $f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in A[X]$. On définit la *dérivée* de f via

$$f' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1} \in A[X] .$$

    (i) Vérifier les formules

$$(f + g)' = f' + g' , \quad (fg)' = f'g + fg' , \quad (af)' = af'$$

    pour tous $f, g \in A[X]$ et $a \in A$.
    (ii) Si $f \in A[X]$ est un polynôme non-nul et $a \in A$ une racine de f, montrer que a est une racine simple si et seulement si $f'(a) \neq 0$.

42. Montrer que si x, y sont deux éléments d'un corps K caractéristique p, alors

$$(x + y)^p = x^p + y^p \in K .$$

43. Soient $0, 1, a, b$ les éléments du corps $\mathbb{F}_4$. Écrire les tables d'addition et de multiplication de ces éléments, en suivant deux stratégies distinctes :
    (i) la stratégie *sudoku*, qui consiste à remplir les tables de l'unique façon possible ;

(ii) en réalisant $\mathbb{F}_4$ comme le quotient $\mathbb{F}_2[X]/(f)$ avec $f \in \mathbb{F}_2[X]$ un polynôme irréductible de degré 2.

44. Soit $K \subset L$ est une extension de degré 2. On a vu en Lemme III.42 (exercice 30) que si $\mathrm{car}(K) \neq 2$, alors il existe $a \in L$ tel que $L = K(a)$ et $a^2 \in K$. Donner un contre-exemple dans le cas de caractéristique 2.

45. (i) Soient $K = \mathbb{F}_q$ un corps fini, et $n \geq 1$ un entier. Montrer que la décomposition de $X^{q^n} - X$ en produits d'irréductibles dans $K[X]$ consiste en le produit de tous les polynômes unitaires irréductibles de degré d pour tout $d \geq 1$ qui divise n.
(ii) Illustrer ce fait avec des calculs explicites dans le cas de $q = 2$ et $n = 1, 2, 3, 4$.

46. À l'aide des résultats du cours, démontrer en une ligne qu'il existe un isomorphisme

$$\mathbb{F}_2[X]/(X^3 + X^2 + 1) \xrightarrow{\simeq} \mathbb{F}_2[X]/(X^3 + X + 1)\,.$$

Ensuite, trouver un isomorphisme explicite.

47. Parmi les extensions suivantes de $\mathbb{Q}$, déterminer lesquelles sont normales :

$$\mathbb{Q}(i, \sqrt[4]{2})\,, \quad \mathbb{Q}(\sqrt{2+\sqrt{2}})\,, \quad \mathbb{Q}(\sqrt{1+\sqrt{3}})\,.$$

48. Soient $K \subset E \subset L$ des extensions. Lesquels des énoncés suivants sont vrais ?
(i) Si $K \subset L$ est normale, alors $K \subset E$ est normale.
(ii) Si $K \subset L$ est normale, alors $E \subset L$ est normale.
(iii) Si $K \subset E$ et $E \subset L$ sont normales, alors $K \subset L$ est normale.

49. Montrer que $\mathbb{Q}(\sqrt[4]{2})$ n'est le corps des racines d'aucun polynôme dans $\mathbb{Q}[X]$.

50. Soit K un corps de caractéristique p. Montrer que $f = X^p - \alpha \in K[X]$ est irréductible si et seulement s'il n'existe pas de $\beta \in K$ tel que $\beta^p = \alpha$.

51. Montrer que l'extension $\mathbb{F}_p(Y^p) \subset \mathbb{F}_p(Y)$ est inséparable. Est-elle simple ?

52. Soient $K \subset E \subset L$ des extensions. Lesquels des énoncés suivants sont vrais ?
(i) Si $K \subset L$ est séparable, alors $K \subset E$ est séparable.
(ii) Si $K \subset L$ est séparable, alors $E \subset L$ est séparable.

Remarque. Il s'avère que si $K \subset E$ et $E \subset L$ sont séparables, alors $K \subset L$ est séparable, mais c'est un peu pénible à vérifier.

53. Soit K un corps de caractéristique p. Montrer que toute extension finie $K \subset L$ dont le degré n'est pas divisible par p est une extension séparable.

Chapitre IV: Théorie de Galois

Evariste Galois (1811-1832)

Nous voici enfin arrivés à ce qui constitue à n'en pas douter un des points culminants des mathématiques du XIX^{e} siècle, et le clou de vos études en algèbre : la théorie de Galois.

Comme son nom l'indique, cette théorie a été initiée par Evariste Galois, figure quasiment mythique du jeune génie au destin tragique. Notons que la formulation de cette théorie dans sa forme actuelle doit beaucoup à Emil Artin, l'un des fondateurs de l'algèbre moderne.

Emil Artin (1898-1962)

Après les bases de la théorie en Sections IV.1 et IV.2, nous pourrons passer aux nombreuses et spectaculaires applications : détermination des polygones constructibles à la règle et au compas (Section IV.3), preuves du théorème fondamental de l'algèbre et du théorème de l'élément primitif (Section IV.4), et caractérisation des équations résolubles par radicaux (Section IV.5).

IV.1 Groupes d'automorphismes et extensions galoisiennes

Rappelons que pour tout corps L, on a un groupe d'automorphismes

$$\mathrm{Aut}(L) = \{\varphi\colon L \to L \mid \varphi \text{ est un isomorphisme de corps}\}\,.$$

L'objet suivant est à la base de la théorie de Galois.

Définition IV.1

Soit $K \subset L$ une extension. Le groupe

$$\mathrm{Aut}_K(L) := \{\varphi \in \mathrm{Aut}(L) \mid \varphi|_K = \mathrm{id}_K\}$$

est appelé le **groupe des automorphismes** de l'extension $K \subset L$.

Remarques IV.2.

1. C'est un groupe pour la loi donnée par la composition des applications, ce qui se vérifie très facilement. On peut l'interpréter comme le groupe des "symétries" de l'extension $K \subset L$.
   Les notations $\mathrm{Aut}(L : K)$, $\mathrm{Aut}(K \subset L)$ et $\mathrm{Aut}(L/K)$ sont parfois utilisées.

2. Soit $f \in K[X]$ et $a \in L$ une racine de f. Comme dans la preuve de la Proposition III.65, si l'on écrit $f = \sum_{i=0}^{d} \lambda_i X^i$, on obtient

$$f(\varphi(a)) = \sum_{i=0}^{d} \lambda_i \varphi(a)^i = \sum_{i=0}^{d} \varphi(\lambda_i)\varphi(a)^i = \varphi\Big(\sum_{i=0}^{d} \lambda_i a^i\Big) = \varphi(f(a)) = \varphi(0) = 0\,.$$

Ainsi, *tout $\varphi \in \mathrm{Aut}_K(L)$ permute les racines de $f \in K[X]$ dans L*. Plus précisément, si l'on note $R := \{a \in L \mid f(a) = 0\}$ l'ensemble des racines de f dans L, on a un homomorphisme de groupes

$$\mathrm{Aut}_K(L) \longrightarrow S(R)\,, \quad \varphi \longmapsto \varphi|_R\,,$$

où $S(R)$ est le groupe des permutations de R.

3. On peut rendre la remarque précédente plus précise de la manière suivante. Supposons que $f \in K[X]$ se décompose en produit d'irréductibles $f = f_1 \cdots f_m \in K[X]$, et notons $R_i := \{a \in L \mid f_i(a) = 0\}$ pour $1 \le i \le m$. Alors, on a un homomorphisme de groupes

$$\mathrm{Aut}_K(L) \longrightarrow S(R_1) \times \cdots \times S(R_m)\,, \quad \varphi \longmapsto (\varphi|_{R_1}, \ldots, \varphi|_{R_m})\,.$$

La preuve est identique, et laissée en exercices.

4. Si $L = K(R)$, alors cet homomorphisme $\mathrm{Aut}_K(L) \to S(R)$ est injectif.

⌜ Si $L = K(R)$, tout élément de L est de la forme $\frac{g(a_1,\ldots,a_n)}{h(a_1,\ldots,a_n)}$ avec $g, h \in K[X_1, \ldots, X_n]$ et $a_1, \ldots, a_n \in R$. Ainsi, tout homomorphisme de corps $\varphi\colon L \to L$ avec $\varphi|_K = \mathrm{id}_K$ satisfait [1] $\varphi\left(\frac{g(a_1,\ldots,a_n)}{h(a_1,\ldots,a_n)}\right) = \frac{g(\varphi(a_1),\ldots,\varphi(a_n))}{h(\varphi(a_1),\ldots,\varphi(a_n))}$. L'automorphisme φ est donc bien déterminé par son image sur R. ⌟

Ces dernières remarques sont d'une importance fondamentale. Tout d'abord, elles valident la vision de Galois du groupe des automorphismes d'une extension comme sous-groupe d'un groupe de permutation de racines. Aussi, elles impliquent facilement le résultat général suivant, et nous aideront dans la détermination des exemples concrets.

Proposition IV.3. *Si $K \subset L$ est une extension finie, alors son groupe des automorphismes $\mathrm{Aut}_K(L)$ est fini* [2].

Démonstration. Comme $K \subset L$ est une extension finie, elle est de génération finie et algébrique : il existe donc $a_1, \ldots, a_n \in L$ algébriques sur K tels que $L = K(a_1, \ldots, a_n)$. Soient $f_1, \ldots f_n \in K[X]$ les polynômes minimaux de $a_1, \ldots, a_n$ sur K, respectivement, et soit $f := f_1 \cdots f_n \in K[X]$. Comme

$$\{a_1, \ldots, a_n\} \subset R := \{a \in L \mid f(a) = 0\} \subset L$$

et $K(a_1, \ldots, a_n) = L$, on a $K(R) = L$. En appliquant la Remarque IV.2.4 à ce polynôme f, on a donc un homomorphisme injectif de groupes $\mathrm{Aut}_K(L) \hookrightarrow S(R)$ avec R fini. Cela implique que $\mathrm{Aut}_K(L)$ est un groupe fini. □

1. Cette égalité généralise l'égalité $\varphi(f(a)) = f(\varphi(a))$ vu en Remarque 2, et se vérifie similairement.

2. On montrera bientôt le résultat plus fort suivant : si $K \subset L$ est une extension finie, alors $|\mathrm{Aut}_K(L)|$ divise $[L : K]$ (voir Remarque IV.11.1).

Exemples IV.4 (groupes d'automorphismes)**.**

1. Par définition, le groupe des automorphismes de l'extension triviale est le groupe trivial : $\mathrm{Aut}_K(K) = \{\mathrm{id}_K\}$.
2. Le groupe des automorphismes de $\mathbb{R} \subset \mathbb{C}$ est $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, \tau\}$, avec τ la conjuguaison complexe.

   ⌜ Le fait que ces deux automorphismes font partie de $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ est clair. Pour vérifier l'inclusion inverse, considérons le polynôme $f = X^2 + 1 \in \mathbb{R}[X]$. Ses racines complexes sont $R = \{\pm i\}$, qui engendrent $\mathbb{C}$ sur $\mathbb{R}$. Ainsi, la Remarque IV.2.4 nous fournit un homomorphisme injectif $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) \hookrightarrow S(\{\pm i\}) = S_2$. Il y a donc au plus deux tels automorphismes, ce qui démontre l'égalité $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, \tau\}$. ⌟
3. Le groupe des automorphismes de $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ est trivial.

   ⌜ Considérons le polynôme $f = X^3 - 2 \in \mathbb{Q}[X]$. Son ensemble de racines dans $\mathbb{Q}(\sqrt[3]{2})$ est $R = \{a \in \mathbb{Q}(\sqrt[3]{2}) \mid f(a) = 0\} = \{\sqrt[3]{2}\}$. Par la Remarque IV.2.4, on a un homomorphisme injectif $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) \hookrightarrow S(R) = \{\mathrm{id}\}$, d'où $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}) = \{\mathrm{id}\}$. ⌟

Terminologie IV.5. Pour tout sous-groupe H de $\mathrm{Aut}_K(L)$, on note

$$L^H := \{a \in L \mid \varphi(a) = a \text{ pour tout } \varphi \in H\}\,.$$

On vérifie facilement qu'il s'agit d'un corps intermédiaire $K \subset L^H \subset L$: on parle du *sous-corps fixe par* H.

Exemples IV.6 (sous-corps fixes)**.**

1. Pour $H = \{\mathrm{id}\}$ le sous-groupe trivial de $\mathrm{Aut}_K(L)$, on a $L^{\{\mathrm{id}\}} = L$ par définition.
2. Pour $H = \mathrm{Aut}_K(L)$, le sous-corps fixe

   $$L^{\mathrm{Aut}_K(L)} = \{a \in L \mid \varphi(a) = a \text{ pour tout } \varphi \in \mathrm{Aut}_K(L)\}$$

   varie selon les cas. Par exemple, l'extension $\mathbb{R} \subset \mathbb{C}$ donne

   $$L^{\mathrm{Aut}_K(L)} = \mathbb{C}^{\{\mathrm{id},\tau\}} = \{z \in \mathbb{C} \mid \tau(z) = z\} = \mathbb{R} = K\,,$$

   puisque $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}, \tau\}$ avec τ la conjugaison complexe (Exemple IV.6.2). En revanche, l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ donne

   $$L^{\mathrm{Aut}_K(L)} = \mathbb{Q}(\sqrt[3]{2})^{\{\mathrm{id}\}} = \mathbb{Q}(\sqrt[3]{2}) = L\,,$$

   puisque $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{\mathrm{id}\}$ par l'Exemple IV.6.3.

Définition IV.7

Une extension finie $K \subset L$ est dite **galoisienne** si $L^{\mathrm{Aut}_K(L)} = K$.
Si tel est la cas, le groupe des automorphismes de $K \subset L$ est appelé le **groupe de Galois** de l'extension, noté $\mathrm{Gal}_K(L)$.

Remarque IV.8. Comme le sous-corps fixe $L^{\mathrm{Aut}_K(L)}$ est un corps intermédiaire $K \subset L^{\mathrm{Aut}_K(L)} \subset L$, demander que l'extension soit galoisienne revient à demander que $L^{\mathrm{Aut}_K(L)}$ soit "le plus petit possible". De manière équivalente, cela correspond à demander que le groupe $\mathrm{Aut}_K(L)$ soit "le plus grand possible". Ainsi, il est instructif d'interpréter les extensions galoisiennes comme celles qui ont "le plus possible de symétries". (Voir aussi la Remarque IV.11.1.)

Exemples IV.9 (extensions galoisiennes)**.**

1. Toute extension triviale $K \subset K$ est (trivialement) galoisienne.
2. L'extension $\mathbb{R} \subset \mathbb{C}$ est galoisienne : cela découle de l'Exemple IV.6.2.
3. L'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ n'est *pas* galoisienne : cela découle également de l'Exemple IV.6.2.
4. Pour toute extension finie $K \subset L$, l'extension intermédiaire $M \subset L$ donnée par $M = L^{\mathrm{Aut}_K(L)}$ est galoisienne, avec $\mathrm{Aut}_M(L) = \mathrm{Aut}_K(L)$.

   ⌜ Le corps $M = L^{\mathrm{Aut}_K(L)}$ est formé des éléments de L fixés par tout $\varphi \in \mathrm{Aut}_K(L)$ qui fixe les éléments de K. Ainsi, on a l'inclusion $\mathrm{Aut}_K(L) \subset \mathrm{Aut}_M(L)$. Comme l'inclusion $\mathrm{Aut}_M(L) \subset \mathrm{Aut}_K(L)$ découle trivialement de $K \subset M$, on a bien l'égalité $\mathrm{Aut}_M(L) = \mathrm{Aut}_K(L)$. Cela implique $L^{\mathrm{Aut}_M(L)} = L^{\mathrm{Aut}_K(L)} = M$. ⌟

Voici le résultat principal de cette section, qui justifie également les considérations de la Section III.8. Comme vous allez le voir, sa preuve est extrêmement riche et tout à fait splendide.

Théorème IV.10: Caractérisation des extensions galoisiennes

Pour une extension finie $K \subset L$, les énoncés suivants sont équivalents :

(i) L'extension $K \subset L$ est galoisienne.

(ii) L'extension $K \subset L$ est normale et séparable.

(iii) L est le corps des racines sur K d'un polynôme $f \in K[X]$ séparable.

(iv) Le groupe $\mathrm{Aut}_K(L)$ est d'ordre $[L : K]$.

Démonstration. Pour vérifier (i)⇒(ii), supposons $K \subset L$ galoisienne, et fixons $f \in K[X]$ irréductible avec une racine $a \in L$: il s'agit de montrer que f possède toutes ses racines dans L, et qu'elles sont simples. Pour ce faire, considérons l'ensemble

$$\{\varphi(a) \mid \varphi \in \mathrm{Aut}_K(L)\},$$

qui n'est autre que l'orbite de a par l'action du groupe $\mathrm{Aut}_K(L)$ sur l'ensemble (fini) des racines de f dans L. Énumérons ses éléments $\{a_1, \dots, a_d\}$ sans répétition, et définissons le polynôme $g := \prod_{i=1}^{d}(X - a_i) \in L[X]$. Par construction, tout $\varphi \in \mathrm{Aut}_K(L)$ permute les éléments $\{a_1, \dots, a_d\}$; ainsi, l'automorphisme $\varphi : L[X] \to L[X]$ satisfait

$$\varphi(g) = \varphi\left(\prod_{i=1}^{d}(X - a_i)\right) = \prod_{i=1}^{d}(X - \varphi(a_i)) = \prod_{i=1}^{d}(X - a_i) = g\,.$$

Comme ce fait est valide pour tout $\varphi \in \mathrm{Aut}_K(L)$, les coefficients de $g \in L[X]$ sont des éléments du sous-corps fixe $L^{\mathrm{Aut}_K(L)}$, qui n'est autre que K par hypothèse. On a donc $g \in K[X]$. Comme $g(a) = 0$ avec $g \in K[X]$, le polynôme minimal f divise g. Par conséquent, toutes les racines de f sont des racines de g. Comme toutes les racines de g sont dans L et sont simples, il en va de même pour les racines de f, ce qui démontre la première implication.

Pour montrer l'implication (ii)⇒(iii), supposons que $K \subset L$ est une extension finie normale et séparable. Comme elle est normale et finie, la Proposition III.65 garantit l'existence de $f \in K[X]$ tel que L est un corps des racines de f sur K. Comme $K \subset L$ est séparable, chaque facteur irréductible de f est séparable. Par définition (Terminologie III.67), il en va de même pour f.

