Algèbre I
semestre de printemps

David Cimasoni

printemps 2022

Table des matières

Introduction

L'étude de structures algébriques abstraites est suffisamment aride pour mériter une introduction historique. Il existe de multiples façons d'expliquer et de motiver l'apparition de l'algèbre formelle : entre toutes, nous avons choisi de présenter brièvement l'histoire édifiante de la résolution des équations polynomiales, même si vous n'en verrez la conclusion mathématique qu'en ALGÈBRE II.

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 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".

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

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)

Pour comprendre, formaliser, et démontrer ces résultats, il est nécessaire de s'appuyer sur les *structures algébriques abstraites*, dont l'étude constitue ce qu'on appelle habituellement *l'algèbre moderne*. C'est l'objet de ce cours, où nous allons aborder ces structures dans l'ordre suivant : d'abord les *groupes* en chapitre I, puis les *anneaux* en chapitre II, et enfin les *espaces vectoriels et modules* en chapitre III.

Les théorèmes d'Abel et de Galois font partie de la *théorie de Galois*, que vous étudierez en détail en Algèbre II. Mais il va sans dire que l'algèbre moderne a donné lieu à une multitude d'autres applications, dans toutes les branches des mathématiques. En voici quelques exemples.

Topologie algébrique (voir cours Géométrie et topologie) :

- La sphère et le tore, illustrés ci-dessous, ne peuvent pas être déformés continûment l'un en l'autre.

- Dans un polyèdre convexe, on a toujours #sommets − #arêtes + #faces = 2.

Géométrie élémentaire (voir cours Géométrie I et Algèbre II) :

- Avec une règle et un compas, il est impossible de trisecter un angle arbitraire, de dupliquer un cube, ou de construire un carré d'aire égale à l'aire d'un cercle donné [3].
- Il est possible de construire le n-gone régulier à la règle et au compas si et seulement si l'entier $n \geq 3$ est de la forme $n = 2^m p_1 \cdots p_\ell$ pour des entiers $m \geq 0$ et $\ell \geq 0$ et des premiers $p_1, \ldots, p_\ell$ distincts, tous de la forme

$$p = 2^{2^\nu} + 1 \quad \text{pour un certain entier } \nu \geq 0\,.$$

3. C'est la fameuse *quadrature du cercle*.

Un premier de la forme ci-dessus est appelé un *premier de Fermat*. Par exemple, $p = 3, 5, 17, 257, 65537$ sont des premiers de Fermat... en fait, les seuls connus à ce jour !

Théorie des nombres :

Pierre de Fermat (1607-1665)

- *Petit théorème de Fermat* (voir section I.5) : Si p est un nombre premier et a est un entier non-divisible par p, alors $a^{p-1} - 1$ est un multiple de p.
- *Théorème des deux carrés de Fermat* (voir section II.5) : Si p est un nombre premier de la forme $4n + 1$, alors il est somme de deux carrés.
- *Grand théorème de Fermat* (seulement démontré en 1994) : Il n'existe pas d'entiers positifs x, y, z tels que $x^n + y^n = z^n$ avec n un entier supérieur à 2.

Il existe aussi des applications en cryptographie, en combinatoire, en physique, en chimie,...

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 [4]. 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 (voire même, à tout citoyen).

Voici une dernière 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*. Pour cette raison, nous terminerons cette introduction avec un conseil, 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 étudier le violon sans savoir lire une partition, ou à étudier Shakespeare dans le texte sans parler l'anglais : c'est une activité absurde et vouée à l'échec.

4. Voir à ce sujet l'ouvrage *Preuves et réfutations* d'Imre Lakatos. C'est pour rappeler que même la théorie la plus parfaitement formelle est le fruit du travail de mathématiciens de chair et d'os, que sont inclus en marge des portraits de ces derniers.

Chapitre I: Groupes

I.1 Groupes : axiomes et exemples

Commençons sans plus attendre avec la définition d'un groupe.

Définition I.1

Soit G un ensemble muni d'une *loi de composition*, c'est-à-dire d'une application

$$G \times G \longrightarrow G, \quad (g,h) \longmapsto g \star h\,.$$

On dit que G est un **groupe** s'il satisfait les trois axiomes suivants :

(*G1*) *Associativité* : $g \star (h \star k) = (g \star h) \star k$ pour tous $g, h, k \in G$.

(*G2*) *Existence d'un élément neutre* : il existe $e \in G$ tel que $e \star g = g \star e = g$ pour tout $g \in G$.

(*G3*) *Existence d'un inverse* : pour tout $g \in G$, il existe $g' \in G$ tel que $g \star g' = g' \star g = e$.

Si de plus cette loi de composition satisfait l'égalité $g \star h = h \star g$ pour tous $g, h \in G$, alors G est dit **commutatif**, ou **abélien**.
Le cardinal de G, noté $|G|$, est appelé son **ordre**.

Cette définition est bien entendu très abstraite. La meilleure manière de la "comprendre" est de se convaincre que de tels objets se retrouvent un peu partout en mathématiques, d'où l'utilité de les étudier de manière abstraite.

Mais avant de donner une liste de tels exemples, quelques remarques s'imposent.

Remarques et notations.

1. Formellement, un groupe est la donnée d'un couple $(G, \star)$, mais on le note simplement G lorsqu'il n'y a pas de confusion possible.
   On adoptera presque systématiquement la notation gh au lieu de $g \star h$: c'est ce qu'on appelle la *notation multiplicative*.
   Dans le cas abélien, on utilise parfois la *notation additive* $g + h$.

2. L'associativité signifie que lorsque l'on calcule dans un groupe, on peut "laisser tomber les parenthèses". Par exemple, étant donnés quatre élé-

ments $g_1, \dots, g_4$ d'un groupe G, l'associativité implique les identités

$$((g_1g_2)g_3)g_4 = (g_1(g_2g_3))g_4 = g_1((g_2g_3)g_4) = g_1(g_2(g_3g_4)) = (g_1g_2)(g_3g_4)\,,$$

et l'on notera donc simplement cet élément par $g_1g_2g_3g_4$.
Néanmoins, on conservera souvent des parenthèses, mais à des fins presque purement pédagogiques.

3. L'élément neutre est nécessairement unique.

   ⌜ En effet, si e_1 et e_2 sont deux éléments neutres dans un groupe G, alors

   $$e_1 = e_1 \star e_2 = e_2\,,$$

   où la première (resp. seconde) égalité découle du fait que e_2 (resp. e_1) est un élément neutre. ⌟

   Cet unique élément neutre est habituellement noté e, ou e_G en cas de confusion possible. En notation multiplicative, on le note 1 ou 1_G, d'où les égalités $1g = g1 = g$ pour tout $g \in G$. Dans le cas abélien, en notation additive, on l'écrit 0 ou 0_G, d'où les égalités $0+g = g+0 = g$ pour tout $g \in G$.
   Remarquons que l'ensemble vide n'est *pas* un groupe, puisqu'il ne contient pas de neutre.

4. L'inverse d'un élément $g \in G$ fixé est unique.

   ⌜ En effet, si $g', g'' \in G$ sont deux inverses de $g \in G$, alors on a les égalités suivantes dans G :

   $$g' \overset{(G2)}{=} g'e \overset{(G3)}{=} g'(gg'') \overset{(G1)}{=} (g'g)g'' \overset{(G3)}{=} eg'' \overset{(G2)}{=} g''\,,$$

   d'où l'identité $g' = g''$. ⌟

   En notation multiplicative, l'unique inverse de $g \in G$ s'écrit g^{-1}, d'où les égalités $gg^{-1} = g^{-1}g = 1$. Dans le cas abélien, en notation additive, on l'écrit $-g$; on écrit aussi $g + (-h) =: g - h$, d'où l'égalité $g - g = 0$ pour tout $g \in G$.

5. Les règles de calcul suivantes se déduisent des définitions (c'est l'exercice 2) :
   - Pour tous $x, g, h \in G$, si $xg = xh$ ou $gx = hx$, alors $g = h$.
   - Pour tous $g, h \in G$, $(g^{-1})^{-1} = g$ et $(gh)^{-1} = h^{-1}g^{-1}$.

   Dans le cas abélien, en notation additive, elles se traduisent comme suit :
   - Pour tous $x, g, h \in G$, si $x + g = x + h$ alors $g = h$.
   - Pour tous $g, h \in G$, $-(-g) = g$ et $-(g + h) = -g - h$.

6. Étant donné un élément $g \in G$ et un entier $n \in \mathbb{Z}$, la *$n^{ième}$ puissance de g* est l'élément $g^n \in G$ défini comme suit (en notation multiplicative) :

$$g^n = \begin{cases} g \cdots g \quad (n \text{ fois}) & \text{si } n > 0, \\ e & \text{si } n = 0, \\ g^{-1} \cdots g^{-1} \quad (|n| \text{ fois}) & \text{si } n < 0. \end{cases}$$

On montre facilement la troisième règle de calcul suivante (exercice 2) :

- Pour tous $g \in G$ et $n, m \in \mathbb{Z}$, $g^n g^m = g^{n+m}$ et $(g^n)^m = g^{nm}$.

Dans le cas abélien, en notation additive, la $n^{\text{ième}}$ puissance de g se note $n \cdot g$. Par définition, on a donc :

$$n \cdot g = \begin{cases} g + \cdots + g \quad (n \text{ fois}) & \text{si } n > 0, \\ e & \text{si } n = 0, \\ (-g) + \cdots + (-g) \quad (|n| \text{ fois}) & \text{si } n < 0, \end{cases}$$

et la troisième règle de calcul se traduit comme suit :

- Pour tous $g \in G$ et $n, m \in \mathbb{Z}$, $n \cdot g + m \cdot g = (n+m) \cdot g$ et $m \cdot (n \cdot g) = (mn) \cdot g$.

7. Lorsqu'on veut démontrer que $(G, \star)$ est un groupe, il faut vérifier les axiomes $(G1), (G2)$ et $(G3)$, mais aussi que la loi $\star$ est une *loi interne*, c'est à dire qu'elle définit bien une application $G \times G \to G$. En d'autres termes, il faut montrer

$$g, h \in G \Rightarrow g \star h \in G\,.$$

Par exemple, l'ensemble $G = \{-1, 0, 1\}$ muni de l'addition satisfait les trois axiomes, mais n'est néanmoins *pas* un groupe !