L'implication (iii)⇒(iv) se montre par récurrence sur $n := [L : K] \geq 1$. Le cas $n = 1$ se vérifie facilement, puisqu'il correspond à l'extension triviale qui satisfait toujours $|\mathrm{Aut}_K(K)| = 1 = [K : K]$. Soit donc $K \subset L$ le corps des racines d'un polynôme $f \in K[X]$ séparable. Supposons $n = [L : K] > 1$, et l'implication démontrée pour tout extension de degré $< n$. Comme $n > 1$, il existe une racine $a \in L$ de f avec $a \notin K$; soit $g \in K[X]$ son polynôme minimal sur K, qui est donc de degré $\deg(g) =: d > 1$. Comme $g(a) = 0$, on a $g \mid f$ dans $K[X]$. Comme f est séparable et g est irréductible, toutes les racines de g sont simples, et toutes sont dans L : énumérons-les $a = a_1, a_2, \ldots, a_d \in L$. Pour tout $i = 1, \ldots, d$, le Corollaire III.29 fournit un isomorphisme canonique $\varphi_i : K(a) \xrightarrow{\simeq} K(a_i)$ tel que $\varphi_i|_K = \mathrm{id}_K$ et $\varphi_i(a) = a_i$. Comme dans la preuve de l'implication (iii)⇒(i) de la Proposition III.65, l'idée est d'appliquer le Lemme III.52 au diagramme suivant :

$$\begin{array}{ccccc} L & & \xhookrightarrow{\quad\Phi_i\quad} & & \\ \cup & & & & \\ K(a) & \xhookrightarrow{\varphi_i} & K(a_i) & \subset & L\,. \end{array}$$

Comme L est un corps des racines de f sur $K(a)$ (puisque c'est un corps des racines de f sur K), et comme $\varphi_i(f)$ est scindée sur L (puisque c'est un corps des racines de $f = \varphi_i(f) \in K[X]$), le Lemme III.52 implique que $K(a) \overset{\varphi_i}{\hookrightarrow} K(a_i) \subset L$ s'étend en un plongement $\Phi_i : L \hookrightarrow L$, qui satisfait donc $\Phi_i(a) = \varphi_i(a) = a_i$. De plus, comme l'extension $K \subset L$ est finie, on a nécessairement [3] $\Phi_i(L) = L$, et donc $\Phi_i \in \mathrm{Aut}_K(L)$. Considérons à présent l'application

$$\begin{aligned} \{1, \ldots, d\} \times \mathrm{Aut}_{K(a)}(L) &\longrightarrow \mathrm{Aut}_K(L) \\ (i, \Psi) &\longmapsto \Phi_i \circ \Psi\,. \end{aligned}$$

Comme on le vérifie facilement, cette application est bijective d'inverse

$$\begin{aligned} \mathrm{Aut}_K(L) &\longrightarrow \{1, \ldots, d\} \times \mathrm{Aut}_{K(a)}(L) \\ \Phi &\longmapsto (\text{l'unique } i \text{ tel que } \Phi(a) = a_i\,,\ \Phi_i^{-1} \circ \Phi)\,, \end{aligned}$$

d'où l'égalité $|\mathrm{Aut}_K(L)| = d \cdot |\mathrm{Aut}_{K(a)}(L)|$. Comme $K(a) \subset L$ est corps des racines de $f \in K(a)[X]$ séparable avec $[L : K(a)] = \frac{[L:K]}{[K(a):K]} = \frac{n}{d} < n$, on peut appliquer

3. Voir la fin de la preuve de (ii)⇒(iii) de la Proposition III.65.

l'hypothèse de récurrence et obtenir

$$|\mathrm{Aut}_K(L)| = d \cdot |\mathrm{Aut}_{K(a)}(L)| = d \cdot [L : K(a)] = [L : K(a)][K(a) : K] = [L : K] .$$

Terminons avec la preuve de (iv)⇒(i). Considérons le corps intermédiaire donné par le sous-corps fixe $M := L^{\mathrm{Aut}_K(L)}$. Par l'Exemple IV.9.4, l'extension $M \subset L$ est galoisienne, avec $\mathrm{Aut}_K(L) = \mathrm{Aut}_M(L)$. Par l'implication (i)⇒(iv) déjà démontrée, le groupe $\mathrm{Aut}_M(L)$ est d'ordre $[L : M]$. On a donc les égalités

$$[L : M][M : K] = [L : K] \overset{\text{(iv)}}{=} |\mathrm{Aut}_K(L)| = |\mathrm{Aut}_M(L)| = [L : M] ,$$

d'où $[M : K] = 1$. Ainsi, l'extension $K \subset M$ est triviale, d'où $K = M = L^{\mathrm{Aut}_K(L)}$. L'extension $K \subset L$ est donc bien galoisienne, ce qui conclut la preuve. □

Cette démonstration est tellement riche qu'elle appelle un certain nombre de remarques.

Remarques IV.11.

1. L'argument dans la preuve de (iv)⇒(i), qui utilise l'implication (i)⇒(iv), montre le fait suivant : si $K \subset L$ est une extension finie, alors $|\mathrm{Aut}_K(L)|$ divise $[L : K]$. C'est un exercice. Ainsi, on a en particulier $|\mathrm{Aut}_K(L)| \leq [L : K]$, et les extensions galoisiennes sont précisément les extensions avec groupe d'automorphisme "maximal".
2. L'équivalence (i)⇔(ii) permet de vérifier facilement les énoncés suivants pour une tour d'extensions $K \subset E \subset L$:
   - Si $K \subset L$ est galoisienne, alors $E \subset L$ est galoisienne.
   - Si $K \subset L$ est galoisienne, alors $K \subset E$ n'est pas nécessairement galoisienne.
   - Si $K \subset E$ et $E \subset L$ sont galoisiennes, alors $K \subset L$ n'est pas nécessairement galoisienne.

   C'est également l'objet d'un exercice.
3. La preuve de (i)⇒(ii) donne une construction quasi-explicite du polynôme minimal d'un élément d'une extension galoisienne à partir de $\mathrm{Gal}_K(L)$. En effet, si $K \subset L$ est une extension galoisienne, le polynôme minimal f de $a \in L$ est un diviseur irréductible de

$$g = \prod_{\varphi \in \mathrm{Gal}_K(L)} (X - \varphi(a)) \in K[X] .$$

   De plus, on a égalité $f = g$ si et seulement si $L = K(a)$. C'est un autre exercice.

Nous allons maintenant utiliser le Théorème IV.10 pour calculer quelques groupes de Galois. Avant cela, une dernière terminologie.

Terminologie IV.12. Une extension galoisienne $K \subset L$ est dite *abélienne* (resp. *cyclique*) si $\mathrm{Gal}_K(L)$ est un groupe abélien (resp. cyclique).

Exemples IV.13 (groupes de Galois)**.**

1. Toute extension $K \subset L$ galoisienne de degré premier est cyclique : en effet, par le Théorème IV.10 ((i)⇒(iv)), le groupe $\mathrm{Gal}_K(L)$ est d'ordre premier, et donc cyclique par Lagrange.
2. Soit $L \subset \mathbb{C}$ le corps des racines de $f = X^3 - 2 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$. Par le Théorème IV.10 ((ii)⇒(i)), c'est une extension galoisienne. Comme on l'a vu en Exemple III.51.5, on a $[L : \mathbb{Q}] = 6$. Par le Théorème IV.10 ((i)⇒(iv)), le groupe de Galois $\mathrm{Gal}_{\mathbb{Q}}(L)$ est d'ordre 6. Mais comme la Remarque IV.2.4 fournit un homomorphisme injectif $\mathrm{Gal}_{\mathbb{Q}}(L) \hookrightarrow S_3$, on a donc

$$\mathrm{Gal}_{\mathbb{Q}}(L) \simeq S_3 \,.$$

   L'argument de cet exemple montre plus généralement le fait suivant : si L est le corps des racines sur K d'un polynôme séparable $f \in K[X]$ de degré d avec $[L : K] = d!$, alors $\mathrm{Gal}_K(L) \simeq S_d$.
3. Soient $K = \mathbb{Q}$ et $L \subset \mathbb{C}$ le corps des racines de $f = X^4 + 1 \in \mathbb{Q}[X]$. L'extension $\mathbb{Q} \subset L$ est galoisienne par le Théorème IV.10, et de degré 4 par l'Exemple III.51.4. Par le Théorème IV.10 et la Remarque IV.2.4, le groupe de Galois $\mathrm{Gal}_{\mathbb{Q}}(L)$ est donc un sous-groupe de S_4 d'ordre 4, ce qui ne nous permet pas de conclure. En effet, ce groupe peut être isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   Pour le déterminer, il va falloir exhiber des éléments explicites de ce groupe. Rappelons que $L = \mathbb{Q}(\omega)$ avec $\omega = \exp(i\pi/4)$, et que les quatre racines de f sont données par $\omega, \omega^3, \omega^5, \omega^7$. Clairement, la restriction de la conjugaison complexe fournit un élément $\tau \in \mathrm{Gal}_{\mathbb{Q}}(L)$ qui permute ces racines via $\omega \overset{\tau}{\leftrightarrow} \omega^7$ et $\omega^3 \overset{\tau}{\leftrightarrow} \omega^5$. De plus, considérons l'extension intermédiaire

$$\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(\omega) = L \,.$$

   Le polynôme minimal de ω sur $\mathbb{Q}(i)$ est $X^2 - i \in \mathbb{Q}(i)[X]$, dont l'autre racine est ω^5. Par le Corollaire III.29, il existe un automorphisme $\sigma \in \mathrm{Gal}_{\mathbb{Q}(i)}(L) \subset \mathrm{Gal}_{\mathbb{Q}}(L)$ tel que $\sigma(\omega) = \omega^5$. On calcule ensuite $\sigma(\omega^3) = (\omega^5)^3 = \omega^7$, et similairement avec les autres racines, pour obtenir la permutation $\omega \overset{\sigma}{\leftrightarrow} \omega^5$ et $\omega^3 \overset{\sigma}{\leftrightarrow} \omega^7$. On voit donc que les permutations[4] $\tau, \sigma \in S_4$ engendrent un sous-groupe d'ordre 4 isomorphe au groupe de Klein

$$\mathrm{Gal}_{\mathbb{Q}}(L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \,.$$

   Notons que cela découlera également d'un résultat bien plus général, le Corollaire IV.35, via l'isomorphisme $(\mathbb{Z}/8\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

4. Bien entendu, la permutation induite par τ est la restriction de la conjugaison complexe, un automorphisme de $\mathbb{C}$ qui se réalise géométriquement comme une réflexion du plan. Attention : si la permutation des racines induite par l'automorphisme σ correspond à la symétrie centrale du plan par l'origine, l'automorphisme $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(L)$ fixe les rationnels point par point. On ne peut donc pas lui donner une *formulation géométrique*. En revanche, il admet une *formulation algébrique* totalement explicite : tout élément de $\mathbb{Q}(\omega) = \mathbb{Q}[\omega]$ est de la forme $a_0 + a_1\omega + a_2\omega^2 + \cdots + a_7\omega^7$ avec $a_i \in \mathbb{Q}$, et cet élément est envoyé par σ sur $a_0 + a_1\omega^5 + a_2\omega^2 + \cdots + a_7\omega^3$, une image entièrement déterminée par la permutation des racines (et même par $\sigma(\omega)$).

De nombreux autres exemples seront traités en exercices.

Terminons cette section avec la détermination du groupe de Galois de toute extension finie d'un corps fini.

Proposition IV.14. *Toute extension finie d'un corps fini est cyclique.*

Démonstration. Soit $K \subset L$ une extension finie (disons, de degré $[L : K] =: n \geq 1$) avec K fini (disons $|K| = q = p^d$ avec p premier et $d \geq 1$). Par la Proposition III.58, le corps L est corps des racines d'un polynôme $f \in K[X]$. Comme K est fini, la Proposition III.69 implique que f est séparable. Par le Théorème IV.10, il suit que $K \subset L$ est bien une extension galoisienne, avec $|\mathrm{Gal}_K(L)| = [L : K] = n$.

Pour montrer que ce groupe est cyclique, considérons l'application

$$\varphi : L \longrightarrow L\,, \quad x \longmapsto \varphi(x) = x^q\,.$$

Par le Lemme III.57 (appliqué d fois), on a $(x+y)^q = x^q + y^q$ pour tous $x, y \in L$. Comme $(xy)^q = x^q y^q$ et $1^q = 1$ trivialement, l'application φ est un homomorphisme[5] de corps. Comme tout homomorphisme de corps, il est injectif, et donc bijectif puisque L est fini. Nous sommes donc en présence d'un automorphisme $\varphi \in \mathrm{Aut}(L)$. Comme K est un corps à q éléments, son groupe des unités K^* est d'ordre $q-1$, d'où $\varphi(x) = x^q = x$ pour tout $x \in K$; l'automorphisme φ est donc un élément de $\mathrm{Gal}_K(L)$.

Nous allons maintenant montrer que φ engendre $\mathrm{Gal}_K(L)$, ce qui terminera la preuve. Pour ce faire, considérons le sous-groupe $\langle\varphi\rangle$ de $\mathrm{Gal}_K(L)$ engendré par φ, et notons k son ordre. Naturellement, l'inclusion $\langle\varphi\rangle \subset \mathrm{Gal}_K(L)$ implique l'inégalité $k = |\langle\varphi\rangle| \leq |\mathrm{Gal}_K(L)| = n$. D'autre part, comme $\varphi^k = \mathrm{id}_L$, les q^n éléments de L sont racines de $X^{q^k} - X$, qui ne peut en avoir plus de q^k. On obtient donc l'inégalité $q^n \leq q^k$, d'où $n \leq k$. On a donc bien l'égalité $k = n$, et donc $\langle\varphi\rangle = \mathrm{Gal}_K(L)$. □

IV.2 Le théorème fondamental de la théorie de Galois

Nous sommes finalement arrivés au cœur de la théorie. Soit donc $K \subset L$ une extension quelconque. Rappelons que pour tout sous-groupe $H < \mathrm{Aut}_K(L)$, on a défini le sous-corps fixe

$$L^H = \{a \in L \mid \varphi(a) = a \text{ pour tout } \varphi \in H\}\,,$$

qui est un corps intermédiaire de l'extension $K \subset L$. Réciproquement, étant donné un corps intermédiaire $K \subset E \subset L$, on peut considérer le sous-groupe

$$\mathrm{Aut}_E(L) = \{\varphi \in \mathrm{Aut}_K(L) \mid \varphi(a) = a \text{ pour tout } a \in E\}$$

de $\mathrm{Aut}_K(L)$. On obtient donc deux applications

$$\{\text{sous-groupes de } \mathrm{Aut}_K(L)\} \rightleftarrows \{\text{extensions intermédiaires de } K \subset L\}$$

$$H \longmapsto L^H$$

$$\mathrm{Aut}_E(L) \longmapsfrom E\,.$$

5. Appelé *homomorphisme de Frobenius.*

Terminologie IV.15. On parle de la *correspondance de Galois* pour $K \subset L$.

Sans aucune hypothèse sur l'extension $K \subset L$, cette correspondance de Galois possède déjà des propriétés remarquables.

Remarques IV.16.

1. L'ensemble des sous-groupes de $\mathrm{Aut}_K(L)$ et l'ensemble des extensions intermédiaires de $K \subset L$ sont ordonnés par inclusion. Et l'on vérifie immédiatement que la correspondance de Galois renverse l'ordre : si $H \subset H'$ sont deux sous-groupes de $\mathrm{Aut}_K(L)$, alors on a $L^{H'} \subset L^H$; si $E \subset E'$ sont deux corps intermédiaires, alors on a $\mathrm{Aut}_{E'}(L) \subset \mathrm{Aut}_E(L)$. C'est un exercice.
2. L'ensemble ordonné des sous-groupes de $\mathrm{Aut}_K(L)$ est en fait un *treillis* : toute paire H_1, H_2 de tels sous-groupes admet une borne inférieure (leur intersection $H_1 \cap H_2$) et une borne supérieure (le sous-groupe $\langle H_1, H_2 \rangle$ de $\mathrm{Aut}_K(L)$ engendré par $H_1 \cup H_2$). Il en va de même pour l'ensemble ordonné des extensions intermédiaires de $K \subset L$: toute paire E_1, E_2 de telles extensions intermédiaires admet une borne inférieure (leur intersection $E_1 \cap E_2$) et une borne supérieure (le sous-corps de L engendré par $E_1 \cup E_2$, noté E_1E_2).

   On vérifiera en exercices que la correspondance de Galois respecte cette structure de treillis, dans le sens suivant. Pour toutes paires E_1, E_2 de corps intermédiaires et H_1, H_2 de sous-groupes de $\mathrm{Aut}_K(L)$, on a

$$\mathrm{Aut}_{E_1E_2}(L) = \mathrm{Aut}_{E_1}(L) \cap \mathrm{Aut}_{E_2}(L) \quad \text{et} \quad L^{\langle H_1, H_2 \rangle} = L^{H_1} \cap L^{H_2}.$$

3. Est-il possible que les deux applications dans la correspondance de Galois soient inverse l'une de l'autre ? On vérifie très facilement que pour toute extension intermédiaire $K \subset E \subset L$, on a $E \subset L^{\mathrm{Aut}_E(L)}$, tandis que pour tout sous-groupe $H < \mathrm{Aut}_K(L)$, on a $H < \mathrm{Aut}_{L^H}(L)$. C'est un troisième exercice.

Mais pour avoir égalité, il faut en particulier avoir $K = L^{\mathrm{Aut}_K(L)}$: ainsi, on doit nécessairement être en présence d'une extension galoisienne. Le théorème fondamental de la théorie de Galois dit que cette condition nécessaire est en fait suffisante pour que la correspondance de Galois soit bijective.

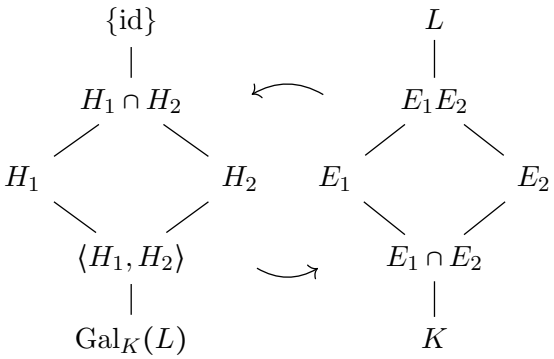
Théorème IV.17: Théorème fondamental de la théorie de Galois

Si $K \subset L$ est une extension galoisienne, alors les deux applications dans la correspondance de Galois sont des bijections inverses l'une de l'autre.

À ce stade, il y a un certain nombre de tâches à accomplir : faire quelques remarques (pour comprendre au mieux cet énoncé), donner des exemples (pour l'illustrer), et fournir une preuve (pour laquelle l'essentiel du travail a déjà été effectué). Nous allons nous y atteler dans ce ordre, avant d'énoncer et de démontrer un supplément à ce théorème.

Remarques IV.18.

1. Ce théorème nous dit donc que si $K \subset L$ est galoisienne, alors $\mathrm{Aut}_{L^H}(L) = H$ pour tout $H < \mathrm{Aut}_K(L)$ et $L^{\mathrm{Aut}_E(L)} = E$ pour tout $K \subset E \subset L$ (ce qu'on peut noter $\mathrm{Gal}_{L^H}(L) = H$ et $L^{\mathrm{Gal}_E(L)} = E$ puisque $E \subset L$ est galoisienne par la Remarque IV.11.2). Ainsi, les Remarques IV.16.1-2 impliquent que la correspondance de Galois est une bijection qui renverse l'ordre et respecte la structure de treillis. Ce fait est illustré par les diagrammes suivants



(IV.1)

où $H_i = \mathrm{Gal}_{E_i}(L)$ et $E_i = L^{H_i}$ $(i = 1, 2)$. Notez que l'inclusion est illustrée de haut en bas pour les sous-groupes (à gauche), mais de bas en haut pour les extensions intermédiaires (à droite).