Voici enfin et comme promis une liste (de familles) d'exemples.

Exemples (de groupes)**.**

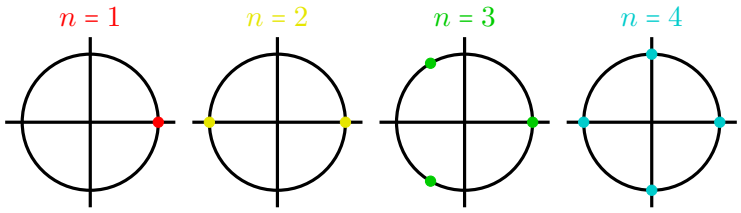
1. *Ensembles de nombres.*
   L'ensemble
   $$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$
   des nombres entiers muni de l'addition est un groupe abélien d'ordre infini. De même, les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition sont des groupes abéliens d'ordre infini. C'est à ces exemples qu'on doit la notation additive dans un groupe abélien.
   Par contre, l'ensemble $\mathbb{N} = \{0, 1, 2, \ldots\}$ des entiers naturels muni de l'addition n'est *pas* un groupe : la loi est bien interne, il satisfait bien les axiomes $(G1)$ et $(G2)$, mais pas $(G3)$, puisqu'aucun élément de $\mathbb{N}$ n'a d'inverse à l'exception du neutre. On parle de *monoïde*.
   L'ensemble $\mathbb{Q}^* \coloneqq \mathbb{Q} \setminus \{0\}$ muni de la multiplication est un groupe abélien d'ordre infini. De même, les ensembles $\mathbb{R}^* \coloneqq \mathbb{R} \setminus \{0\}$ et $\mathbb{C}^* \coloneqq \mathbb{C} \setminus \{0\}$ sont des groupes abéliens (infinis) pour la multiplication, ainsi que $\mathbb{R}_+^* \coloneqq (0, \infty)$.

2. *Espaces vectoriels.*
   Si $(E, +, \cdot)$ est un espace vectoriel sur $K = \mathbb{R}$ ou $\mathbb{C}$, alors $(E, +)$ est un groupe abélien : c'est exactement la signification des premiers quatre axiomes pour un espace vectoriel (qui seront rassemblés en un unique axiome en section III.1).

3. *Groupes de matrices.*
   Pour $n \geq 1$ fixé et $K = \mathbb{R}$ ou $\mathbb{C}$, considérons l'ensemble
   $$\mathrm{GL}(n, K) \coloneqq \{M \in \mathscr{M}_n(K) \mid \det(M) \neq 0\}$$
   des matrices carrées inversibles de taille n à coefficients dans K. Muni de la multiplication matricielle, il forme un groupe appelé le *groupe général linéaire* de degré n de K.
   Notons que pour $n = 1$, on retrouve $\mathrm{GL}(1, K) = K^* = K \setminus \{0\}$, qui est abélien. Le groupe $\mathrm{GL}(n, K)$ n'est en revanche jamais abélien pour $n \geq 2$.
   Similairement, on vérifie facilement que l'ensemble de matrices
   $$\mathrm{SL}(n, K) \coloneqq \{M \in \mathscr{M}_n(K) \mid \det(M) = 1\}$$
   est un groupe pour la multiplication matricielle : il s'agit du *groupe spécial linéaire* de degré n de K. Pour $n = 1$, on trouve $\mathrm{SL}(1, K) = \{(1)\}$, un groupe d'ordre 1. Il s'agit (d'une des "incarnations"[1]) du *groupe trivial*.

4. *Cercle.*
   Considérons l'ensemble
   $$S^1 \coloneqq \{z \in \mathbb{C} \mid ||z|| = 1\}$$
   des nombres complexes de norme 1. Muni de la multiplication complexe, il forme un groupe abélien d'ordre infini.

5. *Racines de l'unité.*
   Soit $n \geq 1$ un entier ; considérons l'ensemble
   $$\mu_n(\mathbb{C}) \coloneqq \{z \in \mathbb{C} \mid z^n = 1\}$$
   des *racines $n^{ièmes}$ de l'unité* dans $\mathbb{C}$, illustré ci-dessous pour $n = 1, 2, 3, 4$.



1. Ce mot recevra un sens précis en section I.3.

Muni de la multiplication complexe, on vérifie que c'est un groupe abélien d'ordre n. Par exemple $\mu_1(\mathbb{C}) = \{1\}$ est une nouvelle incarnation du groupe trivial, tandis que $\mu_2(\mathbb{C}) = \{-1, 1\}$ est un groupe d'ordre 2.
Comme on le verra, le groupe $\mu_n(\mathbb{C})$ est une des incarnations du *groupe cyclique* d'ordre n, voir section I.5.

6. *Groupes symétriques.*
Soit X un ensemble non-vide. Alors, l'ensemble

$$S(X) \coloneqq \{f\colon X \to X \mid f \text{ est bijective}\}$$

muni de la composition des applications est un groupe : cela découle de faits élémentaires vus en LOGIQUE ET THÉORIE DES ENSEMBLES. On notera id ou id_X son neutre, qui est l'application identité. Ce groupe est appelé le *groupe symétrique sur* X. On l'étudiera de manière systématique en section I.6.
Si X est un ensemble fini et que l'on numérote ses éléments $\{1, 2, \dots, n\}$, alors son groupe symétrique est noté S_n. C'est le *groupe des permutations* de n objets, d'ordre $n! = n \cdot (n-1) \cdots 2 \cdot 1$.
On note souvent une permutation $\sigma \in S_n$ par

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Cette notation est un peu encombrante. Pour pouvoir travailler plus efficacement sur ces exemples, nous en introduisons d'ores et déjà une plus légère, qui sera revue de manière plus formelle en section I.6.
On notera simplement $\sigma = (x_1, x_2, \dots, x_r) \in S_n$ la permutation donnée par

$$x_1 \longmapsto x_2 \longmapsto x_3 \longmapsto \dots \longmapsto x_{r-1} \longmapsto x_r \longmapsto x_1$$

et $y \mapsto y$ pour tout $y \in \{1, 2, \dots, n\} \smallsetminus \{x_1, \dots, x_r\}$. On parle de *permutation cyclique* ou de *cycle*. Par exemple, la permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ se note simplement $(1, 2)$, tandis que $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ se note $(1, 2, 3)$. De plus, on va noter $\sigma \circ \tau =: \sigma\tau$ pour tous $\sigma, \tau \in S_n$. Comme toute permutation est composition de cycles (voir section I.6), cela permet une notation très compacte, qu'on utilisera en exercices.
Par exemple, on a $S_1 = \{\mathrm{id}\}$, une nouvelle incarnation du groupe trivial, et $S_2 = \{\mathrm{id}, (1, 2)\}$, un groupe abélien d'ordre 2. Finalement, on a

$$S_3 = \{\mathrm{id}, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$$

un groupe d'ordre $3! = 6$ qui n'est pas abélien. En effet, on vérifie par exemple que $(1, 2)(2, 3) = (1, 2, 3)$ tandis que $(2, 3)(1, 2) = (1, 3, 2)$.

7. *Entiers modulo n.*

Soit $n \geq 1$ un entier fixé. On dit que $a, b \in \mathbb{Z}$ sont *congrus modulo* n, ce que l'on note $a \equiv b \pmod{n}$, si leur différence est un multiple de n :

$$a \equiv b \pmod{n} \quad \Longleftrightarrow \quad a - b \in n\mathbb{Z} \coloneqq \{nk \,|\, k \in \mathbb{Z}\}\,.$$

On vérifie facilement que c'est une relation d'équivalence. La classe d'équivalence de $a \in \mathbb{Z}$ est notée $[a]$. On a donc par définition :

$$[a] \coloneqq \{b \in \mathbb{Z} \,|\, a \equiv b \pmod{n}\} = \{a + nk \,|\, k \in \mathbb{Z}\} =: a + n\mathbb{Z}\,.$$

L'ensemble des classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$. On vérifie facilement

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}\,.$$

Sur cet ensemble, on définit la loi de composition suivante :

$$[a] + [b] \coloneqq [a + b] \quad \text{pour tous } a, b \in \mathbb{Z}\,.$$

Affirmation. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien (d'ordre n).

⌜ Pour démontrer cette affirmation, le point crucial est de vérifier que la loi est *bien définie*, dans le sens qu'elle ne dépend pas du choix des représentants des classes d'équivalence. En d'autres termes, il s'agit de vérifier :

$$[a] = [a'],\ [b] = [b'] \quad \Rightarrow \quad [a + b] = [a' + b']\,.$$

Par définition, la première égalité signifie qu'il existe $k \in \mathbb{Z}$ tel que $a' - a = nk$, et la seconde qu'il existe $\ell \in \mathbb{Z}$ tel que $b' - b = n\ell$. Cela implique

$$(a' + b') - (a + b) = (a' - a) + (b' - b) = nk + n\ell = n(k + \ell) \in n\mathbb{Z}\,,$$

et donc que $[a' + b'] = [a + b]$ comme souhaité. La loi étant clairement interne et commutative, il reste à vérifier les trois axiomes de groupe dans $\mathbb{Z}/n\mathbb{Z}$. En fait, cela découle trivialement des trois axiomes dans $\mathbb{Z}$. En effet, on a

$$([a]+[b])+[c] = [a+b]+[c] = [(a+b)+c] = [a+(b+c)] = [a]+[b+c] = [a]+([b]+[c])$$

pour tous $a, b, c \in \mathbb{Z}$. L'élément neutre est donné par $0_{\mathbb{Z}/n\mathbb{Z}} = [0]$, puisque

$$[0] + [a] = [0 + a] = [a]$$

pour tout $a \in \mathbb{Z}$. Finalement, l'inverse de $[a]$ est donné par $-[a] = [-a]$, puisque

$$[a] + [-a] = [a + (-a)] = [0] = 0_{\mathbb{Z}/n\mathbb{Z}}$$

pour tout $a \in \mathbb{Z}$. Cela termine la preuve de l'affirmation. ⌟

Prenons l'exemple $n = 2$. Deux entiers sont congrus modulo 2 si et seulement s'ils ont même parité. On a $\mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$, avec $[0] = 2\mathbb{Z}$ la classe des nombres pairs et $[1] = 1 + 2\mathbb{Z}$ la classe des nombres impairs. La loi de composition satisfait $[0] + [1] = [1] + [0] = [1]$, $[0] + [0] = [1] + [1] = [0]$, ce qui peut s'interpréter de la façon suivante : l'addition d'un nombre pair avec un nombre impair donne un nombre impair, tandis que l'addition de deux nombres pairs ou de deux nombres impairs donne un nombre pair.