De plus, on vérifie que si $K \subset E_1$ est galoisienne, alors $E_2 \subset E_1E_2$ est galoisienne, et on a un isomorphisme de groupes

$$\mathrm{Gal}_{E_2}(E_1E_2) \simeq \mathrm{Gal}_{E_1 \cap E_2}(E_1)\,. \tag{IV.2}$$

C'est un exercice.

2. Pour toute extension intermédiaire $K \subset E \subset L$ d'une extension galoisienne, on a vu en Remarque IV.11.2 que l'extension $E \subset L$ est galoisienne. Par le Théorème IV.10 et Lagrange, on obtient

$$[E : K] = \frac{[L : K]}{[L : E]} = \frac{|\mathrm{Gal}_K(L)|}{|\mathrm{Gal}_E(L)|} = [\mathrm{Gal}_K(L) : \mathrm{Gal}_E(L)]\,.$$

Par conséquent, pour toute paire d'extensions intermédiaires $E \subset E'$, on a

$$[E' : E] = \frac{[E' : K]}{[E : K]} = \frac{|\mathrm{Gal}_E(L)|}{|\mathrm{Gal}_{E'}(L)|} = [\mathrm{Gal}_E(L) : \mathrm{Gal}_{E'}(L)]\,. \tag{IV.3}$$

Comme la correspondance de Galois est une bijection, cela peut également s'écrire

$$[H : H'] = [L^{H'} : L^H] \tag{IV.4}$$

pour tous sous-groupes $H' \subset H$ de $\mathrm{Gal}_K(L)$. Ainsi, la bijection de treillis (IV.1) respecte également les degrés des extensions, qui correspondent aux indices des sous-groupes. Cela justifie naturellement ces deux notations très similaires.

3. Il est a priori difficile d'énumérer toutes les extensions intermédiaires d'une extension finie donnée ; en particulier, il n'est pas du tout clair qu'elle en

possède un nombre fini. En revanche, il est souvent aisé de décrire le treillis des sous-groupes d'un groupe fini donné ; en particulier, il est évident qu'il en possède un nombre fini.

Dans le cas des extensions galoisiennes, *le théorème fondamental de la théorie de Galois permet de résoudre le problème difficile au moyen du facile*. En particulier, on obtient immédiatement le fait qu'une extension galoisienne ne possède qu'un nombre fini d'extensions intermédiaires. Le même résultat est valide pour les extensions séparables finies, comme le montre le corollaire suivant.

Corollaire IV.19. *Une extension séparable finie n'admet qu'un nombre fini d'extensions intermédiaires.*

Démonstration. Soit $K \subset L$ une extension séparable finie. Comme $K \subset L$ est finie, il existe $a_1, \dots, a_n \in L$ algébriques sur K tels que $L = K(a_1, \dots, a_n)$. Soit $f_i \in K[X]$ le polynôme minimal de a_i sur K, et soit L' le corps des racines de $f := f_1 \cdots f_n \in K[X]$ sur K. Notons les inclusions $K \subset L = K(a_1, \dots, a_n) \subset L'$, puisque L' contient K et chaque a_i. Comme $K \subset L$ est séparable, chaque f_i est séparable, de même que f par définition. Ainsi, L' est le corps des racines d'un polynôme séparable : par le Théorème IV.10, l'extension $K \subset L'$ est donc galoisienne. Par le Théorème IV.17, le nombre d'extensions intermédiaires de $K \subset L'$ est égal au nombre de sous-groupes du groupe fini $\mathrm{Gal}_K(L')$: c'est donc un nombre fini. Comme on a $K \subset L \subset L'$, il en va de même pour le nombre d'extensions intermédiaires de $K \subset L$. □

Venons-en enfin à des premiers exemples concrets d'applications de ce théorème fondamental. D'autres seront vus en exercices, ainsi que plus tard dans le cours.

Exemples IV.20.

1. Soit $K \subset L$ une extension galoisienne de degré p premier. Par le Théorème IV.10, on a $|\mathrm{Gal}_K(L)| = [L : K] = p$. Par Lagrange, il est cyclique et n'admet aucun sous-groupe propre. Par le Théorème IV.17, il n'y a aucune extension intermédiaire propre $K \subsetneq E \subsetneq L$, et on obtient les treillis suivants

$$\begin{array}{ccc} \{\mathrm{id}\} & \rightharpoonup & L \\ \Big| p & & \Big| p \\ \mathbb{Z}/p\mathbb{Z} & \leftharpoondown & K\,, \end{array}$$

   où les décorations dénotent les indices des sous-groupes et les degrés des extensions. Bien-sûr, dans ce cas précis, ce résultat peut aussi être obtenu par la Proposition III.20. Cet exemple n'est donc qu'un *reality check*.

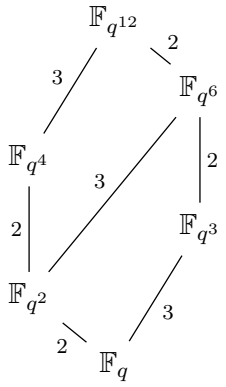
2. Soit $K \subset L$ une extension finie (disons, de degré n) d'un corps fini (disons $K = \mathbb{F}_q$). Par la Proposition IV.14, c'est une extension galoisienne avec

$$\mathrm{Gal}_K(L) = \langle \varphi \mid \varphi^n \rangle \simeq \mathbb{Z}/n\mathbb{Z}\,.$$

Les sous-groupes $H < \langle \varphi \mid \varphi^n \rangle$ sont de la forme $H = \langle \varphi^d \rangle$ avec $d \mid n$; de plus, on a $\langle \varphi^e \rangle \subset \langle \varphi^d \rangle$ pour d, e deux diviseurs de n si et seulement si $d \mid e$. Ainsi, le treillis des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ est donné par l'ensemble des diviseurs de n (inversément) ordonnés par la divisibilité.

Par le Théorème IV.17, le treillis des extensions intermédiaires de $K \subset L$ est donné par l'ensemble des diviseurs de n ordonnés par la divisibilité, où au diviseur d de n correspond l'extension intermédiaire $\mathbb{F}_q \subset \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$. On retrouve en particulier le Corollaire III.60 : il existe une extension $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^e}$ si et seulement si d divise e.

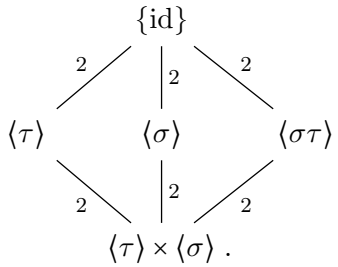
Le cas de $n = 12$ est illustré ci-dessous. D'autres seront en exercices.



3. Considérons l'extension $\mathbb{Q} \subset \mathbb{Q}(\omega)$, où $\omega = \exp(i\pi/4)$. Par l'Exemple IV.13.3, il s'agit d'une extension galoisienne (le corps des racines de $X^4 + 1 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$), avec groupe de Galois

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega)) = \langle \tau \rangle \times \langle \sigma \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

où τ est la restriction de la conjugaison complexe, et σ est un automorphisme de $\mathbb{Q}(\omega)$ tel que $\omega \overset{\sigma}{\leftrightarrow} \omega^5$ et $\omega^3 \overset{\sigma}{\leftrightarrow} \omega^7$. Le treillis des sous-groupes de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega))$ est donné par

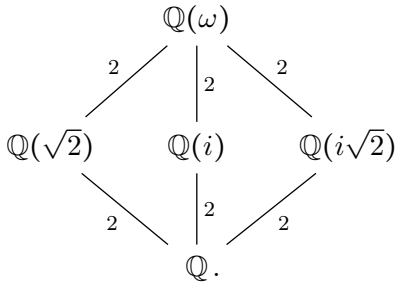


Il s'agit maintenant d'appliquer la correspondance de Galois pour déterminer les treillis des extensions intermédiaires de $\mathbb{Q} \subset \mathbb{Q}(\omega)$.

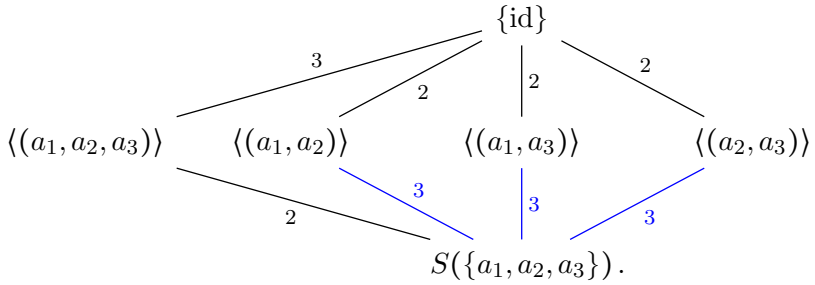
Notons tout d'abord que $\omega + \omega^7 = \sqrt{2}$ est fixé par τ. Ainsi, l'extension intermédiaire $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\omega)$ satisfait $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\omega)^H$ pour $H = \langle \tau \rangle$. Comme

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 = [\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega)) : H] \overset{\text{(IV.4)}}{=} [\mathbb{Q}(\omega)^H : \mathbb{Q}],$$

on a bien $\mathbb{Q}(\omega)^H = \mathbb{Q}(\sqrt{2})$. Comme $\omega^2 = i$ est fixé par σ et $\omega + \omega^3 = i\sqrt{2}$ est fixé par $\sigma\tau$, on obtient similairement $\mathbb{Q}(\omega)^{\langle\sigma\rangle} = \mathbb{Q}(i)$ et $\mathbb{Q}(\omega)^{\langle\sigma\tau\rangle} = \mathbb{Q}(i\sqrt{2})$. Au final, on a le treillis suivant :



4. Considérons l'extension $\mathbb{Q} \subset \mathbb{Q}(\mu, a) =: L$, où $\mu = \exp(2i\pi/3)$ et $a = \sqrt[3]{2}$. Par l'Exemple IV.13.2, c'est une extension galoisienne (le corps des racines de $X^3 - 2 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$). De plus, son groupe de Galois est $\mathrm{Gal}_{\mathbb{Q}}(L) \simeq S_3$, le groupe des permutations des trois racines $(a_1, a_2, a_3) = (a, \mu a, \mu^2 a)$. Voici le treillis des sous-groupes de $S(\{a_1, a_2, a_3\})$, décoré avec les indices :

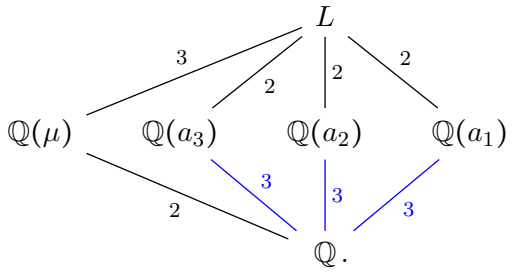


Pour en déduire le treillis des extensions intermédiaires de $\mathbb{Q} \subset L$, il reste à calculer les sous-corps fixes correspondants à ces 4 sous-groupes propres.

Notons tout d'abord que comme $a_1 + a_2 + a_3 = 0$, la racine a_3 est fixée par le sous-groupe $H = \langle(a_1, a_2)\rangle$, d'où l'inclusion $\mathbb{Q}(a_3) \subset L^H$. Comme les degrés

$$[\mathbb{Q}(a_3) : \mathbb{Q}] = 3 = [S_3 : H] = [L^H : \mathbb{Q}]$$

correspondent, on a $L^H = \mathbb{Q}(a_3)$. On calcule similairement $L^{\langle(a_1,a_3)\rangle} = \mathbb{Q}(a_2)$ et $L^{\langle(a_2,a_3)\rangle} = \mathbb{Q}(a_1)$. Finalement, l'élément $\mu = \frac{a_2}{a_1} = \frac{a_3}{a_2} = \frac{a_1}{a_3}$ est fixé par le 3-cycle (a_1, a_2, a_3), d'où $\mathbb{Q}(\mu) \subset L^{\langle(a_1,a_2,a_3)\rangle}$ et égalité via calcul des degrés et indices. Par le Théorème IV.17, le treillis des extensions intermédiaires de $\mathbb{Q} \subset L$ est le suivant :



Notons que sur cet exemple, les extensions qui ne sont *pas* normales sont notées en bleu, et correspondent exactement aux sous-groupes qui ne sont *pas* normaux. Ce n'est pas un hasard, comme on le verra avec le Théorème IV.22 ci-dessous.

Nous allons maintenant donner la preuve du Théorème IV.17, qui repose sur (une bonne partie du Chapitre III et sur) le lemme suivant.

Lemme IV.21. *Soient L un corps, H un sous-groupe fini de $\mathrm{Aut}(L)$, et $L^H \subset L$ le sous-corps fixe correspondant. Alors, on a l'inégalité $[L : L^H] \leq |H|$.*

Démonstration. Posons $n := |H|$, et soient $a_0, a_1, \ldots, a_n$ des éléments quelconques de L. Le but est de voir qu'ils forment une famille liée sur L^H, ce qui impliquera l'inégalité $\dim_{L^H}(L) < n+1$, et donc l'énoncé $[L : L^H] \leq n = |H|$.

Pour ce faire, considérons le système d'équations linéaires donné par

$$x_0\varphi(a_0) + x_1\varphi(a_1) + \cdots + x_n\varphi(a_n) = 0\,, \quad \forall \varphi \in H\,.$$

Il s'agit d'un système de n équations (une pour chaque automorphisme $\varphi \in H$) à $n+1$ inconnues $(x_0, \ldots, x_n) \in L^{n+1}$ – rappelons que les éléments $a_0, \ldots, a_n \in L$ sont fixés. Ainsi, ce système admet des solutions $(x_0, \ldots, x_n) \in L^{n+1}$ non-nulles. Parmi toutes ces solutions non-nulles, on en choisit une avec un nombre minimal (disons, $m+1 > 0$) de composantes non-nulles ; via renumérotation, on peut écrire cette solution $(x_0, \ldots, x_m, 0, \ldots, 0) \in L^n$ avec $x_i \neq 0$ pour $0 \leq i \leq m$. En multipliant par x_0^{-1}, on obtient donc un vecteur $(y_1, \ldots, y_m) \in L^m$ tel que

$$\varphi(a_0) + y_1\varphi(a_1) + \cdots + y_m\varphi(a_m) = 0 \qquad (*_\varphi)$$

pour tout $\varphi \in H$. En appliquant un automorphisme quelconque $\varphi' \in H$ à $(*_\varphi)$ et en lui soustrayant $(*_\psi)$ avec $\psi := \varphi' \circ \varphi \in H$, on obtient l'égalité

$$(\varphi'(y_1) - y_1)\psi(a_1) + \cdots + (\varphi'(y_m) - y_m)\psi(a_m) = 0$$

valide pour tout $\psi \in H$. (Notons que pour tout $\varphi' \in H$ fixé, cette équation est satisfaite pour tout $\psi = \varphi' \circ \varphi \in H$.) Par minimalité de m, on a $\varphi'(y_i) - y_i = 0$ pour tout $i = 1, \ldots, m$, i.e. $\varphi'(y_i) = y_i$. Comme cette égalité est valide pour tout $\varphi' \in H$, on a donc $y_1, \ldots, y_m \in L^H$. En particulier, l'équation $(*_{\mathrm{id}})$ nous fournit la relation

$$a_0 + y_1a_1 + \cdots + y_ma_m = 0$$

avec $y_1, \ldots, y_m \in L^H$, ce qui montre que les éléments $a_0, a_1, \ldots, a_n$ sont linéairement dépendants sur L^H. □

Démonstration du Théorème IV.17. Supposons donc que $K \subset L$ est une extension galoisienne, et soit $K \subset E \subset L$ une extension intermédiaire. Par la Remarque IV.11.2, l'extension $E \subset L$ est également galoisienne, d'où $L^{\mathrm{Aut}_E(L)} = E$.

Soit à present H un sous-groupe de $\mathrm{Aut}_K(L) < \mathrm{Aut}(L)$, et soit L^H le sous-corps fixe correspondant. Par le Lemme IV.21, l'inclusion $H \subset \mathrm{Aut}_{L^H}(L)$ (voir Remarque IV.16.3), et le Théorème IV.10 appliqué à l'extension galoisienne $L^H \subset L$, on a

$$[L : L^H] \leq |H| \leq |\mathrm{Aut}_{L^H}(L)| = [L : L^H]\,.$$

Ainsi, il y a des égalités partout, d'où en particulier $H = \mathrm{Aut}_{L^H}(L)$. □

Rappelons que si $K \subset E \subset L$ est une tour d'extensions avec $K \subset L$ galoisienne, alors $E \subset L$ est galoisienne, mais $K \subset E$ pas forcément (Remarque IV.11.2). Le résultat suivant nous dit précisément quand c'est le cas (et justifie la terminologie).

Théorème IV.22: Supplément au théorème fondamental

Si $K \subset L$ est galoisienne, alors l'extension $K \subset E$ est galoisienne si et seulement si le sous-groupe $\mathrm{Gal}_E(L) < \mathrm{Gal}_K(L)$ est normal ; si tel est le cas, on a un isomorphisme de groupes $\mathrm{Gal}_K(E) \simeq \mathrm{Gal}_K(L)/\mathrm{Gal}_E(L)$.

Remarque IV.23. Notons que l'extension $K \subset E$ est séparable, puisque $K \subset L$ l'est. Ainsi, ce théorème nous dit que l'extension $K \subset E$ est normale si et seulement si le sous-groupe $\mathrm{Gal}_E(L) < \mathrm{Gal}_K(L)$ est normal. Cela justifie naturellement ces terminologies identiques.

La démonstration de ce résultat repose sur un lemme dont la preuve est laissée en exercice.