8. *Produit direct.*
   Soient $(G_1, *)$ et $(G_2, \bullet)$ deux groupes. Alors, on vérifie (exercice 10) que le produit cartésien $G_1 \times G_2$ est un groupe pour la loi de composition suivante : pour $g_1, h_1 \in G_1$ et $g_2, h_2 \in G_2$, on pose

$$(g_1, g_2)(h_1, h_2) = (g_1 * h_1, g_2 \bullet h_2) \in G_1 \times G_2 \,.$$

   On parle du *produit direct* de G_1 et G_2.
   Plus généralement, si $G_1, \ldots, G_n$ sont des groupes, alors le produit cartésien $G_1 \times \cdots \times G_n$ est un groupe pour la loi de composition définie composante par composante.
   Par exemple, le groupe abélien $(\mathbb{R}^n, +)$ n'est autre que le produit direct de n copies de $(\mathbb{R}, +)$.
   Un autre exemple est le *groupe de Klein*

$$V \coloneqq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \,,$$

   qui est un groupe abélien d'ordre 4.

FELIX KLEIN (1849-1925)

9. *Groupes de symétrie.*
   Sans entrer dans les détails formels, mentionnons une dernière classe de groupes qui joue un rôle majeur dans le cours GÉOMÉTRIE I. Pour P un sous-ensemble quelconque de l'espace euclidien $\mathbb{R}^n$, l'ensemble

$$\mathrm{Sym}(P) \coloneqq \{f : \mathbb{R}^n \to \mathbb{R}^n \mid f \text{ est une isométrie et } f(P) = P\}$$

   est un groupe pour la composition des applications, appelé le *groupe de symétrie* de P.
   On terminera cet exemple, et cette section, par la citation suivante, due à M.A. Armstrong :

   Numbers measure size, groups measure symmetry.

En conclusion : les groupes se retrouvent partout en mathématique !

I.2 Sous-groupes

Commençons directement par la définition des sous-groupes.

Définition I.2

Un sous-ensemble H d'un groupe G est appelé un **sous-groupe** de G, noté $H < G$, si H est un groupe pour la restriction de la loi de composition de G à H.

De manière plus concrète, un sous-ensemble $H \subset G$ est un sous-groupe de G si et seulement s'il satisfait les trois propriétés suivantes [2].

(1) Pour tous $h_1, h_2 \in H$, on a $h_1 h_2 \in H$.

(2) L'élément neutre e_G appartient à H.

(3) Pour tout élément $h \in H$, son inverse h^{-1} appartient aussi à H.

En fait, ces 3 axiomes sont équivalents à une unique condition, que voici.

Proposition I.1. *Soit G un groupe. Un sous-ensemble non-vide $H \subset G$ est un sous-groupe de G si et seulement si*

$$h_1, h_2 \in H \quad \Rightarrow \quad h_1 h_2^{-1} \in H\,. \tag{$*$}$$

Démonstration. Soit H un sous-ensemble d'un groupe G satisfaisant les conditions $(1), (2), (3)$ ci-dessus ; on veut vérifier la condition $(*)$. Soient donc $h_1, h_2 \in H$; par (3) appliqué à h_2, on a $h_2^{-1} \in H$ et par (1) appliqué à h_1, h_2^{-1}, on conclut l'appartenance $h_1 h_2^{-1} \in H$ comme souhaité.

Vérifions maintenant la réciproque. Soit donc H un sous-ensemble non-vide de G satisfaisant la condition $(*)$. Comme H est non-vide, il existe $h \in H$. Par la condition $(*)$ appliquée à $h_1 = h_2 = h \in H$, le produit $hh^{-1} = e$ appartient à H, et la seconde propriété est vérifiée. Soit à présent $h \in H$ quelconque ; par la condition $(*)$ appliquée à $h_1 = e$ (élément de H par le point précédent) et $h_2 = h \in H$, on a $eh^{-1} = h^{-1} \in H$, et la troisième propriété est vérifiée. Reste la première propriété. Soient donc $h_1, h_2 \in H$; par la condition $(*)$ appliquée à $h_1 \in H$ et h_2^{-1} (élément de H par le point précédent), on a $h_1 (h_2^{-1})^{-1} = h_1 h_2 \in H$, ce qui conclut la démonstration. □

Remarques.

1. Attention : derrière cette unique condition s'en cache une autre, à savoir le fait que H est non-vide. Pour vérifier qu'un sous-ensemble $H \subset G$ est un sous-groupe, on a donc en réalité deux conditions à vérifier.
2. On montre facilement que l'intersection de deux sous-groupes de G est encore un sous-groupe de G (exercice 14).
3. Tout sous-groupe d'un groupe abélien est également abélien.

Nous allons maintenant donner des exemples de sous-groupes, qui font écho aux exemples de groupes vus en section I.1.

Exemples (de sous-groupes)**.**

1. Pour tout groupe G, les sous-ensembles $H = \{e\}$ et $H = G$ sont trivialement des sous-groupes de G. Un sous-groupe $H < G$ qui n'est *pas* de cette forme est appelé un *sous-groupe propre*.
2. On a la suite de sous-groupes suivants : $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$. De même, on a les sous-groupes $(\mathbb{Q}^*, \cdot) < (\mathbb{R}^*, \cdot) < (\mathbb{C}^*, \cdot)$.

2. La preuve de cette équivalence est triviale, à une subtilité près : si l'on suppose que H est un sous-groupe, il admet un élément neutre $e_H \in H$, et il faut montrer l'égalité $e_H = e_G$. Cela se fait via $e_H e_H = e_H = e_H e_G$ et multiplication à gauche par e_H^{-1}.

3. Si E est un espace vectoriel et $F \subset E$ un sous-espace vectoriel, alors $(F,+)$ est un sous-groupe de $(E,+)$.

4. Pour tout entier $n \geq 1$ et $K = \mathbb{R}, \mathbb{C}$, on a $\mathrm{SL}(n,K) < \mathrm{GL}(n,K)$.

5. Pour tout entier $n \geq 1$, on a $\mu_n(\mathbb{C}) < S^1 < \mathbb{C}^*$.

6. Soit X un ensemble non-vide et A un sous-ensemble de X. Alors, les sous-ensembles

$$\{f \in S(X) \,|\, f(A) = A\} \quad \text{et} \quad \{f \in S(X) \,|\, f(a) = a \ \forall a \in A\}$$

sont des sous-groupes de $S(X)$.

7. Pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z} = \{nk \,|\, k \in \mathbb{Z}\}$ des multiples de n est un sous-groupe de $(\mathbb{Z},+)$ (exercice 12). En fait, on montrera en section I.5 que tous les sous-groupes de $\mathbb{Z}$ sont de cette forme !

8. Soit G un groupe quelconque. Alors, le *centre* de G, défini par

$$Z(G) \coloneqq \{h \in G \,|\, gh = hg \ \forall g \in G\},$$

est un sous-groupe de G.

⌜ Pour montrer cette affirmation, nous allons vérifier les trois conditions d'un sous-groupe, la proposition I.1 n'étant pas d'un grand secours sur cet exemple. Soient donc $h_1, h_2 \in Z(G)$; on veut vérifier que $h_1 h_2 \in Z(G)$. Pour tout $g \in G$, on a

$$(h_1 h_2)g = h_1(h_2 g) = h_1(g h_2) = (h_1 g)h_2 = (g h_1)h_2 = g(h_1 h_2)\,,$$

ce qui montre l'appartenance de $h_1 h_2$ à $Z(G)$ et donc la première condition. La seconde se vérifie trivialement, puisque $e\,g = g = g\,e$ pour tout $g \in G$. Pour ce qui est de la troisième, on l'obtient à partir de l'égalité $hg = gh$ valide pour tout $g \in G$ en la multipliant à gauche et à droite par h^{-1} ; on obtient alors l'égalité $gh^{-1} = h^{-1}g$ pour tout $g \in G$, et donc l'appartenance de h^{-1} à $Z(G)$. Cela conclut la preuve de l'affirmation. ⌟

Notons qu'on a $Z(G) = G$ si et seulement si G est abélien.

9. Soit G un groupe quelconque, et fixons $g \in G$. Alors, le *centralisateur* de g dans G, défini par

$$Z_G(g) \coloneqq \{h \in G \,|\, gh = hg\},$$

est un sous-groupe de G [3].

Justifier les faits suivants est un exercice élémentaire de logique et théorie des ensembles [4] :

(a) $Z_G(e) = G$.

(b) $g \in Z(G) \Leftrightarrow Z_G(g) = G$.

(c) $Z(G) = \bigcap_{g \in G} Z_G(g)$.

3. La preuve est la même que pour $Z(G)$: il faut juste ôter les "pour tout g dans G".

4. Il vous est recommandé faire cet exercice pour vérifier que vous êtes à jour avec ces prérequis.

Comment construire des sous-groupes ?

Nous avons donc vu la définition d'un sous-groupe, ainsi qu'une manière pratique de montrer qu'un sous-ensemble donné est un sous-groupe. Mais comment peut-on construire un sous-groupe d'un groupe G donné ?

Voici une méthode générale, qui nous permettra également d'introduire plusieurs notions importantes.

Soit donc G un groupe arbitraire, et soit S un sous-ensemble non-vide de G. Posons

$$H \coloneqq \langle S \rangle = \{g_1 \cdots g_\ell \,|\, \ell \geq 1 \text{ avec } g_i \in S \text{ ou } g_i^{-1} \in S \text{ pour tout } i = 1, \ldots, \ell\}\,.$$

En clair, H est constitué de l'ensemble des compositions d'éléments de S ou de leurs inverses. On va vérifier qu'il s'agit d'un sous-groupe de G, qu'on appelle le *sous-groupe engendré par* S. On dit que S est un *système de générateurs* de H.

⌜ Pour montrer cette affirmation, nous allons utiliser la proposition I.1. Tout d'abord, il est évident que H est non-vide, puisque S est non-vide. Il reste donc à vérifier que si $h_1, h_2 \in H$, alors $h_1 h_2^{-1} \in H$. Par définition de H, il existe $g_1, \ldots, g_\ell$ tels que $h_2 = g_1 \cdots g_\ell$ avec $g_i \in S$ ou $g_i^{-1} \in S$ pour tout $i = 1, \ldots, \ell$; de même, il existe $g'_1, \ldots, g'_m$ tels que $h_1 = g'_1 \cdots g'_m$ avec $g'_j \in S$ ou $(g'_j)^{-1} \in S$ pour tout $j = 1, \ldots, m$. On a donc

$$h_1 h_2^{-1} = (g'_1 \cdots g'_m)(g_1 \cdots g_\ell)^{-1} = g'_1 \cdots g'_m g_\ell^{-1} \cdots g_1^{-1}\,.$$

Comme $(g^{-1})^{-1} = g$, il s'agit d'une composition d'éléments de S ou de leurs inverses ; on a donc bien $h_1 h_2^{-1} \in H$. ⌟

Exemple. Supposons que $S \subset G$ contient un unique élément g. Dans ce cas, le sous-groupe engendré par S est simplement noté $\langle \{g\} \rangle =: \langle g \rangle$, et est donné par

$$\langle g \rangle = \{g_1 \cdots g_\ell \,|\, \ell \geq 1 \text{ avec } g_i = g \text{ ou } g_i^{-1} = g \text{ pour tout } i = 1, \ldots, \ell\} = \{g^n \,|\, n \in \mathbb{Z}\}\,.$$

Ainsi, le sous-groupe engendré par $g \in G$ n'est autre que l'ensemble des puissances de g.

Terminologie. Si G est un groupe tel qu'il existe $g \in G$ avec $G = \langle g \rangle$, alors on dit que G est un *groupe cyclique*.

En clair, un groupe G est cyclique s'il existe $g \in G$ tel que tout élément de G est une puissance de g (i.e. de la forme g^n pour un certain $n \in \mathbb{Z}$ en notation multiplicative, ou de la forme $n \cdot g$ pour un certain $n \in \mathbb{Z}$ en notation additive).

Exemples (de groupes cycliques)**.**

1. Le groupe $\mathbb{Z}$ est un groupe cyclique, engendré par $g = 1$. En effet, tout élément $n \in \mathbb{Z}$ s'écrit $n = n \cdot 1$ avec $n \in \mathbb{Z}$.
2. Pour tout $n \geq 1$, le groupe $\mu_n(\mathbb{C})$ est un groupe cyclique, engendré par $e^{\frac{2i\pi}{n}}$. En effet, tout $z \in \mathbb{C}$ tel que $z^n = 1$ est de la forme $z = (e^{\frac{2i\pi}{n}})^m$ pour un certain $m \in \mathbb{Z}$.

3. Pour tout $n \geq 1$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique, engendré par $[1]$. En effet, on vérifie facilement que tout $[a] \in \mathbb{Z}/n\mathbb{Z}$ s'écrit $[a] = a \cdot [1]$, avec $a \in \mathbb{Z}$.

Terminologie. Soit g un élément fixé d'un groupe G. Alors, $o(g) \coloneqq |\langle g \rangle|$ est appelé l'*ordre de* g dans G.

Comme cette définition est un peu abstraite, tentons de l'exprimer de manière plus concrète. C'est l'objet de la proposition suivante.

Proposition I.2. *(1) Si $o(g)$ est infini, alors $g^n \neq e$ pour tout entier $n > 0$.*
(2) Si $o(g)$ est fini, alors c'est le plus petit entier $n > 0$ tel que $g^n = e$.

Démonstration. Pour montrer le premier point, supposons par la contraposée qu'il existe un entier $n > 0$ tel que $g^n = e$. On a alors

$$\langle g \rangle = \{g^m \,|\, m \in \mathbb{Z}\} \subset \{e, g, g^2, \ldots, g^{n-1}\},$$

d'où $o(g) = |\langle g \rangle| \leq n < \infty$.

Pour montrer le second point, supposons $o(g)$ fini. On va vérifier l'égalité ensembliste

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{o(g)-1}\},$$

ce qui implique la proposition. Pour ce faire, notons tout d'abord que l'ensemble de droite est inclus dans celui de gauche. De plus, tous les éléments de l'ensemble de droite sont distincts. En effet, dans le cas contraire, on aurait des entiers $0 \leq n < m \leq o(g) - 1$ avec $g^n = g^m$; on aurait alors $g^{m-n} = e$, d'où l'inclusion $\langle g \rangle \subset \{e, g, g^2, \ldots, g^{m-n-1}\}$, et les inégalités $o(g) = |\langle g \rangle| \leq m - n < o(g)$, une contradiction. On a donc l'inclusion de l'ensemble de droite dans celui de gauche, et ces deux ensembles ont même cardinal $o(g)$. Cela implique l'égalité, et conclut la preuve. □

Nous allons maintenant donner quelques exemples de calcul d'ordre d'éléments. D'autres exemples seront traités en exercice 15.

Exemples (d'ordre d'éléments)**.**

1. Le seul élément d'ordre 1 dans un groupe est le neutre.
2. Tout $m \neq 0$ dans $\mathbb{Z}$ est d'ordre infini.
3. Dans $\mathbb{Z}/n\mathbb{Z}$, l'élément $g = [1]$ est d'ordre $o(g) = n$.
4. Dans le groupe de Klein $V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, tous les éléments différents du neutre sont d'ordre 2. Comme ce groupe est d'ordre 4, cela montre que V n'est *pas* un groupe cyclique.

I.3 Homomorphismes de groupes

Voici un principe assez général en mathématiques[5] : après avoir muni un ensemble d'une structure (par exemple, celle d'espace vectoriel), il est utile de considérer les applications qui préservent cette structure (dans cet exemple, les applications linéaires).

Pour la structure de groupe, ce rôle est joué par ce qu'on appelle les *homomorphismes de groupes*.

Définition I.3

Soient $(G, \star)$ et $(G', \bullet)$ deux groupes. Une application $\varphi : G \to G'$ est un **homomorphisme de groupes** (ou plus simplement, un **homomorphisme**) si

$$\varphi(g \star h) = \varphi(g) \bullet \varphi(h)$$

pour tous $g, h \in G$.

Remarques.

1. Il peut sembler surprenant qu'on n'exige ni compatibilité avec l'élément neutre
$$\varphi(e_G) = e_{G'}, \tag{I.1}$$
ni compatibilité avec l'inverse
$$\varphi(g^{-1}) = \varphi(g)^{-1} \text{ pour tout } g \in G. \tag{I.2}$$
En réalité, ces deux propriétés sont toujours automatiquement satisfaites par un homomorphisme de groupes !

   ⌜ Pour montrer la première, on considère la suite d'égalités
$$\varphi(e_G) \bullet \varphi(e_G) = \varphi(e_G \star e_G) = \varphi(e_G) = \varphi(e_G) \bullet e_{G'},$$
que l'on simplifie par $\varphi(e_G)$ (i.e. que l'on multiplie à gauche par $\varphi(e_G)^{-1}$) pour obtenir $\varphi(e_G) = e_{G'}$. Pour montrer la seconde, on fixe $g \in G$ et l'on calcule
$$\varphi(g^{-1}) \bullet \varphi(g) = \varphi(g^{-1} \star g) = \varphi(e_G) \overset{(I.1)}{=} e_{G'}.$$
On a de même $\varphi(g) \bullet \varphi(g^{-1}) = e_{G'}$, ce qui implique $\varphi(g^{-1}) = \varphi(g)^{-1}$. ⌟

2. La composition de deux homomorphismes $\varphi : G \to G'$ et $\psi : G' \to G''$ est encore un homomophisme.

   ⌜ En effet, pour tous $g, h \in G$, on a
$$\begin{aligned}(\psi \circ \varphi)(gh) &= \psi(\varphi(gh)) = \psi(\varphi(g)\varphi(h)) = \psi(\varphi(g))\psi(\varphi(h)) \\ &= (\psi \circ \varphi)(g)(\psi \circ \varphi)(h),\end{aligned}$$
ce qui montre que $\psi \circ \varphi : G \to G''$ est un homomorphisme. ⌟

5. Ce principe est formalisé dans ce qu'on appelle le *langage des catégories*.

Terminologie. Soit $\varphi: G \to G'$ un homomorphisme. Le *noyau* de φ est défini par

$$\mathrm{Ker}(\varphi) \coloneqq \{g \in G \,|\, \varphi(g) = e_{G'}\}\,,$$

tandis que *l'image* de φ est donnée par

$$\mathsf{Im}(\varphi) \coloneqq \{\varphi(g) \in G' \,|\, g \in G\}\,.$$

Proposition I.3. *(i) Le noyau d'un homomorphisme $\varphi: G \to G'$ est un sous-groupe de G, et $\mathrm{Ker}(\varphi) = \{e_G\}$ si et seulement si φ est injectif.*

(ii) L'image d'un homomorphisme $\varphi: G \to G'$ est un sous-groupe de G', et $\mathsf{Im}(\varphi) = G'$ si et seulement si φ est surectif.

Démonstration. Soit donc $\varphi: G \to G'$ un homomorphisme ; on va utiliser la proposition I.1 pour vérifier que $\mathrm{Ker}(\varphi)$ est un sous-groupe de G. Tout d'abord, le noyau n'est pas vide puisqu'il contient e_G par (I.1). Soient à présent $h_1, h_2 \in \mathrm{Ker}(\varphi)$; le calcul

$$\varphi(h_1 h_2^{-1}) = \varphi(h_1)\varphi(h_2^{-1}) \overset{(I.2)}{=} \varphi(h_1)\varphi(h_2)^{-1} = e_{G'} e_{G'}^{-1} = e_{G'}$$

montre que $h_1 h_2^{-1}$ appartient aussi à $\mathrm{Ker}(\varphi)$, et donc qu'il s'agit bien d'un sous-groupe.