Lemme IV.24. *Soit $K \subset L$ une extension quelconque. Pour toute extension intermédiaire $K \subset E \subset L$ et tout $\Phi \in \mathrm{Aut}_K(L)$, les deux sous-groupes $\mathrm{Aut}_{\Phi(E)}(L)$ et $\Phi\mathrm{Aut}_E(L)\Phi^{-1}$ de $\mathrm{Aut}_K(L)$ coïncident.* □

Démonstration du Théorème IV.22. Supposons pour commencer que $K \subset E$ est galoisienne, et considérons l'homomorphisme de groupes donné par la restriction

$$\mathrm{Gal}_K(L) \longrightarrow \mathrm{Gal}_K(E)\,, \quad \Phi \longmapsto \Phi|_E\,.$$

Notons tout d'abord qu'a priori, on a $\Phi|_E : E \to L$, mais c'est bien un automorphisme de E puisque $\Phi(E) = E$ par normalité de $K \subset E$ (i.e. par la Proposition III.65 (i)⇒(iii)). Nous allons maintenant vérifier que cet homomorphisme est surjectif. Soit donc φ un automorphisme de E fixant K. Par la Proposition III.65 ((i)⇒(ii)) appliquée à $E \subset L$, il existe $f \in E[X]$ tel que L est un corps des racines de f sur E. On peut donc appliquer le Lemme III.52 avec $L' = L$: il nous garantit l'existence d'un homomorphisme $\Phi : L \hookrightarrow L$ tel que $\Phi|_E = \varphi$. Comme $\Phi|_K = \varphi|_K = \mathrm{id}_K$ et $K \subset L$ est normale, la Proposition III.65 implique que $\Phi(L) = L$. On a donc bien construit $\Phi \in \mathrm{Gal}_K(L)$ tel que $\Phi|_E = \varphi$. Finalement, le noyau de cet homomorphisme est $\mathrm{Gal}_E(L)$ par définition, ce qui implique $\mathrm{Gal}_E(L) \lhd \mathrm{Gal}_K(L)$. Par le premier théorème d'isomorphisme, on a bien $\mathrm{Gal}_K(E) \simeq \mathrm{Gal}_K(L)/\mathrm{Gal}_E(L)$.

Supposons réciproquement $\mathrm{Gal}_E(L) \lhd \mathrm{Gal}_K(L)$. Comme $K \subset E$ est toujours séparable (puisque $K \subset L$ l'est), il reste à vérifier que $K \subset E$ est normal. Soit donc $f \in K[X]$ irréductible qui admet une racine $a \in E \subset L$. Comme $K \subset L$ est normale, le polynôme f est scindé sur L. Soit $a' \in L$ une racine quelconque de f. Par le Corollaire III.53, il existe $\Phi \in \mathrm{Gal}_K(L)$ tel que $\Phi(a) = a'$. Mais par la Remarque IV.16.3, le Lemme IV.24, l'hypothèse de normalité, et le fait que $E \subset L$ est galoisienne, on a l'inclusion

$$\Phi(E) \subset L^{\mathrm{Aut}_{\Phi(E)}(L)} = L^{\Phi\mathrm{Aut}_E(L)\Phi^{-1}} = L^{\mathrm{Aut}_E(L)} = E\,.$$

En particulier, on a bien $a' = \Phi(a) \in \Phi(E) \subset E$. Comme c'est valable pour toute racine a' de f, cela conclut la preuve de la normalité de $K \subset E$. □

IV.3 Polynômes cyclotomiques et polygones constructibles

Comme première application de la théorie de Galois, nous allons caractériser les polygones constructibles à la règle et au compas, mettant fin à une quête plusieurs fois millénaires. Cela passe par l'étude de polynômes bien particuliers, appelés *polynômes cyclotomiques*.

Dans toute cette section, nous fixons un entier $n \geq 1$ et notons $\omega = \exp(2i\pi/n)$.

Comme vous le savez, les racines complexes du polynôme $X^n - 1$ forment le groupe (cyclique)

$$\mu_n(\mathbb{C}) := \{z \in \mathbb{C} \mid z^n = 1\} = \{\omega^k \mid 1 \leq k \leq n\}$$

des racines $n^{\text{ièmes}}$ de l'unité. Par conséquent, on a l'identité

$$X^n - 1 = \prod_{1 \leq k \leq n} (X - \omega^k) \in \mathbb{C}[X]\,. \tag{IV.5}$$

L'ensemble des générateurs du groupe $\mu_n(\mathbb{C})$ est $\{\omega^k \mid \operatorname{pgcd}(k,n) = 1\}$, dont les éléments sont appelés les *racines primitives* $n^{\text{ièmes}}$ de l'unité. Il y en a

$$\varphi(n) := \#\{1 \leq k \leq n \mid \operatorname{pgcd}(k,n) = 1\}\,.$$

Billet de 10 francs suisses à l'effigie d'Euler, en circulation entre 1979 et 2000

L'application $\varphi\colon \{1,2,\dots\} \to \{1,2,\dots\}$ est appelée la *fonction φ d'Euler*, en l'honneur de notre mathématicien national.

Remarque IV.25. Si un entier $n > 1$ se décompose en facteurs premiers distincts via $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, alors on a

$$\varphi(n) = (p_1 - 1)p_1^{\nu_1 - 1} \cdots (p_r - 1)p_r^{\nu_r - 1}\,.$$

C'est un exercice.

L'objet le plus important de cette section est le suivant, raison pour laquelle une définition lui est due.

Définition IV.26

Le $n^{\text{ième}}$ **polynôme cyclotomique** est

$$\Phi_n(X) := \prod_{\substack{1 \leq k \leq n \\ \operatorname{pgcd}(k,n)=1}} (X - \omega^k) \in \mathbb{C}[X]\,.$$

Notons que par définition, on a $\deg \Phi_n = \varphi(n)$. A priori, le polynôme Φ_n est à coefficients complexes, mais le calcul explicite des premiers exemples

$$\Phi_1 = X-1\,,\ \ \Phi_2 = X+1\,,\ \ \Phi_3 = X^2+X+1\,,\ \ \Phi_4 = X^2+1\,,\ \ \Phi_5 = X^4+X^3+X^2+X+1$$

fait penser qu'ils sont à coefficients entiers, voire à coefficients dans $\{-1,0,1\}$. La première conjecture est correcte, comme le montre le résultat suivant dont la preuve a été vue en ALGÈBRE I.

Lemme IV.27. *(i) Pour tout n, on a l'égalité $X^n-1 = \prod_{d|n} \Phi_d(X)$ dans $\mathbb{C}[X]$.*
(ii) Pour tout n, $\Phi_n(X) \in \mathbb{Z}[X]$. □

Remarques IV.28.

1. L'égalité en (i) se démontre facilement via (IV.5) et la partition

$$\{1,\dots,n\} = \bigsqcup_{d|n} \{1 \le k \le n \mid \operatorname{pgcd}(k,d) = 1\}\,.$$

   Cette égalité peut être utilisée pour des calculs explicites de Φ_n, et implique facilement le second point par récurrence sur $n \ge 1$.

2. La seconde conjecture, à savoir le fait que tous les coefficients de Φ_n sont dans $\{-1,0,1\}$, est vraie tant que n possède au plus 2 diviseurs premiers impairs distincts. En revanche, pour $n = 105 = 3\cdot5\cdot7$, le coefficients de degré 41 est égal à -2. Il s'avère qu'il n'existe pas de borne uniforme pour tous les coefficients de tous les polynômes cyclotomiques.

Pour $n = p$ premier, on a

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

et il n'est pas difficile de vérifier que c'est un polynôme irréductible dans $\mathbb{Q}[X]$. Il s'avère qu'il en va de même pour tous les polynômes cyclotomiques, ce qui est beaucoup plus difficile à montrer, et l'objet du résultat le plus technique de cette section.

Théorème IV.29

Pour tout $n \ge 1$, le polynôme cyclotomique Φ_n est irréductible dans $\mathbb{Q}[X]$.

Remarque IV.30. Rappelons que la version du *lemme de Gauss* vue en ALGÈBRE I nous assure qu'un polynôme $f \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$ si et seulement si f est primitif et irréductible dans $\mathbb{Q}[X]$. Ainsi, comme $\Phi_n \in \mathbb{Z}[X]$ est unitaire (et donc primitif) et irréductible dans $\mathbb{Q}[X]$, il est également irréductible dans $\mathbb{Z}[X]$.

Billet de 10 Deutsche Mark à l'effigie de Gauss, en circulation entre 1991 et 2001

La preuve du Théorème IV.29 repose sur une autre version du lemme de Gauss, que voici.

Lemme IV.31. *Si $f, g \in \mathbb{Z}[X]$ sont primitifs, alors fg est également primitif.*

Démonstration du Lemme IV.31. Soient donc $f, g \in \mathbb{Z}[X]$ primitifs, et soit p un nombre premier arbitraire. Le but est de vérifier que p ne divise pas tous les coefficients de fg, ce qui montrera que fg est primitif.

Pour ce faire, écrivons $f = a_0 + a_1X + \cdots + a_nX^n$ et $g = b_0 + b_1X + \cdots + b_mX^m$. Soit $0 \leq k \leq n$ tel que p divise $a_0, \ldots, a_{k-1}$ mais p ne divise pas a_k : un tel indice existe puisque f est primitif. Similairement, comme g est primitif, il existe un indice $0 \leq \ell \leq m$ tel que p divise $b_0, \ldots, b_{\ell-1}$ mais p ne divise pas b_ℓ. Le coefficient de degré $k+\ell$ de fg est

$$\underbrace{(a_0b_{k+\ell} + \cdots + a_{k-1}b_{\ell+1})}_{\text{multiple de } p} + a_kb_\ell + \underbrace{(a_{k+1}b_{\ell-1} + \cdots + a_{k+\ell}b_0)}_{\text{multiple de } p},$$

où il faut bien entendu poser $a_i = 0$ pour $i > n$ et $b_j = 0$ pour $j > m$. Comme $p \mid a_i$ pour tout $i < k$, les k termes de gauche sont des multiples de p. Comme $p \mid b_j$ pour tout $j < \ell$, les ℓ termes de droite sont aussi des multiples de p. En revanche, comme p est premier et ne divise ni a_k ni b_ℓ, ce premier p ne divise pas le terme a_kb_ℓ. En conclusion, p ne divise pas le coefficient de degré $k+\ell$ de fg. □

Cette version du lemme de Gauss implique immédiatement le résultat suivant.

Corollaire IV.32. *Si $f, g \in \mathbb{Q}[X]$ sont deux polynômes unitaires dont le produit est dans $\mathbb{Z}[X]$, alors on a $f \in \mathbb{Z}[X]$ et $g \in \mathbb{Z}[X]$.*

Démonstration. Comme le polynôme $f \in \mathbb{Q}[X]$ est unitaire, il existe $a \in \mathbb{Z}_{>0}$ tel que $f_1 := af \in \mathbb{Z}[X]$ est primitif. (C'est un exercice facile.) De même, il existe $b \in \mathbb{Z}_{>0}$ tel que $g_1 := bg \in \mathbb{Z}[X]$ est primitif. Par le Lemme IV.31, leur produit $f_1g_1 = ab(fg) \in \mathbb{Z}[X]$ est également primitif. Comme fg est élément de $\mathbb{Z}[X]$ et a, b sont des entiers positifs, cela implique $a = b = 1$, d'où $f = f_1 \in \mathbb{Z}[X]$ et $g = g_1 \in \mathbb{Z}[X]$. □

Nous aurons également besoin du lemme suivant, dont la preuve est laissée en exercices.

Lemme IV.33. *Pour tout $f \in \mathbb{F}_p[X]$, on a l'égalité $f(X)^p = f(X^p)$.* □

Démonstration du Théorème IV.29. Soit donc $n \geq 1$ fixé, et soit $f \in \mathbb{Q}[X]$ le polynôme minimal de $\omega = \exp(2i\pi/n) \in \mathbb{C}$ sur $\mathbb{Q}$. Le but est de montrer l'égalité $f = \Phi_n$, ce qui impliquera que $\Phi_n \in \mathbb{Q}[X]$ est irréductible.

Comme $\Phi_n(\omega) = 0$, on a $f \mid \Phi_n$ dans $\mathbb{Q}[X]$: il existe $g \in \mathbb{Q}[X]$ tel que $\Phi_n = fg$. De plus, comme f et Φ_n sont unitaires, il en va de même pour g. Par le Corollaire IV.32, on a $\Phi_n = fg \in \mathbb{Z}[X]$ avec $f \in \mathbb{Z}[X]$ et $g \in \mathbb{Z}[X]$.

L'affirmation clé est la suivante : si p est un nombre premier tel que $p \nmid n$, et si $f(\omega^\ell) = 0$ pour un $\ell \in \mathbb{Z}$ tel que $\mathrm{pgcd}(\ell, n) = 1$, alors $f(\omega^{p\ell}) = 0$. Cette affirmation implique le théorème de la façon suivante. Pour tout $1 \leq k \leq n$ avec $\mathrm{pgcd}(k, n) = 1$, on peut décomposer $k = p_1 \cdots p_r$ avec $p_1, \ldots, p_r$ premiers (pas nécessairement distincts) tels que $p_i \nmid n$ pour tout i. Comme $f(\omega) = 0$, l'affirmation appliquée à $\ell = 1$ et $p = p_1$ implique $f(\omega^{p_1}) = 0$. Ensuite, l'affirmation

appliquée à $\ell = p_1$ et $p = p_2$ implique $f(\omega^{p_1 p_2}) = 0$. Après r application successives de cette affirmation, nous pouvons conclure que $f(\omega^{p_1 \cdots p_r}) = f(\omega^k) = 0$. Nous avons ainsi trouvé $\varphi(n)$ racines distinctes de f (les racines primitives $n^{\text{ièmes}}$ de l'unité), d'où $\deg(f) \geq \varphi(n) = \deg(\Phi_n)$. Comme f divise Φ_n et tous les deux sont unitaires, on obtient bien l'égalité $\Phi_n = f$, qui implique le théorème.

La preuve de l'affirmation se fait par l'absurde : supposons qu'il existe $\ell \in \mathbb{Z}$ tel que $\operatorname{pgcd}(\ell, n) = 1$ et un premier p tel que $p \nmid n$ et $f(\omega^\ell) = 0$ mais $f(\omega^{p\ell}) \neq 0$. Comme $\operatorname{pgcd}(p\ell, n) = 1$, on a $0 = \Phi_n(\omega^{p\ell}) = f(\omega^{p\ell}) g(\omega^{p\ell})$, d'où $g(\omega^{p\ell}) = 0$. Ainsi, ω^ℓ est racine de $g(X^p) \in \mathbb{Z}[X]$. Mais comme $f(\omega^\ell) = 0$ avec $f \in \mathbb{Q}[X]$ irréductible, le polynôme $g(X^p)$ est un multiple de f : il existe $h \in \mathbb{Q}[X]$ tel que $g(X^p) = f(X)h(X)$. Comme $f, g \in \mathbb{Z}[X]$ sont unitaires, il en va de même pour $h \in \mathbb{Q}[X]$. Une nouvelle application du Corollaire IV.32 donne $h \in \mathbb{Z}[X]$. On a donc l'égalité $g(X^p) = f(X)h(X)$ avec $f, g, h \in \mathbb{Z}[X]$. En notant $\overline{f}, \overline{g}, \overline{h} \in \mathbb{F}_p[X]$ leurs projections, le Lemme IV.33 implique l'égalité

$$\overline{f}\,\overline{h} = \overline{g}^p \in \mathbb{F}_p[X]\,.$$

Toujours à la recherche d'une contradiction, rappelons que comme $\mathbb{F}_p$ est un corps, l'anneau $\mathbb{F}_p[X]$ est principal, ce qui implique qu'il est factoriel (Théorème III.13) et que les premiers coïncident avec les irréductibles. Ainsi, le polynôme $\overline{f} \in \mathbb{F}_p[X]$ admet un facteur premier (unitaire) $\overline{q} \in \mathbb{F}[X]$. Comme $\overline{q}$ premier divise $\overline{f}\,\overline{h} = \overline{g}^p$, on obtient que $\overline{q}$ divise $\overline{g}$. Comme $\overline{q} \mid \overline{f}$ et $\overline{q} \mid \overline{g}$, on a $\overline{q}^2 \mid \overline{f}\overline{g} = \overline{\Phi}_n$. Par Lemme IV.27(i) (projeté de $\mathbb{Z}[X]$ dans $\mathbb{F}_p[X]$), on obtient $\overline{q}^2 \mid X^n - 1 \in \mathbb{F}_p[X]$. Ainsi, il existe $\overline{r} \in \mathbb{F}_p[X]$ tel que

$$X^n - 1 = \overline{q}^2 \overline{r} \in \mathbb{F}_p[X]\,.$$

La dérivée formelle de cette égalité donne

$$\overline{n} X^{n-1} = \overline{2}\overline{q}\,\overline{q}'\overline{r} + \overline{q}^2\overline{r}' = \overline{q}(\overline{2}\overline{q}'\overline{r} + \overline{q}\,\overline{r}') \in \mathbb{F}_p[X]\,.$$

Comme p ne divise pas n, on a $\overline{n} \neq 0 \in \mathbb{F}_p$. Ainsi, l'égalité ci-dessus dans l'anneau factoriel $\mathbb{F}_p[X]$ implique que les facteurs irréductibles unitaires du côté droit sont égaux à X ; en particulier, on a $\overline{q} = X$, d'où $X = \overline{q} \mid X^n - 1$, ce qui est absurde puisque 0 n'est pas une racine de $X^n - 1 \in \mathbb{F}_p[X]$. □

Cette preuve est l'une des plus techniques de ce cours, mais le jeu en valait la chandelle : les applications vont maintenant tomber comme des fruits mûrs.

Corollaire IV.34. *Pour tout $n \geq 1$, le nombre complexe $\omega = \exp(2i\pi/n)$ est algébrique sur $\mathbb{Q}$, de degré $\deg_{\mathbb{Q}}(\omega) = \varphi(n)$.*

Démonstration. Comme $\Phi_n(\omega) = 0$ avec $\Phi_n \in \mathbb{Q}[X]$ irréductible et unitaire, il s'agit du polynôme minimal de ω sur $\mathbb{Q}$, d'où $\deg_{\mathbb{Q}}(\omega) = \deg(\Phi_n) = \varphi(n)$. □

Corollaire IV.35. *Pour tout $n \geq 1$, l'extension*[6] *$\mathbb{Q} \subset \mathbb{Q}(\omega)$ avec $\omega = \exp(2i\pi/n)$ est une extension galoisienne, de groupe de Galois*

$$\operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \simeq (\mathbb{Z}/n\mathbb{Z})^*\,.$$

6. Habituellement appelée *extension cyclotomique*.

Démonstration. Le corps $\mathbb{Q}(\omega) = \mathbb{Q}(\omega, \omega^2, \ldots, \omega^n)$ est le corps des racines du polynôme $X^n - 1 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$. Par la Proposition III.69 et le Théorème IV.10, l'extension $\mathbb{Q} \subset \mathbb{Q}(\omega)$ est donc bien galoisienne. Par ce même théorème et le Corollaire IV.34, on a

$$|\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega))| = [\mathbb{Q}(\omega) : \mathbb{Q}] = \deg_{\mathbb{Q}}(\omega) = \varphi(n) = |\,(\mathbb{Z}/n\mathbb{Z})^*\,|\,,$$

où $(\mathbb{Z}/n\mathbb{Z})^* = \{[k] \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{pgcd}(k, n) = 1\}$. Comme ω est racine de $\Phi_n \in \mathbb{Q}[X]$, la Remarque IV.2.2 implique que tout $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega))$ envoie ω sur une racine de Φ_n, donc un nombre complexe de la forme ω^k avec $[k] \in (\mathbb{Z}/n\mathbb{Z})^*$. Ainsi, on a une application

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*\,, \quad \sigma \longmapsto [k] \text{ tel que } \sigma(\omega) = \omega^k\,.$$

C'est clairement un homomorphisme de groupes, qui est injectif car tout automorphisme $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega))$ est entièrement déterminé par $\sigma(\omega)$, voir Remarque IV.2.4. Finalement, l'égalité $|\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega))| = |\,(\mathbb{Z}/n\mathbb{Z})^*\,|$ implique qu'il s'agit d'un homomorphisme bijectif, et donc d'un isomorphisme. □

Les remarques suivantes nous seront utiles en Section IV.5.