Vérifions à présent que $\mathrm{Ker}(\varphi) = \{e_G\}$ si et seulement si φ est injectif, en commençant par l'implication de droite à gauche. Soit donc φ injectif, et soit $g \in \mathrm{Ker}(\varphi)$. On a l'égalité

$$\varphi(e_G) = e_{G'} = \varphi(g)\,,$$

ce qui implique $g = e_G$ par injectivité. Ainsi, on a l'inclusion $\mathrm{Ker}(\varphi) \subset \{e_G\}$; l'autre inclusion étant toujours valide, cette implication est démontrée.

Pour vérifier l'autre implication, on suppose que $\mathrm{Ker}(\varphi)$ est trivial, et on montre que φ est injective. Soient donc $g, h \in G$ tels que $\varphi(g) = \varphi(h)$; on veut voir que $g = h$. Pour ce faire, on calcule

$$\varphi(gh^{-1}) = \varphi(g)\varphi(h^{-1}) \overset{(I.2)}{=} \varphi(g)\varphi(h)^{-1} = \varphi(g)\varphi(g)^{-1} = e_{G'}\,.$$

On a donc $gh^{-1} \in \mathrm{Ker}(\varphi) = \{e_G\}$, et donc $gh^{-1} = e_G$, ce qui est équivalent à $g = h$. Cela termine la preuve du premier point.

La preuve du second est l'objet de l'exercice 16. □

Exemples (d'homomorphismes de groupes)**.**

1. L'application identité $\mathrm{id}_G: G \to G$ est un homomorphisme, de noyau $\{e_G\}$ est d'image G.

2. Si H est un sous-groupe d'un groupe G, alors l'inclusion $i: H \to G$ est un homomorphisme, de noyau $\{e_G\}$ est d'image H.

3. Pour tous groupes G, G' l'application constante $G \to G', g \mapsto e_{G'}$ est un homomorphisme de groupes. On parle d'*homomorphisme trivial*. Son noyau est le groupe G tout entier, son image est $\{e_{G'}\}$.

4. Soit G un groupe, et $g \in G$ fixé. Alors, l'application

$$\varphi\colon \mathbb{Z} \longrightarrow G, \quad n \longmapsto g^n$$

est un homomorphisme, puisque pour tous $n, m \in \mathbb{Z}$, on a

$$\varphi(n+m) = g^{n+m} = g^n g^m = \varphi(n)\varphi(m)\,.$$

Par définition, son image est $\langle g \rangle$; par la proposition I.2, son noyau est donné par

$$\mathrm{Ker}(\varphi) = \begin{cases} o(g)\mathbb{Z} & \text{si } o(g) < \infty, \\ \{0\} & \text{si } o(g) = \infty. \end{cases}$$

5. L'application

$$\mathbb{C}^* \longrightarrow \mathbb{R}_+^*, \quad z \longmapsto |z|$$

est un homomorphisme, puisque $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ pour tous $z_1, z_2 \in \mathbb{C}^*$. Son noyau est le cercle S^1, et son image $\mathbb{R}_+^*$.

6. Pour $K = \mathbb{R}, \mathbb{C}$, le déterminant définit un homomorphisme de groupes

$$\det\colon \mathrm{GL}(n, K) \longrightarrow K^*\,,$$

puisque $\det(M_1 M_2) = \det(M_1)\det(M_2)$ pour tous $M_1, M_2 \in \mathrm{GL}(n, K)$. Par définition, son noyau $\mathrm{SL}(n, \mathbb{R})$, et l'on vérifie facilement que son image est K^*.

7. Une application linéaire $f\colon E \to E'$ est un homomorphisme entre $(E, +)$ et $(E', +)$: le premier axiome d'une application linéaire ne dit rien d'autre.

8. L'application

$$(\mathbb{R}, +) \longrightarrow (\mathbb{C}^*, \cdot), \quad t \longmapsto e^{ix}$$

est un homomorphisme, puisque $e^{i(x+y)} = e^{ix} \cdot e^{iy}$. Son image est le cercle S^1, et son noyau est donné par $2\pi\mathbb{Z} = \{2\pi k \,|\, k \in \mathbb{Z}\}$.

9. Soit $m \in \mathbb{Z} \smallsetminus \{0\}$ fixé. La multiplication par m définit une application $\mathbb{Z} \to \mathbb{Z}$, $n \mapsto mn$. C'est un homomorphisme puisque $m(n_1 + n_2) = mn_1 + mn_2$ pour tous $n_1, n_2 \in \mathbb{Z}$. Son noyau est $\{0\}$ car m est non-nul, et son image l'ensemble $m\mathbb{Z}$ des multiples de m.

10. L'application $\mathrm{sgn}\colon (\mathbb{R}^*, \cdot) \to \{-1, 1\}$ donnée par

$$\mathrm{sgn}(x) = \begin{cases} +1 & \text{si } x > 0, \\ -1 & \text{si } x < 0, \end{cases}$$

est un homomorphisme de noyau $\mathbb{R}_+^*$ et d'image $\{-1, 1\}$.

En conclusion : comme les groupes, les homomorphismes de groupes se trouvent partout !

Dans la liste de groupes donnée en section I.1, il apparaît clairement que certains groupes devraient être considérés comme "les mêmes". Il est maintenant possible de donner un sens précis à cette intuition.

Définition I.4

Un homomorphisme de groupes $\varphi : G \to G'$ est appelé un **isomorphisme (de groupes)** s'il existe un homomorphisme $\psi : G' \to G$ avec $\varphi \circ \psi = \mathrm{id}_{G'}$ et $\psi \circ \varphi = \mathrm{id}_G$.

S'il existe un tel isomorphisme, on dit que G et G' sont **isomorphes**, ce qui est noté $G \simeq G'$.

Remarques.

1. Soit $\varphi : G \to G'$ un homomorphisme. Alors, φ est un isomorphisme si et seulement si φ est bijectif.

   ⌜ En effet, si φ est un isomorphisme, alors il admet un inverse à droite et à gauche, et est donc bijectif. Réciproquement, un homomorphisme $\varphi : G \to G'$ bijectif admet un inverse $\psi : G' \to G$, mais il reste à vérifier que ψ est un homomorphisme. Soient donc $g'_1, g'_2 \in G'$; en utilisant l'égalité $\varphi \circ \psi = \mathrm{id}_{G'}$, le fait que φ est un homomorphisme, et l'égalité $\psi \circ \varphi = \mathrm{id}_G$, on obtient

   $$\psi(g'_1 g'_2) = \psi(\varphi(\psi(g'_1))\varphi(\psi(g'_2))) = \psi(\varphi(\psi(g'_1)\psi(g'_2))) = \psi(g'_1)\psi(g'_2)\,,$$

   ce qu'il fallait démontrer. ⌟

2. On montre facilement les trois affirmations suivantes :
   (a) L'application id_G est un isomorphisme (d'où $G \simeq G$).
   (b) La composition de deux isomorphismes est un isomorphisme (d'où $G \simeq G', G' \simeq G'' \Rightarrow G \simeq G''$).
   (c) L'inverse d'un isomorphisme est un isomorphisme (d'où $G \simeq G' \Rightarrow G' \simeq G$).

   Peut-on pour autant dire que "être isomorphe" est une relation d'équivalence ? Pas formellement, puisque "l'ensemble des groupes" n'existe pas ![6]

3. Néanmoins, on aura tendance à "identifier" deux groupes isomorphes, à les considérer comme deux "incarnations"[7] d'un même groupe, de la même manière qu'on "identifie" deux espaces vectoriels isomorphes en algèbre linéaire, ou deux ensembles en bijection en théorie des ensembles.

4. Toutes les "propriétés étudiées en théorie des groupes" sont préservées par isomorphismes[8]. Par exemple, si $\varphi : G \to G'$ est un isomorphisme, alors :
   - Les groupes G et G' ont même ordre ;

6. En théorie des ensembles, on parle de *classe propre*.
7. Voilà donc la signification formelle de ce mot dans notre contexte.
8. C'est d'ailleurs sans doute la définition la plus précise qu'on puisse donner de la théorie des groupes : l'étude des propriétés de groupes préservées par isomorphismes.

- G est abélien si et seulement si G' est abélien ;
- Pour tout $g \in G$, on a $o(g) = o(\varphi(g))$.

⌜ Le premier fait est évident puisqu'un isomorphisme est bijectif, et le troisième est le sujet de l'exercice 18 ; vérifions le second. Supposons donc G' abélien, et fixons $g, h \in G$. Comme φ est un homomorphisme et G' est abélien, on a

$$\varphi(gh) = \varphi(g)\varphi(h) = \varphi(h)\varphi(g) = \varphi(hg)\,,$$

ce qui implique $gh = hg$ puisque φ est injectif. Réciproquement, supposons G abélien, et fixons $g', h' \in G'$. Comme φ surjectif, il existe $g, h \in G$ tels que $\varphi(g) = g'$ et $\varphi(h) = h'$. Comme φ est un homomorphisme et G est abélien, on a

$$g'h' = \varphi(g)\varphi(h) = \varphi(gh) = \varphi(hg) = \varphi(h)\varphi(g) = h'g'\,,$$

ce qui conclut la preuve [9]. ⌟

5. Pour montrer que deux groupes sont isomorphes, il faut construire un isomorphisme entre ces deux groupes. Pour montrer que deux groupes ne sont *pas* isomorphes, il faut trouver une propriété préservée par isomorphismes, qu'un des groupes possède, et l'autre ne possède pas.

Exemples (d'isomorphismes)**.**

1. Tous les groupes à un élément sont évidemment isomorphes entre eux : on parle donc *du* groupe trivial. En particulier, les groupes $\mathrm{SL}(1, K)$, $\mu_1(\mathbb{C})$, S_1, et $\mathbb{Z}/1\mathbb{Z}$ sont isomorphes.

2. Tous les groupes à deux éléments sont isomorphes entre eux.

   ⌜ En effet, si $G = \{e, g\}$ est un groupe, alors la loi de composition est entièrement déterminée par les axiomes : on a forcément $eg = ge = g$ et $ee = gg = e$. Ainsi, si $G = \{e_G, g\}$ et $G' = \{e_G, g'\}$ sont deux groupes d'ordre 2, ils sont isomorphes via $\varphi : G \to G', e_G \mapsto e_{G'}, g \mapsto g'$. ⌟

   Par conséquent, on peut parler *du* groupe d'ordre deux. En particulier, les groupes $\mu_2(\mathbb{C})$, S_2, et $\mathbb{Z}/2\mathbb{Z}$ sont isomorphes.

3. Tous les groupes d'ordre trois sont isomorphes entre eux : c'est l'exercice 19.

4. En revanche, il n'est pas vrai que tous les groupes d'ordre 4 sont isomorphes. En effet, les groupes $\mathbb{Z}/4\mathbb{Z}$ et $V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes, car l'élément $[1]$ est d'ordre 4 dans $\mathbb{Z}/4\mathbb{Z}$, tandis que tous les éléments de V sont d'ordre 1 ou 2, on l'avait vu. Comme l'ordre des éléments est préservé par isomorphisme, on peut conclure.

5. Les groupes S_3 et $\mathbb{Z}/6\mathbb{Z}$ sont tous les deux d'ordre 6 mais ne sont pas isomorphes, puisque le premier n'est pas abélien et le second si [10].

9. On aurait aussi pu ne montrer qu'une implication et invoquer le point (c) ci-dessus pour en déduire la seconde.

10. On peut aussi raisonner en termes d'ordres d'éléments comme dans l'exemple précédent.

6. L'application
$$\exp\colon (\mathbb{R},+) \longrightarrow (\mathbb{R}_+^*,\cdot)$$
donnée par $\exp(x) = e^x$ est un isomorphisme, puisque $e^{x+y} = e^x e^y$ pour tous $x, y \in \mathbb{R}$, et que c'est un bijection (d'inverse $\log\colon \mathbb{R}_+^* \to \mathbb{R}$).

7. S'il existe une bijection $f\colon X \to Y$, alors les deux groupes symétriques $S(X)$ et $S(Y)$ sont isomorphes via $\varphi\colon S(X) \to S(Y)$ donnée par $\varphi(\sigma) = f \circ \sigma \circ f^{-1}$. C'est un excellent exercice de théorie des ensembles, voir exercice 22.

8. Pour tout $n \geq 1$, l'application $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mu_n(\mathbb{C})$ donnée par $\varphi([a]) = e^{\frac{2\pi i}{n}a}$ est un isomorphisme de groupes, d'où $\mathbb{Z}/n\mathbb{Z} \simeq \mu_n(\mathbb{C})$.

   ⌜ Vérifions d'abord que φ est bien définie. Si $a, a' \in \mathbb{Z}$ sont tels que $[a] = [a'] \in \mathbb{Z}/n\mathbb{Z}$, cela signifie qu'il existe $k \in \mathbb{Z}$ tel que $a' = a + kn$. Ainsi, on a
   $$\varphi([a']) = e^{\frac{2\pi i}{n}a'} = e^{\frac{2\pi i}{n}a} e^{2\pi i \cdot k} = e^{\frac{2\pi i}{n}a} = \varphi([a])\,.$$
   De plus, on a $\varphi([a])^n = 1$ pour tout a. Nous sommes donc bien en présence d'une application $\varphi\colon \mathbb{Z} \to \mu_n(\mathbb{C})$. C'est un homomorphisme, car
   $$\varphi([a]+[b]) = e^{\frac{2\pi i}{n}(a+b)} = e^{\frac{2\pi i}{n}a} e^{\frac{2\pi i}{n}b} = \varphi([a])\varphi([b])$$
   pour tous $a, b \in \mathbb{Z}$. Finalement, φ est surjectif de manière évidente, et donc bijectif puisque $|\mathbb{Z}/n\mathbb{Z}| = |\mu_n(\mathbb{C})| = n$. C'est donc un isomorphisme. ⌟

Terminologie. Un isomorphisme $\varphi\colon G \to G$ est appelé un *automorphisme* de G.

Remarque. L'ensemble $\mathrm{Aut}(G)$ des automorphismes de G muni de la composition des applications forme un groupe. Cela découle immédiatement de la remarque 2 ci-dessus.

Exemples (d'automorphismes)**.**

1. Tentons de déterminer le groupe $\mathrm{Aut}(\mathbb{Z})$ des automorphismes de $\mathbb{Z}$.
   Pour ce faire, notons que tout homomorphisme $\varphi\colon \mathbb{Z} \to \mathbb{Z}$ est donné par la multiplication par $\varphi(1) \in \mathbb{Z}$. En effet :
   (a) Si $n > 0$, alors $\varphi(n) = \varphi(\overbrace{1 + \cdots + 1}^{n}) = \overbrace{\varphi(1) + \cdots + \varphi(1)}^{n} = \varphi(1) \cdot n$.
   (b) Si $n = 0$, alors $\varphi(0) = 0 = \varphi(1) \cdot 0$.
   (c) Si $n < 0$, alors $\varphi(n) = \varphi(-(-n)) = -\varphi(-n) \overset{-n>0}{=} -\varphi(1) \cdot (-n) = \varphi(1) \cdot n$.
   Ainsi, on a bien $\varphi(n) = \varphi(1) \cdot n$ pour tout $n \in \mathbb{Z}$. En particulier, l'image de φ est donnée par l'ensemble $\varphi(1)\mathbb{Z}$ des multiples de $\varphi(1)$. Par conséquent, l'homomorphisme φ n'est surjectif que si $\varphi(1) = \pm 1$, et les seuls homomorphismes surjectifs sont donc donnés par $\mathrm{id}_{\mathbb{Z}}$ et $-\mathrm{id}_{\mathbb{Z}}$. Comme ce sont des automorphismes, on a $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}_{\mathbb{Z}}, -\mathrm{id}_{\mathbb{Z}}\}$.

2. Soit G un groupe quelconque, et soit $g \in G$. Alors, l'application $\iota_g : G \to G$ donnée par $\iota_g(x) = gxg^{-1}$ est un automorphisme de G, appelé la *conjugaison* par $g \in G$.

   ⌜ En effet, pour tout $x, y \in G$, on a

   $$\iota_g(xy) = g(xy)g^{-1} = gx(g^{-1}g)yg^{-1} = (gxg^{-1})(gyg^{-1}) = \iota_g(x)\iota_g(y)\,,$$

   ce qui montre que ι_g est un homomorphisme. De plus, pour tout $x \in G$, on a

   $$(\iota_g \circ \iota_{g^{-1}})(x) = \iota_g(g^{-1}xg) = (gg^{-1})x(gg^{-1}) = x\,,$$

   ce qui montre que $\iota_g \circ \iota_{g^{-1}} = \mathrm{id}_G$. On vérifie de même que $\iota_{g^{-1}} \circ \iota_g = \mathrm{id}_G$, et donc que ι_g est bien un automorphisme, d'inverse $(\iota_g)^{-1} = \iota_{g^{-1}}$. ⌟

   De plus, l'application $\iota : G \to \mathrm{Aut}(G)$ donnée par $g \mapsto \iota_g$ est un homomorphisme de noyau $Z(G)$.

   ⌜ En effet, pour tout $g_1, g_2 \in G$ et tout $x \in G$, on a

   $$(\iota_{g_1} \circ \iota_{g_2})(x) = \iota_{g_1}(\iota_{g_2}(x)) = \iota_{g_1}(g_2xg_2^{-1}) = g_1g_2xg_2^{-1}g_1^{-1} = (g_1g_2)x(g_1g_2)^{-1} = \iota_{g_1g_2}(x)\,,$$

   ce qui montre que $\iota_{g_1} \circ \iota_{g_2} = \iota_{g_1g_2} \in \mathrm{Aut}(G)$, et que ι est un homomorphisme. De plus, un élément $g \in G$ est dans le noyau de ι si et seulement si $\iota_g = \mathrm{id}_G$. Or $\iota_g(x) = x$ est équivalent à $gx = xg$. Ainsi, on a $g \in \mathrm{Ker}(\iota)$ si et seulement si $g \in Z(G)$. ⌟

   L'image de ι est notée $\mathrm{Int}(G)$: c'est le groupe des *automorphismes intérieurs* de G.

I.4 Théorème de Lagrange

Nous allons enfin voir le premier résultat "non-trivial" de ce cours, un théorème qui porte le nom du mathématicien Joseph-Louis Lagrange bien que ce dernier ne l'ait démontré que pour le groupe symétrique S_n (mais sans la notion abstraite de groupe à disposition).

Pour l'énoncer et le démontrer, nous aurons besoin d'un certain de nombre de notations et de terminologie. Les voici.

Notation. Soit G un groupe fixé. Pour X, Y des sous-ensembles de G et $g \in G$, on va noter

$$gX \coloneqq \{gx \,|\, x \in X\}\,, \qquad Xg = \{xg \,|\, x \in X\}\,,$$
$$XY \coloneqq \{xy \,|\, x \in X, y \in Y\}\,, \qquad X^{-1} \coloneqq \{x^{-1} \,|\, x \in X\}\,.$$

Dans le cas abélien avec la notation additive, on va bien-sûr noter

$$g + G \coloneqq \{g + x \,|\, x \in X\}\,, \quad X + Y \coloneqq \{x + y \,|\, x \in X, y \in Y\}\,, \quad -X \coloneqq \{-x \,|\, x \in X\}\,.$$

Remarque. Notons les égalités ensemblistes

$$g(hX) = (gh)X \quad \text{et} \quad (gX)^{-1} = X^{-1}g^{-1}$$

et l'équivalence $gh \in X \Leftrightarrow h \in g^{-1}X$ pour tous $g, h \in G$ et $X \subset G$, qu'on utilisera de manière systématique. (Voir aussi l'exercice 24.)

Terminologie. Soit H un sous-groupe d'un groupe G.

- Pour $g \in G$, l'ensemble gH (resp. Hg) est appelé la *classe à gauche* (resp. *classe à droite*) de $g \in G$ modulo H.