Remarques IV.36.

1. Plus généralement, étant donné un corps K de caractéristique nulle, on peut considérer le corps des racines $K \subset M$ de $X^n - 1 \in K[X]$. Comme ce polynôme est séparable, il admet n racines qui forment le sous-groupe

   $$\mu_n(M) := \{\omega \in M \mid \omega^n = 1\}$$

   de M^*. Par une généralisation immédiate du Théorème III.1, le groupe $\mu_n(M)$ est cyclique. On a donc une extension galoisienne $K \subset M = K(\omega)$ pour tout générateur $\omega \in M$ de $\mu_n(M)$: on dit que ω est une *racine primitive* $n^{ième}$ *de l'unité* dans M.
2. La preuve du Corollaire IV.35 s'étend mot à mot pour montrer qu'il existe un homomorphisme de groupes injectif[7] $\mathrm{Gal}_K(K(\omega)) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$. En particulier, le groupe $\mathrm{Gal}_K(K(\omega))$ est toujours abélien.

Nous sommes finalement en mesure de présenter l'une des plus belles applications de la théorie de Galois : une preuve magnifique du *Théorème de Gauss-Wantzel* qui caractérise les polygones réguliers constructibles à la règle et au compas, résolvant ainsi un problème plusieurs fois millénaire.

Nous allons commencer par énoncer et démontrer ce résultat, avant d'en esquisser la passionnante histoire sous forme d'une suite de remarques.

Théorème IV.37: Théorème de Gauss-Wantzel

Pour $n \geq 3$, le n-gone régulier est constructible à la règle et au compas si et seulement $n = 2^j p_1 \cdots p_r$ pour des entiers $j, r \geq 0$, où $p_1, \ldots, p_r$ sont des

7. Un isomorphisme si et seulement si $\deg_K(K(\omega)) = \varphi(n)$, ce qui n'est pas toujours le cas.

premiers distincts de la forme $p_i = 2^{2^{k_i}} + 1$ avec $k_i \geq 0$ entier.

Démonstration. Supposons pour commencer que $n \geq 3$ est tel que le n-gone régulier est constructible à la règle et au compas à partir de $S = \{0,1\}$. Dans ce cas, on a $\omega = \exp(2i\pi/n) \in \mathscr{C}(\{0,1\})$. Par les Corollaires III.44 et IV.34, cela implique que $\deg_{\mathbb{Q}}(\omega) = \varphi(n)$ est une puissance de 2. En général, si la décomposition en produits de premiers distincts de n est de la forme $n = 2^j p_1^{\nu_1} \cdots p_r^{\nu_r}$ avec $p_1, \ldots, p_r$ des premiers impairs distincts, alors on sait par la Remarque IV.25 qu'on a $\varphi(n) = 2^{j-1}(p_1-1)p_1^{\nu_1-1} \cdots (p_r-1)p_r^{\nu_r-1}$. Si cet entier est une puissance de 2, alors on a nécessairement $\nu_1 = \cdots = \nu_r = 1$ et $p_i = 2^{s_i} + 1$ pour un certain entier $s_i > 0$ pour tout $1 \leq i \leq r$. Il reste à remarquer que si l'on peut écrire $s = k\ell$ avec $k \in \mathbb{Z}_{>0}$ et $\ell > 1$ impair, alors

$$2^s + 1 = 2^{k\ell} + 1 = \underbrace{(2^k + 1)}_{>1 \text{ puisque } k>0} \underbrace{(2^{k(\ell-1)} - 2^{k(\ell-2)} \pm \cdots - 2^k + 1)}_{>1 \text{ puisque } \ell > 1}$$

n'est jamais un nombre premier. Ainsi, pour que chaque $p_i = 2^{s_i} + 1$ soit un premier, il est nécessaire que chaque s_i soit une puissance de 2.

Supposons réciproquement que la décomposition de $n \geq 3$ en produit de premiers distincts soit de la forme $n = 2^j p_1 \cdots p_r$ avec $p_i = 2^{2^{k_i}} + 1$. Par le calcul ci-dessus, $\varphi(n)$ est une puissance de 2, disons $\varphi(n) = 2^m$, et il faut trouver une tour d'extensions comme dans le Théorème de Wantzel (Théorème III.43) : un jeu d'enfants avec la correspondance de Galois. En effet, par le Corollaire IV.35, l'extension $\mathbb{Q} \subset \mathbb{Q}(\omega)$ est galoisienne, et son groupe de Galois d'ordre $\varphi(n) = 2^m$. Par des applications successives de la Proposition II.97 avec $p = 2$, il existe une chaîne de sous-groupes

$$\{e\} = H_m < H_{m-1} < \cdots < H_1 < H_0 = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega))$$

avec $|H_i| = 2^{m-i}$ pour tout $0 \leq i \leq m$. Par Lagrange, on a donc $[H_{i-1} : H_i] = 2$ pour tout i. Par la correspondance de Galois (Théorème IV.17), la tour d'extensions

$$\mathbb{Q} = L^{H_0} \subset L^{H_1} \subset \cdots \subset L^{H_{m-1}} \subset L^{H_m} = \mathbb{Q}(\omega) \ni \omega$$

satisfait $[L^{H_i} : L^{H_{i-1}}] \overset{(IV.4)}{=} [H_{i-1} : H_i] = 2$ pour tout $0 \leq i \leq m$. Le Théorème III.43 implique alors $\omega \in \mathscr{C}(\{0,1\})$, et la donnée de $\omega = \exp(2i\pi/n)$ permet facilement de construire le n-gone régulier, ce qui conclut la preuve. □

Remarques IV.38.

1. Les nombres de la forme $F_k = 2^{2^k} + 1$ avec $k \geq 0$ entier sont appelés les *nombres de Fermat*. Ils tirent leur nom de Pierre de Fermat, qui remarque en 1640 que
$$F_0 = 3\,, \quad F_1 = 5\,, \quad F_2 = 17\,, \quad F_3 = 257\,, \quad F_4 = 65\,537$$
sont tous premiers, et conjecture que F_k est premier pour tout $k \geq 0$. C'est le jeune Leonhard Euler qui réfute cette conjecture en 1732, en calculant :
$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417\,.$$

Pierre de Fermat (1607-1665)

Leonhard Euler (1707-1783)

Aux dernières nouvelles, on sait que F_k n'est pas premier pour $5 \leq k \leq 32$, et l'on conjecture qu'aucun n'est premier pour $k \geq 5$.

Ainsi, on conjecture que les seuls polygones réguliers à nombre impair de côtés sont les 31 correspondant aux produits d'un nombre non-nul d'éléments de $\{3, 5, 17, 257, 65\,537\}$.

Voici une liste avec en bleu les entiers $3 \leq n \leq 60$ tels que le n-gone régulier est constructible, et en rouge les autres :

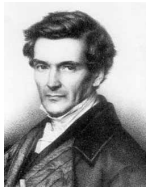
3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60.

2. La construction du 3-gone régulier, plus connu sous le nom de triangle équilatéral, est connu depuis l'Antiquité : il s'agit même de la toute première proposition des *Éléments* d'Euclide. Ce livre contient également une construction du 5-gone régulier (*pentagone*).

   Il fallu attendre près de 2000 ans et le génie du jeune Carl Friedrich Gauss, pour que ce problème avance : en 1796 (à l'âge de 19 ans), il parvient à construire le 17-gone régulier (ou *heptadécagone*) à la règle et au compas. Deux ans plus tard, dans ses fameuses *Disquisitiones Arithmeticae* (seulement publiées en 1801), il rédige une démonstration de la partie constructive du Théorème IV.37 : si $\varphi(n)$ est une puissance de 2, alors le n-gone régulier est constructible. Bien entendu, cette démonstration repose sur l'étude par Gauss des polynômes cyclotomiques, en particulier via le lemme qui porte son nom. Il est remarquable de noter que ce résultat a été obtenu par Gauss avant l'émergence de la théorie de Galois et la formalisation de la théorie des groupes.

Carl Friedrich Gauss (1777-1855)

3. Gauss avait annoncé que sa condition suffisante est également nécessaire, mais n'en avait pas donné de preuve. C'est en 1837 que Pierre-Laurent Wantzel démontre le théorème qui porte son nom (Théorème III.43), et en déduit la réciproque du résultat de Gauss.



Pierre-Laurent Wantzel (1814-1848)

4. Un aspect remarquable de la théorie de Galois, sur laquelle nous n'aurons malheureusement pas le loisir d'insister suffisamment, est sa qualité *explicite* et *constructive*. Dans le cas des polygones, la théorie de Galois ne nous donne pas seulement l'existence d'une construction à la règle et au compas de certains d'entre eux : elle permet d'obtenir une méthode explicite de construction. En effet, étant donné n tel que $\varphi(n) = 2^m$, il suffit de trouver une suite de sous-groupes $\{e\} = H_m < H_{m-1} < \cdots < H_1 < H_0 = (\mathbb{Z}/n\mathbb{Z})^*$ d'indices successifs 2, d'utiliser la correspondance de Galois pour déterminer les extensions correspondantes $\mathbb{Q} = L^{H_0} \subset L^{H_1} \subset \cdots \subset L^{H_{m-1}} \subset L^{H_m} = \mathbb{Q}(\omega)$, puis le théorème de Wantzel pour en déduire une construction de ω à la règle et au compas.

   On verra l'exemple du pentagone en exercices. La construction explicite du 17-gone avec cette méthode est très bien expliquée dans cet article Wikipedia. Les premières constructions explicites du 257-gone ont été accomplie par Magnus Georg Paucker en 1822 et Friedrich Richelot en 1832. Finalement, une

Johann Gustav Hermes (1846-1912)

construction du 65 537-gone a été explicitée par Johann Gustav Hermes en 1894, ce qui lui a pris 10 ans de travail [8].

IV.4 Applications diverses

Avant de se plonger dans le problème de la résolubilité des équations par radicaux, nous allons illustrer la puissance de la théorie de Galois avec des preuves concises et très élégantes de résultats qui vous sont familiers : le théorème fondamental de l'algèbre et le théorème de l'élément primitif.

Bien entendu, il est impossible de donner une démonstration purement algébrique du théorème fondamental de l'algèbre, puisque la définition du corps des complexes se base sur celle du corps des réels, qui est de nature analytique. Néanmoins, il est possible de s'en approcher en utilisant un résultat élémentaire d'analyse, que voici.

Adrien-Marie Legendre (1752-1833)

Lemme IV.39. *Tout polynôme dans $\mathbb{R}[X]$ de degré impair possède une racine dans $\mathbb{R}$.* □

Il est intéressant de noter que la preuve qui suit est essentiellement due à Adrien-Marie Legendre [9], mais que la démonstration d'origine comportait des lacunes qui ont été comblées plus tard à l'aide de la théorie de Galois et de la théorie des groupes.

Cette preuve repose également sur le résultat facile suivant, dont la vérification est laissée en exercices.

Lemme IV.40. *Le corps des complexes n'admet pas d'extension de degré 2.* □

Voici donc cette fameuse preuve.

Démonstration du Théorème III.10. Soit $f \in \mathbb{C}[X]$ un polynôme et soit $\mathbb{C} \subset M$ son corps des racines sur $\mathbb{C}$. Il s'agit de vérifier que $\mathbb{C} = M$, ce qui implique que toutes les racines de f sont dans $\mathbb{C}$: une des formulations possibles du théorème fondamental de l'algèbre que nous tentons de démontrer.

Considérons l'extension $\mathbb{R} \subset M$, qui est finie puisque $\mathbb{C} \subset M$ est finie, mais pas nécessairement galoisienne. Pour y remédier, considérons $a_1, \dots, a_n \in M$ tels que $M = \mathbb{R}(a_1, \dots, a_n)$, soient $g_i \in \mathbb{R}[X]$ le polynôme minimal de a_i sur $\mathbb{R}$, et $\mathbb{R} \subset L$ le corps des racines de $g_1 \cdots g_n \in \mathbb{R}[X]$ sur $\mathbb{R}$. Notons l'inclusion $M = \mathbb{R}(a_1, \dots, a_n) \subset L$ puisque L contient $\mathbb{R}$ et tous les a_i. On a donc une tour d'extensions

$$\mathbb{R} \subset \mathbb{C} \subset M \subset L\,.$$

Comme L est le corps des racines d'un polynôme sur le corps $\mathbb{R}$ de caractéristique nulle, l'extension $\mathbb{R} \subset L$ est bien galoisienne. Nous allons maintenant vérifier l'égalité $\mathbb{C} = L$, ce qui impliquera $\mathbb{C} = M$ et concluera la preuve. Cela se fait en deux étapes, correspondant aux deux termes de la factorisation $[L : \mathbb{R}] = 2^r m$ avec m impair.

8. D'où sa devise : *Geduld ist die Pforte der Freude*.
9. La caricature ci-contre semble être le seul portrait connu de Legendre.

Par le premier théorème de Sylow, il existe un 2-sous-groupe de Sylow H de $G := \mathrm{Gal}_{\mathbb{R}}(L)$, qui est d'ordre 2^r puisque $|G| = [L : \mathbb{R}] = 2^r m$ avec m impair. Considérons le sous-corps fixe associé $\mathbb{R} \subset L^H \subset L$, qui satisfait donc

$$[L^H : \mathbb{R}] = [L^H : L^G] \overset{(IV.4)}{=} [G : H] = \frac{|G|}{|H|} = m\,.$$

Tout $a \in L^H$ a polynôme minimal sur $\mathbb{R}$ de degré $\deg_{\mathbb{R}}(a) = [\mathbb{R}(a) : \mathbb{R}]$ qui divise m impair : il est donc de degré impair. Par le Lemme IV.39, ce polynôme irréductible possède une racine dans $\mathbb{R}$: il est donc de degré 1, ce qui implique $a \in \mathbb{R}$. On a montré $L^H = \mathbb{R}$, et donc $m = 1$.

Ainsi, l'extension galoisienne $\mathbb{R} \subset L$ est de degré une puissance de 2. Par conséquent, il en va de même pour l'extension galoisienne $\mathbb{C} \subset L$, et $\mathrm{Gal}_{\mathbb{C}}(L)$ est un 2-groupe. Supposons par l'absurde que $\mathrm{Gal}_{\mathbb{C}}(L)$ soit non-trivial. Par la Proposition II.97, il admettrait un sous-groupe H' d'indice 2. Par (IV.4), il lui correspondrait une extension $\mathbb{C} \subset L^{H'}$ de degré $[L^{H'} : \mathbb{C}] = [\mathrm{Gal}_{\mathbb{C}}(L) : H'] = 2$, ce qui est impossible par le Lemme IV.40. Ainsi, le groupe $\mathrm{Gal}_{\mathbb{C}}(L)$ est trivial, ce qui par le Théorème IV.10 implique $\mathbb{C} = L$ et conclut la démonstration. □

Remarque IV.41. Un des intérêts de cette démonstration est qu'elle se généralise à des cas non couverts par les preuves traditionnelles du théorème fondamental de l'algèbre. En effet, elle permet de montrer que si K est un *corps ordonné*[10] dans lequel tout élément positif admet une racine carrée et tout polynôme de degré impair a une racine, alors $K[X]/(X^2+1) \simeq K(i)$ est algébriquement clos.

Venons-en à la seconde application de cette brève section.

Théorème IV.42: Théorème de l'élément primitif

Toute extension séparable et finie est une extension simple.

Démonstration. Soit donc $K \subset L$ une extension séparable et finie. Notons que si K est fini, on sait bien que l'extension $K \subset L$ est simple, voir l'Exemple III.23.4. On peut donc supposer que K est infini.

L'affirmation clé est la suivante : si l'on fixe un corps intermédiaire $K \subset K' \subset L$ et deux éléments $a, b \in L$, alors il existe $c \in L$ tel que $K'(a,b) = K'(c)$. Pour montrer cette affirmation, notons tout d'abord que comme $K \subset L$ est finie et séparable, il en va de même pour $K' \subset L$. Par le Corollaire IV.19 (et c'est ici que nous utilisons la correspondance de Galois), il y a un nombre fini d'extensions intermédiaires dans $K' \subset L$. Mais comme K' est infini (puisqu'il contient K qui est infini), il existe $x \neq y \in K'$ tels que $K'(a+xb) = K'(a+yb)$. En particulier, les éléments $a+xb$ et $a+yb$ sont tous deux éléments du sous-corps $K'(a+bx)$. Comme on a supposé $x \neq y \in K'$, on a $x - y \in (K')^* \subset K'(a+bx)^*$, d'où

$$b = (x-y)^{-1}((a+xb) - (a+yb)) \in K'(a+xb)\,,$$

10. Il s'agit d'un corps K muni d'une relation d'ordre total $\leq$ tel que $x \leq y \Rightarrow x+z \leq y+z$ pour tous $x, y, z \in K$ et $x \leq y \Rightarrow xz \leq yz$ pour tous $x, y, z \in K$ avec $z \geq 0$. On vérifie facilement qu'un tel corps est de caractéristique nulle.

ce qui implique également

$$a = (a + bx) - bx \in K'(a + xb)\,.$$

On a donc bien trouvé $c = a + xb \in L$ tel que $a, b \in K'(c)$, d'où l'égalité recherchée $K'(a, b) = K'(c)$.

Retournons maintenant à l'extension $K \subset L$ elle-même. Comme elle est finie, il existe $a_1, \ldots, a_n \in L$ tels que $L = K(a_1, \ldots, a_n)$. Si $n = 1$, il n'y a rien à faire, l'extension est simple. Si $n \geq 2$, on a $L = K'(a_{n-1}, a_n)$ avec $K' = K(a_1, \ldots, a_{n-2})$. Par l'affirmation, il existe $c \in L$ tel que $L = K'(c) = K(a_1, \ldots, a_{n-2}, c)$. En appliquant inductivement cette affirmation, on parvient finalement au cas $n = 1$, et donc à un élément $a \in L$ tel que $L = K(a)$. □

Remarques IV.43.