  Dans le cas abélien, les classes à gauche et à droite de $g \in G$ modulo H coïncident ; en notation additive, c'est l'ensemble $g + H = H + g$.
- L'ensemble des classes à gauche (resp. à droite) modulo H dans G est noté G/H (resp. $H\backslash G$). En d'autres termes, on a

$$G/H \coloneqq \{gH \,|\, g \in G\} \quad \text{et} \quad H\backslash G \coloneqq \{Hg \,|\, g \in G\}\,.$$

- Le cardinal de G/H, donc le nombre de classes à gauche modulo H dans G, est appelé *l'indice* de H dans G, et noté $[G : H]$.

Remarque. En fait, l'indice est aussi égal au nombre de classes à droite.

⌜ En effet, considérons l'application définie sur l'ensemble G/H via $gH \mapsto (gH)^{-1}$. Comme H est un sous-groupe, on a $H^{-1} = H$, d'où $(gH)^{-1} = H^{-1}g^{-1} = Hg^{-1}$. Ainsi, on a une application $G/H \to H\backslash G$. Cette application admet l'inverse $(Hg) \mapsto (Hg)^{-1} = g^{-1}H$, et est donc bijective, d'où l'égalité $|G/H| = |H\backslash G|$. ⌟

Exemples (de classes à gauche/droite et d'indice)**.**

1. Soit G un groupe quelconque, et $H = \{e\}$ le sous-groupe trivial. Les classes à gauche modulo $\{e\}$ sont simplement données par les singletons correspondants :

   $$gH = \{gh \,|\, h = e\} = \{g\}\,,$$

   et de même pour les classes à droite. On a donc $[G : \{e\}] = |G|$.
2. Soit G un groupe quelconque, et $H = G$. Les classes à gauche modulo G coïncident toutes avec G :

   $$gH = \{gh \,|\, h \in G\} = G\,,$$

   et de même pour les classes à droite. On a donc une seule classe à gauche modulo G, d'où $[G : G] = 1$.
3. Soit $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ pour un certain $n \in \{1, 2, 3 \ldots\}$. La classe (à gauche ou à droite) de $m \in \mathbb{Z}$ modulo H est donnée par le sous-ensemble

   $$m + H = m + n\mathbb{Z} = \{m + nk \,|\, k \in \mathbb{Z}\}$$

   de $\mathbb{Z}$, qui n'est autre que la classe d'équivalence de m modulo n. Ainsi, l'ensemble G/H des classes modulo H coïncide avec l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes d'équivalence modulo n, ce qui justifie la notation et la terminologie *modulo*.

   De plus, on a $[\mathbb{Z} : n\mathbb{Z}] = |\mathbb{Z}/n\mathbb{Z}| = n$.

Voici enfin le résultat principal de cette section, et le premier théorème du cours.

Théorème I.4: Théorème de Lagrange

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

Joseph-Louis Lagrange (1736-1813)

Démonstration. Soit donc G un groupe (quelconque), et soit H un sous-groupe de G. On définit une relation sur G via

$$g_1 \sim g_2 \iff g_2^{-1} g_1 \in H$$

pour $g_1, g_2 \in G$. (Par exemple, pour $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, cette relation est la congruence modulo n.) Les trois axiomes d'une relation d'équivalence découlent des trois axiomes d'un sous-groupe :

- On a bien $g \sim g$ pour tout $g \in G$, puisque $g^{-1} g = e$ est un élément de H : la réflexivité est ainsi satisfaite via le second axiome d'un sous-groupe.
- Si on a $g_1 \sim g_2$, i.e. $g_2^{-1} g_1 \in H$, cela implique que H contient aussi l'inverse $(g_2^{-1} g_1)^{-1} = g_1^{-1} g_2$, d'où $g_2 \sim g_1$: la symétrie est vérifiée via le troisième axiome.
- Si on a $g_1 \sim g_2$ et $g_2 \sim g_3$, i.e. $g_2^{-1} g_1 \in H$ et $g_3^{-1} g_2 \in H$, cela implique que H contient aussi la composition $(g_3^{-1} g_2)(g_2^{-1} g_1) = g_3^{-1} g_1$, d'où $g_1 \sim g_3$: la transitivité découle donc du premier axiome.

Maintenant que nous savons qu'il s'agit bien d'une relation d'équivalence, calculons la classe d'équivalence de $g \in G$:

$$[g] \coloneqq \{g' \in G \,|\, g' \sim g\} = \{g' \in G \,|\, g^{-1} g' \in H\} = \{g' \in G \,|\, g' \in gH\} = gH\,.$$

En clair, les classes d'équivalence sont simplement les classes à gauche modulo H. Or, les classes d'équivalence forment toujours une partition de l'ensemble sur lequel la relation est définie ; ainsi, les classes à gauche modulo H forment une partition de G (en $[G : H]$ sous-ensembles, par définition de l'indice).

Pour finir, toutes les classes à gauche modulo H sont en bijection avec H. En effet, l'application $H \to gH$ donnée par $h \mapsto gh$ est surjective par définition, et injective par la "règle de calcul" $gh_1 = gh_2 \Rightarrow h_1 = h_2$. Ainsi, toutes les classes à gauche ont le même cardinal que H.

En conclusion, on a partitionné G en $[G : H]$ sous-ensembles, qui sont tous d'ordre $|H|$. On a donc bien l'égalité $|G| = [G : H] \cdot |H|$. □

Remarque. Où a-t-on utilisé que G est fini ? Nulle part : ce résultat est valide pour tout groupe, mais l'égalité $|G| = [G : H] \cdot |H|$ fait alors intervenir des cardinaux non nécessairement finis.

Voyons quelques exemples pour illustrer ce théorème.

Exemples.

1. Comme on l'a montré, le sous-groupe $H = \{e\}$ donne l'indice $[G : \{e\}] = |G|$ (et bien entendu, $|H| = 1$). On vérifie donc bien l'égalité $|G| = |G| \cdot 1$.
2. À l'autre extrême, le choix de $H = G$ donne l'indice $[G : G] = 1$ (et bien entendu, $|H| = |G|$). On a donc bien $|G| = 1 \cdot |G|$.
3. Dans $G = S_n$, considérons le sous-groupe

$$H = \{\sigma \in S_n \,|\, \sigma(n) = n\}$$

qui est clairement isomorphe à S_{n-1}, et tentons de calculer son indice. En reprenant la notation de la preuve, on a que $\sigma_1, \sigma_2 \in S_n$ sont équivalents si et seulement si

$$\sigma_1 \sim \sigma_2 \Leftrightarrow \sigma_2^{-1}\sigma_1 \in H \Leftrightarrow \sigma_2^{-1}\sigma_1(n) = n \Leftrightarrow \sigma_1(n) = \sigma_2(n) \in \{1, \ldots, n\}\,.$$

Ainsi, les classes à gauche modulo H sont en bijection avec $\{1, \ldots, n\}$, d'où $[G : H] = n$.
Par Lagrange, on a ainsi $|S_n| = |G| = [G : H] \cdot |H| = n \cdot |S_{n-1}|$. Par induction, on obtient le résutat bien connu $|S_n| = n(n-1)(n-2)\cdots 2 \cdot 1 = n!$.

Après ces exemples de type "reality check", voici quelques conséquences moins évidentes du théorème de Lagrange.

Corollaire I.5. *Si H est un sous-groupe d'un groupe fini G, alors $|H|$ et $[G : H]$ divisent $|G|$.* □

Corollaire I.6. *Si g est un élément d'un groupe fini G, alors $o(g)$ divise $|G|$.*

Démonstration. On applique le corollaire I.5 au sous-groupe $H = \langle g \rangle$. □

Corollaire I.7. *Un groupe d'ordre premier est cyclique.*

Démonstration. Soit donc G un groupe d'ordre premier, et soit $g \in G \setminus \{e\}$. Comme g n'est pas le neutre, son ordre satisfait $o(g) \geq 2$. Par le corollaire I.6, on sait également que $o(g)$ divise $|G|$. Comme $|G|$ est premier, cela implique l'égalité $o(g) = |G|$. Comme les groupes $\langle g \rangle \subset G$ sont finis et de même cardinalité, on a donc $\langle g \rangle = G$, et le groupe G est bien cyclique [11]. □

Corollaire I.8. *Dans un groupe fini G, on a $g^{|G|} = e$ pour tout $g \in G$.*

Démonstration. Soit donc g un élément quelconque d'un groupe fini G. Par le corollaire I.6, il existe un entier n tel que $|G| = o(g) \cdot n$. Cela implique

$$g^{|G|} = g^{o(g)\cdot n} = (g^{o(g)})^n = e^n = e\,,$$

ce qu'il fallait démontrer. □

On verra très bientôt une application de ce résultat en théorie des nombres.

11. Cette preuve montre de plus que G est engendré par n'importe quel élément différent du neutre.

I.5 Groupes cycliques

Pour rappel, un groupe G est dit *cyclique* s'il existe $g \in G$ tel que

$$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

On a vu les exemples suivants de groupes cycliques :

- le groupe $\mathbb{Z}$, cyclique d'ordre infini ;
- pour tout $n \geq 1$, le groupe $\mathbb{Z}/n\mathbb{Z}$, cyclique d'ordre n (isomorphe à $\mu_n(\mathbb{C})$.

Le premier but de cette section est de montrer qu'en fait, ce sont les seuls groupes cycliques à isomorphisme près. Ce résultat, appelé le théorème de *classification des groupes cycliques*, repose sur l'énoncé suivant.

Proposition I.9. *Pour tout sous-groupe H de $\mathbb{Z}$, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.*

Démonstration. Soit donc H un sous-groupe quelconque de $\mathbb{Z}$. Si H est le sous-groupe trivial $\{0\}$, alors on a bien $H = n\mathbb{Z}$ pour $n = 0$ et il n'y a rien à montrer. Supposons donc que H ne coïncide pas avec $\{0\}$. Dans ce cas, H contient un élément non-nul, et comme c'est un sous-groupe (et donc, $h \in H \Rightarrow -h \in H$), il contient au moins un entier strictement positif. En d'autres termes, l'intersection $H \cap \{1, 2, \ldots\}$ est non-vide. Il existe donc un élément minimal de $H \cap \{1, 2, \ldots\}$, que l'on va noter n. Il s'agit maintenant de montrer l'égalité $H = n\mathbb{Z}$, par double-inclusion.