1. La théorie de Galois a été utilisée de manière minimale dans cette preuve : nous nous sommes uniquement appuyés sur le Corollaire IV.19 qui assure qu'une extension finie et séparable n'admet qu'un nombre fini d'extensions intermédiaires. Il est tout à fait possible de donner des preuves du théorème de l'élément primitif qui ne reposent pas sur la théorie de Galois, puis d'utiliser ce théorème pour simplifier l'exposé de la théorie de Galois. [11]
2. Cette preuve montre que toute extension finie avec un nombre fini d'extensions intermédiaires est simple. On peut montrer la réciproque : une extension finie simple n'admet qu'un nombre fini d'extensions intermédiaires. C'est un exercice.
3. Plus généralement, il est possible de montrer le résultat suivant : si $K \subset L$ est une extension algébrique avec $L = K(a, c_1, \ldots, c_n)$ tel que le polynôme minimal de c_i sur K est séparable pour tout i, alors il existe $c \in L$ tel que $L = K(c)$.
4. Ainsi, si l'on souhaite construire une extension $K \subset L$ finie mais pas simple, le corps K doit être infini de caractéristique p, et elle doit être engendrée par deux éléments dont les polynômes minimaux sur K inséparables. Un exemple est donné par $L = \mathbb{F}_p(X, Y)$, le corps des fractions de l'anneau $\mathbb{F}_p[X, Y]$, et son sous-corps $K = \mathbb{F}_p(X^p, Y^p)$. Par le point 2 ci-dessus, cette extension finie admet un nombre infini d'extensions intermédiaires. Les détails seront vus en exercices.

IV.5 Equations polynomiales résolubles par radicaux

Nous allons conclure ce cours avec l'application la plus spectaculaire la théorie de Galois, à savoir le théorème de Galois qui caractérise les équations polynomiales résolubles par radicaux. De cette manière, nous fermons la boucle initiée dans l'introduction, puisque ce problème nous avait servi de motivation principale.

Bien-sûr, une *équation polynomiale* est une équation de la forme $f(X) = 0$ pour un $f \in K[X]$. La *résolution* de cette équation, c'est la détermination des racines de f. Le but est d'exprimer ces racines en fonction des coefficients de f.

11. Comme l'avait fait Galois lui-même.

Le résultat principal de cette section est le suivant : *une équation polynomiale est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.* Si les termes de cet énoncé ont déjà été utilisés dans l'introduction [12], il s'agit à présent de les définir formellement. Ensuite, nous pourrons formuler le théorème de manière précise, avant de donner quelques préliminaires et l'idée générale de la preuve. Dans un dernier temps, nous donnerons la preuve formelle.

Dans toute cette section, on supposera le corps K de caractéristique nulle. [13]

Le groupe de Galois d'une équation polynomiale

Soit donc K un corps de caractéristique nulle.

Terminologie IV.44. Soit $f \in K[X]$ un polynôme non-nul. Le *groupe de Galois* de f est le groupe $\mathrm{Gal}(f) := \mathrm{Gal}_K(L)$, où $K \subset L$ est un corps des racines de f sur K.

Remarques IV.45.

1. Comme $\mathrm{car}(K) = 0$, le polynôme $f \in K[X]$ est séparable (Proposition III.69). Par le Théorème IV.10, il suit que l'extension $K \subset L$ est galoisienne. Cela justifie la notation $\mathrm{Gal}_K(L)$.
2. L'extension $K \subset L$ n'est pas unique, mais si $K \subset L'$ en est une autre, alors il existe un isomorphisme $\Phi : L \to L'$ tel que $\Phi|_K = \mathrm{id}_K$ (Théorème III.49). Or, on vérifie facilement qu'un tel isomorphisme induit un isomorphisme de groupes $\mathrm{Gal}_K(L) \simeq \mathrm{Gal}_K(L')$. Ainsi, le groupe de Galois $\mathrm{Gal}(f)$ est bien défini à isomorphisme près. En particulier, l'énoncé "$\mathrm{Gal}(f)$ est résoluble" (ou cyclique, abélien,...) fait sens.
3. Si l'on note R les racines de $f \in K[X]$ dans L, alors l'application

$$\mathrm{Gal}(f) \longrightarrow S(R)\,, \quad \varphi \longmapsto \varphi|_R$$

   définit un homomorphisme de groupes injectif (Remarque IV.2.4). Ainsi, on peut interpréter le groupe de Galois de f comme un sous-groupe du groupe des permutations de ses racines.

   Par conséquent, si f est de degré d, alors $\mathrm{Gal}(f)$ est isomorphe à un sous-groupe de S_d.
4. Si $f \in K[X]$ est irréductible, alors $\mathrm{Gal}(f)$ agit transitivement sur les racines. C'est une reformulation du Corollaire III.53.

Exemples IV.46 (groupes de Galois de f)**.**

1. Si $f \in K[X]$ est de degré ≤ 1, alors $\mathrm{Gal}(f) = \mathrm{Gal}_K(K) = \{\mathrm{id}_K\}$ est le groupe trivial.

12. Il est recommandé de relire cette introduction pour se remémorer ce problème.

13. Toutes les définitions et de nombreux résultat restent valides en plus grande généralité, mais cette hypothèse permettra de simplifier légèrement certains énoncés.

2. Soit $f \in K[X]$ de degré 2, sans racine dans K. Alors f est irréductible. Par la Remarque IV.45.4, le groupe $\mathrm{Gal}(f)$ est un sous-groupe de $S(\{a_1, a_2\})$ qui agit transitivement sur $\{a_1, a_2\}$: on a donc forcément $\mathrm{Gal}(f)$ d'ordre 2.
   Par exemple, on a $\mathrm{Gal}(f) \simeq \mathbb{Z}/2\mathbb{Z}$ pour $f = X^2 - 2 \in \mathbb{Q}[X]$ et $f = X^2 + 1 \in \mathbb{R}[X]$.
3. Le groupe de Galois de $f = X^3 - 2 \in \mathbb{Q}[X]$ est $\mathrm{Gal}(f) \simeq S_3$: c'est une conséquence de l'Exemple IV.13.2.
   Plus généralement, si f est irréductible de degré d avec $|\mathrm{Gal}(f)| = d!$, on a nécessairement $\mathrm{Gal}(f) \simeq S_d$ par la Remarque IV.45.3.
4. Le groupe de Galois de $f = X^4 + 1 \in \mathbb{Q}[X]$ est $\mathrm{Gal}(f) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: ce calcul a été fait en Exemple IV.13.3.
   Plus généralement, pour $f = \Phi_n \in \mathbb{Q}[X]$ ou $f = X^n - 1 \in \mathbb{Q}[X]$, on obtient de groupe de Galois $\mathrm{Gal}(f) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ par le Corollaire IV.35.

Le lemme suivant nous sera utile pour donner des exemples explicites d'équations polynomiales non-résolubles par radicaux.

Lemme IV.47. *Si $f \in \mathbb{Q}[X]$ est irréductible de degré p premier avec exactement deux racines dans $\mathbb{C} \setminus \mathbb{R}$, alors $\mathrm{Gal}(f) \simeq S_p$.*

Démonstration. Comme on travaille en caractéristique nulle, la Proposition III.69 nous assure que les racines de f dans $\mathbb{C}$ sont distinctes : notons-les $a_1, \ldots, a_p$, avec $a_1, a_2 \in \mathbb{C} \setminus \mathbb{R}$ et $a_3, \ldots, a_p \in \mathbb{R}$. Nous sommes donc en présence d'une extension galoisienne $\mathbb{Q} \subset \mathbb{Q}(a_1, \ldots, a_p) = L \subset \mathbb{C}$, et d'un homomorphisme injectif de groupes

$$\mathrm{Gal}(f) = \mathrm{Gal}_{\mathbb{Q}}(L) \longrightarrow S(\{a_1, \ldots, a_p\}) = S_p\,.$$

Il reste à vérifier que cet homomorphisme de restriction est également surjectif.

Notons tout d'abord que la conjugaison complexe $\tau \in \mathrm{Aut}(\mathbb{C})$ fixe $\mathbb{Q}$ et satisfait $\tau(\{a_1, \ldots, a_p\}) = \{a_1, \ldots, a_p\}$. Comme $L = \mathbb{Q}(a_1, \ldots, a_p)$, on a $\tau(L) = L$: la restriction de la conjugaison complexe définit un élément $\tau \in \mathrm{Gal}_{\mathbb{Q}}(L) = \mathrm{Gal}(f)$. Par hypothèse, sa restriction aux racines est la permutation donnée par la transposition élémentaire (a_1, a_2), correspondant à l'élément $(1, 2) \in S_p$.

Ensuite, comme l'extension $\mathbb{Q} \subset L$ est galoisienne et $f \in \mathbb{Q}[X]$ irréductible, on a

$$|\mathrm{Gal}(f)| = |\mathrm{Gal}_{\mathbb{Q}}(L)| = [L : \mathbb{Q}] = [L : \mathbb{Q}(a_1)][\mathbb{Q}(a_1) : \mathbb{Q}] = [L : \mathbb{Q}(a_1)] \cdot p\,.$$

Ainsi, le premier p divise l'ordre de $\mathrm{Gal}(p)$. Par le Théorème de Cauchy (Théorème II.92), il existe $\varphi \in \mathrm{Gal}(f)$ d'ordre p. Comme l'homomorphisme de restriction est injectif, la restriction de φ aux racines est un élément de S_p d'ordre p, donc un p-cycle.

Par conséquent, l'image de l'homomorphisme de restriction $\mathrm{Gal}(f) \to S_p$ contient la transposition $(1, 2)$ et un p-cycle. Comme ces deux éléments engendrent S_p, cet homomorphisme est bien surjectif. □

Extensions par radicaux

Venons-en au second terme technique du théorème de Galois : la résolubilité par radicaux.

Terminologie IV.48. • Une *extension par radicaux* est une extension de la forme

$$K \subset K(b_1) \subset K(b_1, b_2) \subset \cdots \subset K(b_1, b_2, \ldots, b_r) = E$$

telle que pour tout $1 \leq i \leq r$, il existe un entier $n_i \geq 1$ avec $b_i^{n_i} \in K(b_1, \ldots, b_{i-1})$.

• Soit $f \in K[X]$, et soit $K \subset L$ son corps des racines sur K. Le polynôme[14] f est dit *résoluble par radicaux* s'il existe une extension par radicaux $K \subset E$ avec $K \subset L \subset E$.

Remarques IV.49.

1. Dans une extension par radicaux, l'existence d'entiers $n_i \geq 1$ tels que $a_i := b_i^{n_i}$ est un élément de $K(b_1, \ldots, b_{i-1})$ doit être comprise comme le fait que b_i est une racine $n_i^{\text{ième}}$ de $a_i \in K(b_1, \ldots, b_{i-1})$. Ainsi, si l'on écrit $b_i = \sqrt[n_i]{a_i}$, tous les éléments de E peuvent s'écrire à l'aide d'éléments de K, des quatre opérations fondamentales, et des racines $\sqrt[n_1]{\ }, \ldots, \sqrt[n_r]{\ }$.

   Par conséquent, la définition de résolubilité par radicaux formalise la notion vue en introduction : les racines de f appartiennent au corps des racines L contenu dans une extension par radicaux E, donc elles peuvent s'exprimer à partir d'éléments du corps K à l'aide des quatre opérations fondamentales et de racines.
2. Notez qu'on ne demande pas que l'extension $K \subset L$ elle-même soit une extension par radicaux, mais que le corps des racines L soit un corps intermédiaire d'une extension par radicaux $K \subset E$. Cette précision est nécessaire, car le fait que $K \subset E$ soit par radicaux ne garantit pas que $K \subset L$ le soit. Un exemple sera vu en exercices.

Exemples IV.50 (extensions par radicaux)**.**

1. Tout $f \in K[X]$ de degré 1 est résoluble par radicaux. En effet, son corps des racines est l'extension triviale $K \subset K$, qui est une extension par radicaux (avec $r = 0$).
2. Toute extension $K \subset L$ de degré 2 avec $\mathrm{car}(K) \neq 2$ est une extension par radicaux (avec $r = 1$ et $n_1 = 2$) : c'est une reformulation du Lemme III.42. Par conséquent, tout $f \in K[X]$ de degré 2 est résoluble par radicaux, puisque son corps des racines $K \subset L$ satisfait $[L : K] \leq 2$.
3. Le polynôme $f = X^4 + \alpha X^2 + \beta \in \mathbb{Q}[X]$ est résoluble par radicaux. En effet, ses racines sont $\pm\sqrt{-\frac{\alpha}{2} \pm \sqrt{\Delta}}$ avec $\Delta = (\frac{\alpha}{2})^2 - \beta \in \mathbb{Q}$. Ainsi son corps des racines $\mathbb{Q} \subset L$ est donné par l'extension par radicaux

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{\Delta}\right) \subset \mathbb{Q}\left(\sqrt{\Delta}, \sqrt{-\alpha/2 + \sqrt{\Delta}}\right) \subset \mathbb{Q}\left(\sqrt{\Delta}, \sqrt{-\alpha/2 + \sqrt{\Delta}}, \sqrt{-\alpha/2 - \sqrt{\Delta}}\right),$$

   où $n_1 = n_2 = n_3 = 2$.

14. Ou l'équation polynomiale associée $f = 0$.

4. Le polynôme $f = X^n - a \in \mathbb{Q}[X]$ est résoluble par radicaux pour tout $a \in \mathbb{Q}$. En supposant $a \geq 0$, les racines en sont $b\omega, b\omega^2, \ldots, b\omega^n$ avec $b = \sqrt[n]{a} \in \mathbb{R}_{\geq 0}$ et $\omega = \exp(2i\pi/n) \in \mathbb{C}$. Ainsi, le corps des racines est donné par l'extension par radicaux
$$\mathbb{Q} \subset \mathbb{Q}(\omega) \subset \mathbb{Q}(\omega, b)\,,$$
où $n_1 = n_2 = n$.

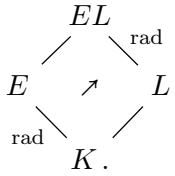
Nous aurons besoin d'un certain nombre d'observations, toutes essentiellement triviales, que nous présentons sous la forme d'une liste de remarques.

Remarques IV.51.

1. Si $K \subset E$ est une extension par radicaux, alors pour toute extension intermédiaire $K \subset L \subset E$, l'extension $L \subset E$ est par radicaux. [15]

   ⌜ En effet, si on a $E = K(b_1, \ldots, b_r)$ avec $b_i^{n_i} \in K(b_1, \ldots, b_{i-1})$ pour tout $1 \leq i \leq r$, alors $E = L(b_1, \ldots, b_r)$ avec $b_i^{n_i} \in K(b_1, \ldots, b_{i-1}) \subset L(b_1, \ldots, b_{i-1})$. ⌟

2. Si $K \subset L$ et $L \subset E$ sont par radicaux, alors $K \subset E$ est clairement par radicaux.
3. Supposons que $K \subset E$ et $K \subset L$ sont deux extensions algébriques d'un même corps K. Rappelons que l'on peut considérer EL, le plus petit sous-corps [16] contenant E et L. Si $K \subset E$ est par radicaux, alors l'extension $L \subset EL$ est aussi par radicaux :



   ⌜ En effet, si $E = K(b_1, \ldots, b_r)$ avec $b_i^{n_i} \in K(b_1, \ldots, b_{i-1})$, alors $EL = L(b_1, \ldots, b_r)$ avec $b_i^{n_i} \in K(b_1, \ldots, b_{i-1}) \subset L(b_1, \ldots, b_{i-1})$. ⌟

Le théorème de Galois et ses conséquences

Nous sommes finalement en mesure d'énoncer le théorème principal de cette section, et d'en explorer quelques conséquences.

Théorème IV.52: Théorème de Galois

Soit $f \in K[X]$ avec K de caractéristique nulle. Alors, f est résoluble par radicaux si et seulement si le groupe $\mathrm{Gal}(f)$ est résoluble.

Remarques IV.53.

15. En revanche, l'extension $K \subset L$ n'est pas nécessairement par radicaux.
16. D'une extension quelconque de K contenant E et L, par exemple la clôture algébrique $\overline{K}$.

1. Comme vous l'avez compris depuis longtemps (voir Remarque II.20.2), c'est l'origine de cette terminologie en théorie des groupes.
2. Notons que l'implication f résoluble $\Rightarrow \mathrm{Gal}(f)$ résoluble est valide sans hypothèse de caractéristique. Mais la réciproque est fausse en général.
3. Les deux implications de ce théorème sont des résultats remarquables. L'implication f résoluble $\Rightarrow \mathrm{Gal}(f)$ résoluble l'est de manière évidente, puisqu'elle permet de donner des exemples explicites d'équations polynomiales non-résolubles (voir Corollaire IV.55 ci-dessous). Mais l'autre implication aussi : en effet, la théorie donne non seulement l'existence d'une solution par radicaux, mais une méthode de construction explicite de cette solution. Nous n'aurons malheureusement pas le temps d'en voir des exemples en détails en cours, juste quelques uns en exercices.

Voici quelques conséquences de ce théorème.

Corollaire IV.54. *Toute équation polynomiale de degré au plus* 4 *est résoluble par radicaux.*

Démonstration. Soit $f \in K[X]$ de degré $d \leq 4$. Par la Remarque IV.45.3, on a un homomorphisme injectif de groupes $\mathrm{Gal}(f) \hookrightarrow S_d < S_4$. Ainsi, le groupe de Galois de f est isomorphe à un sous-groupe de S_4, qui est résoluble par le Théorème II.19. Il est donc lui-même résoluble, d'où f résoluble par le Théorème de Galois. □

Corollaire IV.55. *Si $f \in \mathbb{Q}[X]$ est irréductible de degré $p \geq 5$ premier avec exactement deux racines dans $\mathbb{C} \setminus \mathbb{R}$, alors f n'est pas résoluble par radicaux.*

Démonstration. Par le Lemme IV.47, ces hypothèses impliquent $\mathrm{Gal}(p) \simeq S_p$, qui n'est pas résoluble pour $p \geq 5$ par le Théorème II.19. Par le Théorème de Galois, f n'est pas résoluble par radicaux. □

En voici un exemple concret.

Exemple IV.56. Le polynôme $f = X^5 - 6X + 3 \in \mathbb{Q}[X]$ est irréductible par Eisenstein. De plus, l'étude de la fonction polynomiale $x \mapsto x^5 - 6x + 3$ montre qu'elle possède exactement 3 zéros, d'où exactement 3 racines réelles pour f. Par le Corollaire IV.55, l'équation polynomiale $X^5 - 6X + 3 = 0$ n'est pas résoluble par radicaux.

Terminons cette liste de conséquences avec l'*équation polynomiale générale* de degré d sur K, à savoir le polynôme

$$X^d + t_1 X^{d-1} + \cdots + t_{d-1} X + t_d \in K(t_1, \ldots, t_d)[X] .$$

Notons que ce polynôme a coefficients dans le corps $K(t_1, \ldots, t_d)$: ces coefficients sont considérés comme des variables formelles. Une résolution par radicaux de cette équation polynomiale générale donne donc une formule pour résoudre par radicaux tout polynôme de degré d en fonction de ses coefficients.

Paolo Ruffini (1765-1822)

Une caractérisation des équations polynomiales générales résolubles par radicaux avait été formulée et partiellement démontrée par Paolo Ruffini en 1799, puis démontrée par Niels Abel en 1824. Ce résultat est donc antérieur à la théorie de Galois, mais cette théorie en donne une explication limpide.

Théorème IV.57: Théorème d'Abel-Ruffini

L'équation polynomiale générale de degré d sur K de caractéristique nulle est résoluble par radicaux si et seulement si $d \leq 4$.

Niels Abel (1802-1829)

Idée de la preuve. Au moyen de la théorie des polynômes symétriques, il n'est pas difficile de montrer que l'équation polynomiale générale de degré d a groupe de Galois isomorphe à S_d. Le résultat découle alors des Théorèmes II.19 et IV.52. □

Preuve du théorème de Galois

Avant de donner la preuve formelle du Théorème IV.52, il ne parait pas inutile d'en donner d'abord une preuve "approximative", qui en transmet néanmoins les idées principales.

Soit donc $f \in K[X]$ avec $\mathrm{car}(K) = 0$, et soit $K \subset L$ son corps des racines. Par le Lemme II.23, le groupe $G := \mathrm{Gal}(f) = \mathrm{Gal}_K(L)$ est résoluble si et seulement s'il existe une suite de sous-groupes

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r = \{e\}$$

avec G_{i-1}/G_i cyclique (d'ordre premier) pour tout i. Par la correspondance de Galois, que l'on peut appliquer puisque $K \subset L$ est galoisienne, c'est équivalent à l'existence d'une tour d'extensions

$$K = K_0 \subset K_1 \subset \cdots \subset K_{r-1} \subset K_r = L$$

avec $[K_i : K_{i-1}] = [G_{i-1} : G_i]$ premier, et donc $K_{i-1} \subset K_i$ cyclique, pour tout i. Par une analyse des extensions cycliques à venir [17], pour tout i, il existe $b_i \in K_{i+1}$ et un entier $n_i \geq 1$ tel que $b_i^{n_i} \in K_i$. Ainsi, l'extension $K \subset L$ est par radicaux, ce qui signifie [18] que f est résoluble par radicaux.

Il n'est pas totalement trivial de transformer cette ébauche de preuve en une démonstration rigoureuse. C'est ce que nous allons faire dans la fin de ce cours, qui ne fait pas partie du champ de l'examen.

Il nous faut tout d'abord quelques préliminaires sur les extensions cycliques.

Lemme IV.58. *Soient K un corps de caractéristique nulle, et $n \geq 1$ un entier tel que $X^n - 1$ est scindé sur K. Considérons une extension finie $K \subset L$.*

17. Comme on le verra en Lemme IV.58 ci-dessous, cet énoncé n'est valide que si $X^{n_i} - 1$ est scindé sur K_i, ce qui amène une première complication.

18. Pas tout à fait : il se pourrait que f soit résoluble mais que $K \subset L$ ne soit pas par radicaux (voir Remarque IV.49.2), ce qui amène une seconde complication dans la preuve formelle.

(i) S'il existe $b \in L$ tel que $L = K(b)$ et $b^n \in K$, alors $K \subset L$ est une extension cyclique.

(ii) Si $K \subset L$ est une extension cyclique de degré n, alors il existe $b \in L$ tel que $L = K(b)$ et $b^n \in K$.

Remarque IV.59. Notons que pour un corps K de caractéristique nulle et un entier $n \geq 1$, le polynôme $X^n - 1$ est scindé sur K si et seulement si K contient une racine primitive $n^{\text{ième}}$ de l'unité : cela découle de la Remarque IV.36.1. On utilisera donc ces deux conditions de manière interchangeable.

Démonstration du Lemme IV.58. Soient K un corps de caractéristique nulle et $n \geq 1$ un entier tel que $X^n - 1$ est scindé sur K. Par la Remarque IV.59, il existe $\omega \in K$ tel que $\{\omega^k \mid 1 \leq k \leq n\}$ est l'ensemble des n racines de $X^n - 1$ dans K.

Pour montrer le premier point, soit $b \in L$ tel que $L = K(b)$ et $a := b^n \in K$. Pour tout $1 \leq k \leq n$, on a $\left(\omega^k b\right)^n = (\omega^n)^k b^n = a$, donc $\{\omega^k b \mid 1 \leq k \leq n\}$ est l'ensemble des n racines de $f := X^n - a \in K[X]$ dans L. Ainsi, $K \subset L = K(b)$ est le corps des racines du polynôme séparable $f \in K[X]$: elle est donc galoisienne. Comme $b \in L$ est racine de $f \in K[X]$, tout $\varphi \in \mathrm{Gal}_K(L)$ envoie b sur une racine de f, donc sur $\omega^k b$ avec $[k] \in \mathbb{Z}/n\mathbb{Z}$. On a ainsi une application

$$\mathrm{Gal}_K(L) \longrightarrow \mathbb{Z}/n\mathbb{Z}\,, \quad \varphi \longmapsto [k] \text{ tel que } \varphi(b) = \omega^k b\,.$$

C'est un homomorphisme de groupes, qui est injectif car tout $\varphi \in \mathrm{Gal}_K(L)$ est entièrement déterminé par $\varphi(b)$. Par conséquent, le groupe $\mathrm{Gal}_K(L)$ est un sous-groupe du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$: c'est donc bien un groupe cyclique.

Supposons réciproquement que $K \subset L$ est une extension cyclique de degré n. Ainsi, il existe $\varphi \in \mathrm{Gal}_K(L)$ d'ordre n : les homomorphismes $\mathrm{id}, \varphi, \ldots, \varphi^{n-1} : L \to L$ sont donc tous distincts. Par un exercice, ils sont linéairement indépendants sur L. En particulier, il existe $x \in L$ tel que

$$b := x + \omega\varphi(x) + \omega^2\varphi^2(x) + \cdots + \omega^{n-1}\varphi^{n-1}(x) \neq 0 \in L\,.$$

Comme $\omega^n = 1$ et $\varphi^n = \mathrm{id}$ tandis que $\varphi(\omega) = \omega$ (puisque $\omega \in K$), on calcule facilement $\varphi(b) = \omega^{-1}b$. Ainsi, l'élément $a := b^n \in L$ satisfait

$$\varphi(a) = \varphi(b^n) = \varphi(b)^n = \left(\omega^{-1}b\right)^n = b^n = a\,.$$

Comme φ engendre $\mathrm{Gal}_K(L)$ et l'extension $K \subset L$ est galoisienne, l'élément $a \in L$ est en fait dans $L^{\mathrm{Gal}_K(L)} = K$. Il reste à voir que $L = K(b)$. Pour ce faire, considérons le polynôme minimal $f \in K[X]$ de $b \in L$. Notons que $\varphi \in \mathrm{Gal}_K(L)$ permute les racines de f ; par conséquent, les images $\varphi^k(b) = \omega^{-k}b \in L$ pour $1 \leq k \leq n$ sont des racines de f, qui sont distinctes puisque $b \neq 0$. Il suit

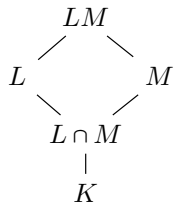
$$[K(b) : K] = \deg_K(b) = \deg(f) \geq n = [L : K] = [L : K(b)][K(b) : K]\,,$$

d'où $[L : K(b)] \leq 1$ et $L = K(b)$. □

Nous sommes finalement en mesure de donner la preuve complète du théorème de Galois.

Démonstration du Théorème IV.52. Soit donc $f \in K[X]$ avec $\mathrm{car}(K) = 0$, et supposons dans un premier temps que $\mathrm{Gal}(f)$ est résoluble. Le groupe $\mathrm{Gal}_K(L)$ est donc résoluble, où L est un corps des racines de f sur K. Soit $K \subset M$ un corps des racines de $X^n - 1 \in K[X]$, où $n = |\mathrm{Gal}_K(L)|$. On a donc $M = K(\omega)$ avec $\omega \in M$ une racine primitive $n^{\text{ième}}$ de

l'unité, ce qui nous permettra d'appliquer le Lemme IV.58. Considérons à présent LM, le plus petit sous-corps [19] contenant L et M. On a donc le treillis suivant :



Par la (fin de la) Remarque IV.18.1, comme $K \subset L$ est galoisienne, il en va de même pour $M \subset LM$, et on a

$$\mathrm{Gal}_M(LM) \overset{(\mathrm{IV}.2)}{\simeq} \mathrm{Gal}_{L\cap M}(L) < \mathrm{Gal}_K(L)\,.$$

Comme $\mathrm{Gal}_K(L)$ est résoluble, le groupe $\mathrm{Gal}_M(LM)$ est également résoluble (voir Remarque II.17.1). Par le Lemme II.23, il existe une suite de sous-groupes

$$\mathrm{Gal}_M(LM) = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{r-1} \triangleright G_r = \{e\}$$

avec G_{i-1}/G_i cyclique pour tout i. Posons $n_i := |G_{i-1}/G_i|$, et notons que n_i divise n, puisque c'est un diviseur de l'ordre du sous-groupe G_{i-1} de $\mathrm{Gal}_M(LM)$, lui même isomorphe à un sous-groupe de $\mathrm{Gal}_K(L)$ d'ordre n. Par la correspondance de Galois, que l'on peut appliquer puisque $M \subset LM$ est galoisienne, il existe une tour d'extensions

$$M = M_0 \subset M_1 \subset \cdots \subset M_{r-1} \subset M_r = LM$$

avec $\mathrm{Gal}_{M_i}(LM) = G_i$ pour tout $0 \le i \le r$. De plus, comme G_i est normal dans G_{i-1}, le Théorème IV.22 nous garantit que l'extension $M_{i-1} \subset M_i$ est galoisienne, avec

$$\mathrm{Gal}_{M_{i-1}}(M_i) \simeq \mathrm{Gal}_{M_{i-1}}(LM)/\mathrm{Gal}_{M_i}(LM) = G_{i-1}/G_i$$

cyclique d'ordre n_i. Ainsi, l'extension $M_{i-1} \subset M_i$ est cyclique de degré n_i. De plus, comme $M_{i-1} \supset M_0 = M = K(\omega)$ et n_i divise n, le corps M_{i-1} contient la racine primitive $n_i^{\text{ième}}$ de l'unité ω^{n/n_i}. Nous sommes donc en mesure d'appliquer le Lemme IV.58(ii) : il existe $b_i \in M_i$ tel que $M_i = M_{i-1}(b_i)$ et $b_i^{n_i} \in M_{i-1}$. Par définition, l'extension $K \subset LM$ est par radicaux via

$$K \subset K(\omega) \subset K(\omega, b_1) \subset \ldots K(\omega, b_1, \ldots, b_r) = LM\,.$$

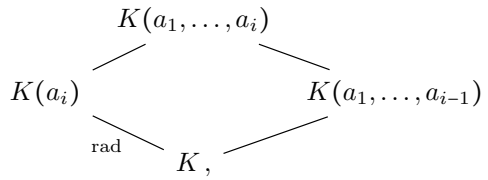
Comme le corps des racines L de f est inclu dans LM, cela signifie que f est résoluble par radicaux.

Supposons réciproquement que $f \in K[X]$ est résoluble par radicaux. Il existe donc une extension par radicaux $K \subset E$ qui admet le corps des racines L de f comme corps intermédiaire. Comme on suppose $\mathrm{car}(K) = 0$, l'extension $K \subset L$ est galoisienne, mais cela n'implique pas que $K \subset E$ le soit. Néanmoins, on peut toujours supposer que $K \subset E$ est galoisienne : c'est l'objet de la première étape, que voici.

Comme $K \subset E$ est une extension finie et séparable (puisque $\mathrm{car}(K) = 0$), le théorème de l'élément primitif garantit l'existence de $c \in E$ tel que $E = K(c)$. Soit $g \in K[X]$ le polynôme minimal de $c \in E$ sur K, et soit $E' = K(a_1, \ldots, a_d)$ le corps des racines de $g \in K[X]$ sur K. Notons que $K \subset E'$ est une extension galoisienne (car corps des racines d'un polynôme séparable), et $E' \supset K(c) = E$ (car $E' \supset K$ et $E' \ni c$). Notons également que comme $K \subset K(c) = E$ est par radicaux, il en va de même pour $K \subset K(a_i)$

19. D'une extension de K contenant L et M, par exemple $\overline{K}$.

pour tout i : cela découle du Corollaire III.29 qui fournit un isomorphisme $K(c) \simeq K(a_i)$ fixant K. Par la Remarque IV.51.3 appliquée au diagramme



l'extension $K(a_1,\dots,a_{i-1}) \subset K(a_1,\dots,a_i)$ est par radicaux pour tout i. Par la Remarque IV.51.2, il en va de même pour $K \subset K(a_1,\dots,a_d) = E'$. Nous avons donc bien une extension par radicaux $K \subset E'$ *galoisienne* qui admet le corps des racines L de f comme corps intermédiaire, ce qui conclut la première étape.

Il existe donc des extensions galoisiennes $K \subset L \subset E$ avec $K \subset E$ par radicaux. Comme $K \subset L$ est galoisienne, le Théorème IV.22 implique l'isomorphisme

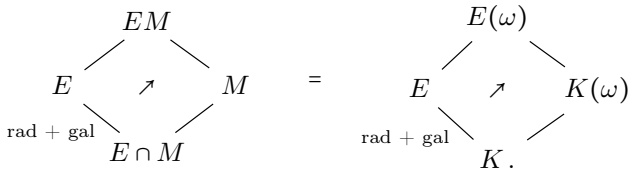
$$\mathrm{Gal}_K(L) \simeq \mathrm{Gal}_K(E)/\mathrm{Gal}_L(E)\,.$$

Ainsi, il nous suffit de montrer que $\mathrm{Gal}_K(E)$ est résoluble, puisque son quotient $\mathrm{Gal}_K(L)$ le sera également via la Proposition II.22. Pour ce faire, rappelons que comme $K \subset E$ est par radicaux, il existe une tour

$$K = K_0 \subset K_1 \subset \cdots \subset K_{r-1} \subset K_r = E$$

telle que $K_i = K_{i-1}(b_i)$ avec $b_i^{n_i} \in K_{i-1}$ pour tout $1 \leq i \leq r$. Nous souhaitons utiliser le Lemme IV.58(i), mais il n'est applicable que si K_{i-1} contient une racine primitive $n_i^{\text{ième}}$ de l'unité. Néanmoins, on peut toujours le supposer : c'est l'objet de la seconde étape.

Posons $n := n_1 \cdots n_r$, et soit $K \subset M$ un corps des racines de $X^n - 1 \in K[X]$. On a donc $M = K(\omega)$ avec $\omega \in M$ une racine primitive $n^{\text{ième}}$ de l'unité. Considérons l'extension $M = K(\omega) \subset E(\omega) = EM$; par les Remarques IV.18.1 et IV.51.3, comme $K = E \cap M \subset E$ est galoisienne et par radicaux, il en va de même pour $M \subset EM$:



De plus, l'extension $K \subset E(\omega)$ est galoisienne. En effet, comme $K \subset E$ est galoisienne, c'est le corps des racines d'un $g \in K[X]$. Par définition, $K \subset K(\omega)$ est le corps des racines de $X^n - 1 \in K[X]$. Il en résulte que $K \subset E(\omega)$ est le corps des racines de $(X^n - 1)g \in K[X]$, et donc bien une extension galoisienne. On peut donc appliquer le Théorème IV.22, qui implique les isomorphismes

$$\mathrm{Gal}_K(K(\omega)) \simeq \mathrm{Gal}_K(E(\omega))/\mathrm{Gal}_{K(\omega)}(E(\omega))$$

et

$$\mathrm{Gal}_K(E) \simeq \mathrm{Gal}_K(E(\omega))/\mathrm{Gal}_E(E(\omega))\,.$$

Rappelons que par la Remarque IV.36.2, le groupe $\mathrm{Gal}_K(K(\omega))$ est abélien (et donc résoluble). Ainsi, si $\mathrm{Gal}_{K(\omega)}(E(\omega))$ est résoluble, alors $\mathrm{Gal}_K(E(\omega))$ est résoluble par le premier isomorphisme et la Proposition II.22. Par une nouvelle application de la Proposition II.22, cette fois au second isomorphisme ci-dessus, cela impliquera que $\mathrm{Gal}_K(E)$

est résoluble et terminera la démonstration. En conclusion de cette seconde étape, quitte à remplacer l'extension galoisienne et par radicaux $K \subset E$ par l'extension galoisienne et par radicaux $K(\omega) \subset E(\omega)$, on peut supposer que K contient une racine primitive $n^{\text{ième}}$ de l'unité ω.

Nous avons donc extension galoisienne $K \subset E$ qui est une tour d'extensions

$$K = K_0 \subset K_1 \subset \cdots \subset K_{r-1} \subset K_r = E$$

telle que $K_i = K_{i-1}(b_i)$ avec $b_i^{n_i} \in K_{i-1}$ pour tout $1 \leq i \leq r$, et K contient une racine primitive $n^{\text{ième}}$ de l'unité ω, où $n = n_1 \cdots n_r$. Ainsi, pour tout $1 \leq i \leq r$, la racine primitive $n_i^{\text{ième}}$ de l'unité ω^{n/n_i} est dans $K \subset K_{i-1}$. Par le Lemme IV.58(i), l'extension $K_{i-1} \subset K_i$ est cyclique. À cette tour d'extensions correspond donc une suite de sous-groupes normaux

$$\mathrm{Gal}_K(E) = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{r-1} \triangleright G_r = \{\mathrm{id}\}$$

avec $G_{i-1}/G_i \simeq \mathrm{Gal}_{K_{i-1}}(E)/\mathrm{Gal}_{K_i}(E) \simeq \mathrm{Gal}_{K_i}(K_{i-1})$ cyclique (et donc abélien) pour tout $1 \leq i \leq r$. Par la Proposition II.21(ii), le groupe $\mathrm{Gal}_K(E)$ est résoluble. Cela conclut la démonstration. □

Exercices

1. Soit $K \subset L$ une extension de degré 2.
   (i) Montrer que le groupe $\mathrm{Aut}_K(L)$ compte au plus deux éléments.
   (ii) Vérifier que si $\mathrm{car}(K) \neq 2$, alors $\mathrm{Aut}_K(L)$ est (cyclique) d'ordre 2.

2. (i) Déterminer le groupe des automorphismes $\mathrm{Aut}(K)$ pour $K = \mathbb{Q}$ et $K = \mathbb{F}_p$.
   (ii) Montrer que $\mathrm{Aut}(L) = \mathrm{Aut}_K(L)$ avec $K = \mathbb{Q}$ (resp. $K = \mathbb{F}_p$) si L est de caractéristique nulle (resp. de caractéristique p).

3. Démontrer la Remarque IV.2.3 : si $f = f_1 \cdots f_m \in K[X]$ avec $f_i \in K[X]$, on a un homomorphisme de groupes

$$\mathrm{Aut}_K(L) \longrightarrow S(R_1) \times \cdots \times S(R_m), \quad \varphi \longmapsto (\varphi|_{R_1}, \ldots, \varphi|_{R_m}),$$

   où $R_i = \{a \in L \mid f_i(a) = 0\}$.

4. Montrer que l'extension

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{2}, \sqrt[7]{2}, \sqrt[9]{2}, \ldots)$$

   est un extension infinie avec groupe d'automorphismes trivial.

5. Soient $K \subset L$ une extension, et H un sous-groupe de $\mathrm{Aut}_K(L)$. Vérifier que

$$L^H := \{a \in L \mid \varphi(a) = a \text{ pour tout } \varphi \in H\}$$

   est un corps intermédiaire de $K \subset L$.

6. Montrer que si $K \subset L$ est une extension finie, alors $|\mathrm{Aut}_K(L)|$ divise $[L : K]$.

7. Soient $K \subset E \subset L$ des extensions. Lesquels des énoncés suivants sont vrais ?

(i) Si $K \subset L$ est galoisienne, alors $K \subset E$ est galoisienne.
(ii) Si $K \subset L$ est galoisienne, alors $E \subset L$ est galoisienne.
(iii) Si $K \subset E$ et $E \subset L$ sont galoisiennes, alors $K \subset L$ est galoisienne.

8. (i) Vérifier que si $K \subset L$ est une extension galoisienne, alors le polynôme minimal f de $a \in L$ sur K est un diviseur irréductible de

$$g = \prod_{\varphi \in \mathrm{Gal}_K(L)} (X - \varphi(a)) \in K[X].$$

(ii) Montrer qu'on a égalité $f = g$ si et seulement si $L = K(a)$.
(iii) Illustrer ces points sur les exemples suivants :
(a) L'extension triviale $K \subset K$.
(b) L'extension $\mathbb{R} \subset \mathscr{C}$ avec $a \in \mathscr{C}$ quelconque.

9. Montrer que le Théorème IV.10 implique une nouvelle preuve très rapide de l'exercice 38 du Chapitre III (si $f \in K[X]$ est de degré d, alors $[L_f : K]$ divise $d!$) dans le cas où f est séparable.

10. Soit $L \subset \mathbb{C}$ le corps des racines de $f = (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$ sur $\mathbb{Q}$.
(i) Calculer le degré de l'extension $\mathbb{Q} \subset L$.
(ii) Déterminer le groupe de Galois $\mathrm{Gal}_{\mathbb{Q}}(L)$.
(iii) Au moyen de l'exercice 8, calculer le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$.

11. Soit $L \subset \mathbb{C}$ le corps des racines de $f = X^4 + 2 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$.
(i) Montrer en une ligne que $\mathrm{Gal}_{\mathbb{Q}}(L) \simeq D_8$ en utilisant l'exercice 35 du Chapitre III et les résultats du cours (y compris Sylow).
(ii) Redémontrer ce résultat "à la main", en vous basant toujours sur le même exercice, mais cette fois en explicitant des générateurs du groupe et en analysant leur action par permutation sur les racines de f dans $L \subset \mathbb{C}$ (placées dans les coins d'un carré).

12. Calculer le groupe de Galois de l'extension $\mathbb{Q} \subset L$, avec $L \subset \mathbb{C}$ le corps des racines du polynôme $f = X^4 - X^2 - 2 \in \mathbb{Q}[X]$.

13. À l'aide de l'exercice 40 du Chapitre III, calculer les groupes de Galois $\mathrm{Gal}_{\mathbb{Q}}(L_f)$ et $\mathrm{Gal}_{\mathbb{F}_2}(L_{\overline{f}})$, où L_f est le corps des racines de $f = X^3 + X^2 + 1$ sur $\mathbb{Q}$ et $L_{\overline{f}}$ le corps des racines de $\overline{f} = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$ sur $\mathbb{F}_2$.

14. Vérifier que la correspondance de Galois renverse les inclusions. En d'autres termes, montrer que pour toute extension $K \subset L$:
(i) si $H \subset H'$ sont deux sous-groupes de $\mathrm{Aut}_K(L)$, alors L^H contient $L^{H'}$;
(ii) si $E \subset E'$ sont deux corps intermédiaires, alors on a $\mathrm{Aut}_{E'}(L) \subset \mathrm{Aut}_E(L)$.

15. Soit $K \subset L$ une extension quelconque.
(i) Vérifier que pour tout $K \subset E \subset L$, on a $E \subset L^{\mathrm{Aut}_E(L)}$.
(ii) Montrer que pour tout sous-groupe H de $\mathrm{Aut}_K(L)$, on a $H < \mathrm{Aut}_{L^H}(L)$.

16. Soit $K \subset L$ une extension quelconque. Pour toutes paires E_1, E_2 de corps intermédiaires et H_1, H_2 de sous-groupes de $\mathrm{Aut}_K(L)$, vérifier les égalités

$$\mathrm{Aut}_{E_1 E_2}(L) = \mathrm{Aut}_{E_1}(L) \cap \mathrm{Aut}_{E_2}(L) \quad \text{et} \quad L^{\langle H_1, H_2 \rangle} = L^{H_1} \cap L^{H_2},$$

avec E_1E_2 le plus petit sous-corps de L qui contient $E \cup E'$ et $\langle H_1, H_2\rangle$ le sous-groupe de $\mathrm{Aut}_K(L)$ engendré par $H_1 \cup H_2$.

17. Décrire le treillis des extensions intermédiaires de $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ pour $n = 24, 30, 64$.

18. À l'aide de l'exercice 12, déterminer le treillis (décoré avec le degré de chaque extension) des corps intermédiaires de l'extension $\mathbb{Q} \subset L$, avec $L \subset \mathbb{C}$ le corps des racines de $f = X^4 - X^2 - 2 \in \mathbb{Q}[X]$.

19. Même question pour le polynôme $f = (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$.

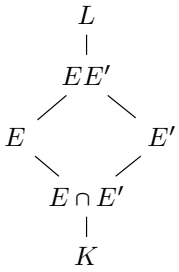
20. Même question pour $X^3 + X^2 + 1 \in \mathbb{Q}[X]$ et pour $X^3 + X^2 + 1 \in \mathbb{F}_2[X]$.

21. Soient $K \subset L$ une extension galoisienne, et $a \in L$. Montrer en deux lignes que $L = K(a)$ si et seulement si le stabilisateur

$$H = \{\varphi \in \mathrm{Gal}_K(L) \mid \varphi(a) = a\}$$

de a dans $\mathrm{Gal}_K(L)$ est trivial.

22. Soit $K \subset L$ une extension finie, et soient E, E' deux corps intermédiaires. Rappelons qu'on peut considérer le plus petit sous-corps de L contenant E et E', noté EE'. On obtient donc le treillis suivant :



Montrer que si $K \subset E$ est galoisienne, alors $E' \subset EE'$ est galoisienne, et la restriction induit un isomorphisme de groupes $\mathrm{Gal}_{E'}(EE') \simeq \mathrm{Gal}_{E\cap E'}(E)$.

23. Reprendre les treillis d'extensions décrits dans les exercices 17–20, et déterminer quelles extensions apparaissant dans ces treillis sont galoisiennes.

24. Soit $K \subset L$ une extension abélienne (resp. cyclique). Montrer que pour tout corps intermédiaire E, les extensions $K \subset E$ et $E \subset L$ sont également abéliennes (resp. cycliques).

25. Soit $K \subset L$ une extension quelconque. Pour toute extension intermédiaire $K \subset E \subset L$ et tout $\varphi \in \mathrm{Aut}_K(L)$, montrer que les deux sous-groupes $\mathrm{Aut}_{\varphi(E)}(L)$ et $\varphi\mathrm{Aut}_E(L)\varphi^{-1}$ de $\mathrm{Aut}_K(L)$ coïncident.

26. Rappelons que la fonction φ d'Euler est la fonction $\varphi\colon \{1, 2, \dots\} \to \{1, 2, \dots\}$ définie par

$$\varphi(n) = \#\{1 \le k \le n \mid \mathrm{pgcd}(k, n) = 1\}\,.$$

Vérifier que si un entier $n > 1$ se décompose en facteurs premiers distincts via $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, alors on a

$$\varphi(n) = (p_1 - 1)p_1^{\nu_1 - 1} \cdots (p_r - 1)p_r^{\nu_r - 1}\,.$$

Indication. Le théorème chinois peut simplifier la résolution de cet exercice.

27. (i) Pour tout $n \geq 1$, vérifier l'égalité $X^{n-1} + \cdots + X + 1 = \prod_{d|n,\, d>1} \Phi_d(X)$.
(ii) Montrer que $\Phi_{2n}(X) = \Phi_n(-X)$ pour tout $n > 1$ impair.
(iii) Pour tout $n \geq 1$ et nombre premier p, vérifier que

$$\Phi_{np}(X) = \begin{cases} \Phi_n(X^p) & \text{si } p|n\,; \\ \Phi_n(X^p)/\Phi_n(X) & \text{sinon}\,. \end{cases}$$

Indication. Pour le second point, considérer la restriction aux racines primitives de l'application $\mu_n(\mathbb{C}) \to \mu_{2n}(\mathbb{C})$ donnée par $\zeta \mapsto -\zeta$. Pour le troisième, faire de même avec l'application $\mu_{np}(\mathbb{C}) \to \mu_n(\mathbb{C})$, $\zeta \mapsto \zeta^p$.

28. Montrer les propriétés suivantes des polynômes cyclotomiques.
(i) $\Phi_n(0) = 1$ pour tout $n \geq 1$.
(ii) $\Phi_n(1) = p$ si $n = p^k$ avec p premier et $k \geq 1$, et $\Phi_n(1) = 1$ sinon.
(iii) Pour tout n, le polynôme Φ_n est *palindromique*, i.e. $X^{\varphi(n)}\Phi_n(1/X) = \Phi_n(X)$.
(iv) $\Phi_n(-1) = 0$ si $n = 2$, $\Phi_n(-1) = 2$ si $n = 2^k$ avec $k \geq 2$, $\Phi_n(-1) = p$ si $n = 2p^k$ avec $k \geq 1$ et p un premier impair, et $\Phi_n(-1) = 1$ sinon.

Indication. Procéder par récurrence en utilisant l'exercice 27.

29. (i) Pour tout $f \in \mathbb{F}_p[X]$, montrer l'égalité $f(X)^p = f(X^p)$.
(ii) Cette égalité est-elle valide pour tout $f \in K[X]$ avec $\mathrm{car}(K) = p$?
(iii) Si K est un corps de caractéristique p, est-ce que *l'homomorphisme de Frobenius* $\varphi\colon K \to K$ défini par $\varphi(x) = x^p$ est toujours un isomorphisme ?

30. Pour tout polynôme $f \in \mathbb{Q}[X]$ unitaire, montrer qu'il existe un entier positif a tel que $af \in \mathbb{Z}[X]$ est primitif.

31. Soit $\omega = e^{2i\pi/5}$.
(i) En utilisant Φ_5, montrer que $\omega + \overline{\omega}$ est racine du polynôme $X^2 + X - 1$.
(ii) En déduire la valeur de $\cos(2\pi/5)$.
(iii) Comment construire le pentagone régulier à la règle et au compas ?

32. Montrer de deux façons que si le n-gone régulier et le m-gone régulier sont constructibles à la règle et au compas, alors le ppcm(n,m)-gone régulier l'est aussi :
(i) via une description explicite de la construction ;
(ii) via le théorème de caractérisation des polygones constructibles.

33. Pour $k \geq 1$ un entier, notons $\omega_k = e^{2i\pi/k} \in \mathbb{C}$.
(i) Montrer que si $m, n \geq 1$ sont premiers entre eux, alors $\mathbb{Q}(\omega_n, \omega_m) = \mathbb{Q}(\omega_{mn})$.
(ii) En déduire qu'avec cette même hypothèse, Φ_n est irréductible dans $\mathbb{Q}(\omega_m)[X]$.
(iii) Identifier l'extension $\mathbb{Q}(\omega_n, \omega_m)$ pour $m, n \geq 1$ arbitraires.

34. (i) Montrer que si $z \in \mathbb{C}$ est constructible à la règle et au compas (à partir de $S = \{0,1\}$), alors pour tout sous-corps $M \subset \mathbb{C}$, le degré $[M(z) : M]$ est une puissance de 2.

(ii) Soit $f \in \mathbb{Q}[X]$ irréductible, et $\mathbb{Q} \subset L_f$ son corps des racines. Montrer qu'une racine z de f est constructible à la règle et au compas si et seulement si le groupe $\mathrm{Gal}(L_f)$ est d'ordre une puissance de 2.

(iii) Montrer que le polynôme $f = X^4 + 8X + 12 \in \mathbb{Q}[X]$ est irréductible. Il s'avère que son groupe de Galois satisfait $\mathrm{Gal}(L_f) \simeq A_4$ (ce que nous ne démontrerons pas).

(iv) Vérifier que toute racine de $X^4 + 8X + 12 \in \mathbb{Q}[X]$ est de degré une puissance de 2, mais n'est néanmoins *pas* constructible à la règle et au compas.

35. Sans utiliser le théorème fondamental de l'algèbre, montrer que le corps des complexes n'admet pas d'extension de degré 2.

36. Un *corps ordonné* est un corps K muni d'un ordre total $\leq$ tel que

(a) $x \leq y \Rightarrow x + z \leq y + z$ pour tous $x, y, x \in K$;

(b) $x \leq y \Rightarrow xz \leq yz$ pour tous $x, y, x \in K$ avec $z \geq 0$.

(i) Montrer que dans un corps ordonné K, on a $x^2 \geq 0$ pour tout $x \in K$.

(ii) Vérifier qu'un corps ordonné est de caractéristique nulle.

37. Soient $K \subset L$ et $K \subset L'$ deux extensions d'un même corps K. Vérifier qu'un isomorphisme de corps $\Phi : L \to L'$ tel que $\Phi|_K = \mathrm{id}_K$ induit un isomorphisme de groupes $\mathrm{Aut}_K(L) \xrightarrow{\sim} \mathrm{Aut}_K(L')$.

38. Soit $K \subset K(a)$ une extension finie simple.

(i) Soient $K \subset L \subset K(a)$ une extension intermédiaire, et $f = \sum_{i=0}^{d} a_i X^i \in L[X]$ le polynôme minimal de a sur L. Vérifier que $L = K(a_0, \ldots, a_d)$.

(ii) En déduire qu'extension intermédiaire $K \subset L \subset K(a)$ est entièrement déterminée par le polynôme minimal de a sur L.

(iii) En conclure qu'une extension finie simple n'admet qu'un nombre fini d'extensions intermédiaires.

39. Dans tout cet exercice, on fixe un premier p et l'on considère l'extension

$$K = \mathbb{F}_p(X^p, Y^p) \subset \mathbb{F}_p(X, Y) = L\,.$$

(i) Montrer qu'il s'agit d'une extension de degré p^2, engendrée par deux éléments.

(ii) Vérifier que pour tout $f \in L$, on a $f^p \in K$.

(iii) Déduire des points précédents que $K \subset L$ n'est pas simple.

(iv) Vérifier qu'elle admet un nombre infini d'extensions intermédiaires.

40. Trouver des extensions de $\mathbb{Q}$ par radicaux contenant les éléments suivants de $\mathscr{C}$:

$$(\sqrt{13} - \sqrt[9]{21})/\sqrt[4]{2}\,, \qquad (\sqrt{7} + 2\sqrt[5]{5})^3\,, \qquad (2\sqrt[5]{7} - 1)/\sqrt{1 + \sqrt{99}}\,.$$

41. Montrer que les polynômes $X^5 - 4X + 2 \in \mathbb{Q}[X]$ et $X^7 - 10X^5 + 15X + 5 \in \mathbb{Q}[X]$ ne sont pas résolubles par radicaux.

42. Soit $\mathbb{Q} \subset E$ le corps des racines de $X^7 - 1 \in \mathbb{Q}[X]$.

(i) Montrer que $\mathbb{Q} \subset E$ est une extension par radicaux.

(ii) Soit $L = \mathbb{Q}(\omega + \omega^{-1})$, où $\omega \in \mathbb{C}$ est une racine primitive $7^{\text{ième}}$ de l'unité. En notant que $\mathbb{Q} \subset L$ est une extension normale avec $L \subset \mathbb{R}$, montrer que $\mathbb{Q} \subset L$ n'est pas une extension par radicaux.

(iii) En déduire l'existence d'un polynôme $f \in \mathbb{Q}[X]$ qui est résoluble par radicaux tandis que son corps des racines $\mathbb{Q} \subset L$ n'est pas une extension par radicaux.

43. Vérifier que si $\varphi_1 \ldots, \varphi_n : L_1 \to L_2$ sont des homomorphismes de corps deux à deux distincts, alors ils forment une famille linéairement indépendante sur L_2.

Indication. Procéder par récurrence sur $n \geq 1$. Pour le pas de récurence, fixer $a \in L_1$ tel que $\varphi_1(a) \neq \varphi_n(a)$ et considérer la combinaison L_2-linéaire des homomorphismes évaluée en $x \in L_1$ et en $ax \in L_1$.

44. Pour un entier $d \geq 2$ fixé, on considère l'équation polynomiale générale de degré d

$$f = X^d + t_1 X^{d-1} + \cdots + t_{d-1} X + t_d \in K[X]$$

avec $K = \mathbb{Q}(t_1, \ldots, t_d)$, dont le groupe de Galois est isomorphe à S_d.
Si l'on note $K \subset L$ son corps des racines sur K et $a_1, \ldots, a_d \in L$ ses racines, le *discriminant* de f est

$$\Delta := \prod_{1 \leq i < j \leq d} (a_i - a_j)^2 \in L\,.$$

(i) Montrer que le discriminant est un élément de K.

(ii) Vérifier que le corps fixe correspondant au sous-groupe A_d de $S_d \simeq \mathrm{Gal}(f)$ est égal à $L^{A_d} = K(\sqrt{\Delta})$, où $\sqrt{\Delta} = \prod_{i<j}(a_i - a_j) \in L$.

(iii) Considérons le cas $d = 2$.

(a) Déduire des points précédents que les deux racines appartiennent à $K(\sqrt{\Delta})$.

(b) En développant l'égalité

$$X^2 + t_1 X + t_2 = (X - a_1)(X - a_2) \in L[X]\,,$$

calculer explicitement $\Delta \in K = \mathbb{Q}(t_1, t_2)$.

(c) Utiliser ces points pour retrouver la formule exprimant les racines a_1, a_2 en fonction des coefficients t_1, t_2.

(iv) Regardons à présent le cas $d = 3$. Soient $a_1, a_2, a_3 \in L$ les trois racines, et posons

$$y := a_1 + \omega a_2 + \omega^2 a_3\,, \quad z := a_1 + \omega^2 a_2 + \omega a_3\,,$$

où ω est une racine primitive troisième de l'unité.

(a) Considérer la suite dérivée $\{\mathrm{id}\} \lhd A_3 \lhd S_3$, et déterminer la tour d'extensions correspondante. Que peut-on en déduire sur les racines a_1, a_2, a_3 ?

(b) Vérifier que les trois racines se calculent en fonction de t_1, y, z via

$$a_1 = \frac{1}{3}(t_1 + y + z)\,, \quad a_2 = \frac{1}{3}(t_1 + \omega^2 y + \omega z)\,, \quad a_3 = \frac{1}{3}(t_1 + \omega y + \omega^2 z)\,.$$

(c) Montrer que $y^3 z^3$ et $y^3 + z^3$ sont des éléments de K.

(d) Déduire des points précédents une stratégie de calcul des racines a_1, a_2, a_3 en fonction des coefficients t_1, t_2, t_3.