L'inclusion $n\mathbb{Z} \subset H$ est évidente, puisque n appartient à H qui est un sous-groupe. Soit à présent $h \in H$; on veut vérifier que $h \in n\mathbb{Z}$. Par division euclidienne, on peut écrire $h = qn + r$ avec $q \in \mathbb{Z}$ et $0 \leq r < n$. Si $r = 0$, alors $h = qn \in n\mathbb{Z}$ et l'on a terminé. Supposons donc par l'absurde $r > 0$. Par hypothèse, on a $h \in H$ et $n \in H$, et H un sous-groupe ; cela implique que $r = h - qn$ est aussi un élément de H. Comme on a $0 < r < n$, cela contredit la minimalité de n dans $H \cap \{1, 2, \ldots\}$.

On a donc montré que tout sous-groupe $H < \mathbb{Z}$ est de la forme $H = n\mathbb{Z}$ avec $n \in \mathbb{N}$. Reste encore à vérifier que ce n est unique. On peut le montrer, par exemple, en remarquant que l'indice de $H = n\mathbb{Z}$ dans $\mathbb{Z}$ est donné par

$$[\mathbb{Z} : H] = [\mathbb{Z} : n\mathbb{Z}] = \begin{cases} n & \text{si } n > 0, \\ \infty & \text{si } n = 0. \end{cases}$$

On voit donc qu'il est impossible d'avoir $H = n\mathbb{Z} = n'\mathbb{Z}$ avec $n \neq n'$ dans $\mathbb{N}$. □

Voici finalement le théorème promis.

Théorème I.10: 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 $n = |G|$.

Démonstration. Soit donc G un groupe cyclique. Par définition, il existe $g \in G$ tel que $G = \langle g \rangle = \{g^a \mid a \in \mathbb{Z}\}$. Ainsi, l'homomorphisme

$$\varphi : \mathbb{Z} \longrightarrow G, \quad a \longmapsto g^a$$

est surjectif. Par la proposition I.3, le noyau de φ est un sous-groupe de $\mathbb{Z}$; par la proposition I.9, il existe $n \in \mathbb{N}$ tel que $\mathrm{Ker}(\varphi) = n\mathbb{Z}$. En clair, on a donc

$$g^a = e \;\Leftrightarrow\; a \in n\mathbb{Z}\,. \qquad (*)$$

Il y a maintenant deux cas à différencier. Supposons dans un premier temps que $n = 0$. Cela signifie que le noyau de φ est trivial, ce qui par la proposition I.3 implique que φ est injectif. Comme φ est aussi surjectif, c'est un isomorphisme, et l'on a donc bien $G \simeq \mathbb{Z}$.

Supposons dans un second temps que $n > 0$. Dans ce cas, nous allons montrer que l'application $\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to G$ définie par $\overline{\varphi}([a]) = g^a$ est un isomorphisme.

⌜ Vérifions d'abord que $\overline{\varphi}$ est bien défini. Si $[a] = [b]$ cela signifie que $a - b = nk$ avec $k \in \mathbb{Z}$, ce qui implique

$$\overline{\varphi}([a])\overline{\varphi}([b])^{-1} = g^a (g^b)^{-1} = g^{a-b} = g^{nk} \overset{(*)}{=} e\,.$$

On a donc bien $\overline{\varphi}([a]) = \overline{\varphi}([b])$, et $\overline{\varphi}$ est bien définie. Le fait que $\overline{\varphi}$ est un homomorphisme est clair, via les égalités

$$\overline{\varphi}([a] + [b]) = \overline{\varphi}([a + b]) = g^{a+b} = g^a g^b = \overline{\varphi}([a])\overline{\varphi}([b])\,,$$

valides pour tous $a, b \in \mathbb{Z}$.

On a donc un homomorphisme bien défini $\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to G$, qui est surjectif puisque $G = \langle g \rangle$: pour tout $h \in G$, il existe $a \in \mathbb{Z}$ tel que $g^a = h$. Finalement, l'injectivité de $\overline{\varphi}$ découle de l'équivalence $(*)$ ci-dessus. En effet, si un entier $a \in \mathbb{Z}$ satisfait $[a] \in \mathrm{Ker}(\overline{\varphi})$, cela signifie que $g^a = e$, et donc, que a est un multiple de n ; on a ainsi $[a] = [0] \in \mathbb{Z}/n\mathbb{Z}$, et la proposition I.3 permet de conclure. ⌟

Dans ce cas, on a donc $G \simeq \mathbb{Z}/n\mathbb{Z}$ avec $n = |\mathbb{Z}/n\mathbb{Z}| = |G|$.

Ainsi, si G est cyclique infini, on est nécessairement dans le cas $n = 0$; tandis que si G est cyclique fini, on est dans le cas $n > 0$ avec $n = |G|$. Cela conclut la preuve. □

Nous allons maintenant nous tourner vers les premières applications à la théorie des nombres, plus précisément à *l'arithmétique dans* $\mathbb{Z}$, une théorie que vous avez effleuré en LOGIQUE ET THÉORIE DES ENSEMBLES, et qui sera généralisée au chapitre II.

Terminologie.

- Pour $a, b \in \mathbb{Z}$, on dit que a *divise* b dans $\mathbb{Z}$, noté $a \mid b$, s'il existe $q \in \mathbb{Z}$ tel que $aq = b$.
- Pour $a, b \in \mathbb{Z}$, le *plus grand commun diviseur* de a et b, noté $\mathrm{pgcd}(a, b)$, est défini par les propriétés suivantes : $d = \mathrm{pgcd}(a, b) \geq 0$ satisfait $d \mid a$ et $d \mid b$, et si $c \in \mathbb{Z}$ est tel que $c \mid a$ et $c \mid b$, alors $c \mid d$ [12].

12. La première propriété assure que d est un commun diviseur, et la seconde que c'est le plus grand. Comme on demande de plus que $d \geq 0$, cela le caractérise entièrement.

- Deux entiers $a, b \in \mathbb{Z}$ sont dits *premiers entre eux* si $\text{pgcd}(a, b) = 1$.
- Un entier $p \geq 2$ est dit *premier* si, lorsque $p \mid ab$ avec $a, b \in \mathbb{Z}$, alors $p \mid a$ ou $p \mid b$.

On montrera au chapitre II que cette définition de nombre premier est équivalente à celle que vous connaissez. On verra aussi que pour tout entier $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$, il existe un premier qui le divise.

Voici un premier résultat d'arithmétique.

Proposition I.11. *Pour tous $a, b \in \mathbb{Z}$, on a $\{ax + by \mid x, y \in \mathbb{Z}\} = \text{pgcd}(a, b)\mathbb{Z}$.*

Démonstration. Soient donc $a, b \in \mathbb{Z}$, et soit $H \subset \mathbb{Z}$ donné par $H = \{ax + by \mid x, y \in \mathbb{Z}\}$. On vérifie très facilement que H est un sous-groupe de $\mathbb{Z}$. Par la proposition I.9, il existe $d \in \mathbb{N}$ tel que $H = d\mathbb{Z}$. Il reste à vérifier que cet entier $d \geq 0$ satisfait bien les deux propriétés qui caractérisent $\text{pgcd}(a, b)$.

Comme a peut s'écrire $a = ax + by$ avec $x = 1$ et $y = 0$, on a bien $a \in H = d\mathbb{Z}$, d'où $d \mid a$. De même, on peut écrire $b = ax + by$ avec $x = 0$ et $y = 1$, d'où $b \in H = d\mathbb{Z}$ et $d \mid b$. L'entier d satisfait donc bien la première propriété. Pour montrer la seconde, considérons $c \in \mathbb{Z}$ tel que $c \mid a$ et $c \mid b$. Dans ce cas, l'entier c divise tout entier de la forme $ax + by$ avec $x, y \in \mathbb{Z}$, et donc, tout élément de $H = d\mathbb{Z}$. En particulier, comme $d \in H$, on a bien $c \mid d$, ce qui conclut la preuve. □

Théorème I.12: Théorème de Bézout

Deux entiers $a, b \in \mathbb{Z}$ sont premiers entre eux si et seulement s'il existe $x, y \in \mathbb{Z}$ tels que $ax + by = 1$.

Etienne Bézout (1730-1783)

Démonstration. Par définition, deux entiers $a, b \in \mathbb{Z}$ sont premiers entre eux si et seulement si $\text{pgcd}(a, b) = 1$. Par la proposition I.11, cela implique l'égalité

$$\{ax + by \mid x, y \in \mathbb{Z}\} = \mathbb{Z},$$

qui implique la conclusion puisque $\mathbb{Z}$ contient 1.

Réciproquement, si l'ensemble $\{ax + by \mid x, y \in \mathbb{Z}\}$ contient 1, alors il coïncide avec $\mathbb{Z}$ puisque c'est un sous-groupe. Par la proposition I.11, cela ne peut arriver que si $\text{pgcd}(a, b) = 1$. □

Nous allons maintenant appliquer le théorème de Bézout à la théorie des groupes, avant d'appliquer le résultat obtenu à la théorie des nombres.

Pour tout $n \geq 1$, notons

$$(\mathbb{Z}/n\mathbb{Z})^* \coloneqq \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \text{pgcd}(a, n) = 1\},$$

et définissons sur cet ensemble la loi de composition

$$[a] \cdot [b] = [ab]$$

pour tous $a, b \in \mathbb{Z}$ avec $\text{pgcd}(a, n) = \text{pgcd}(b, n) = 1$.

Proposition I.13. *L'ensemble* $(\mathbb{Z}/n\mathbb{Z})^*$ *muni de cette loi de composition est un groupe abélien.*

Démonstration. Il s'agit tout d'abord de vérifier que l'ensemble $(\mathbb{Z}/n\mathbb{Z})^*$ est bien défini, i.e. que si $[a] = [a']$, alors $\mathrm{pgcd}(a, n) = \mathrm{pgcd}(a', n)$. En effet, l'égalité $[a] = [a']$ signifie qu'il existe $k \in \mathbb{Z}$ tel que $a' - a = nk$. Cela implique que pour tout $c \in \mathbb{Z}$, on a $c \mid a$ et $c \mid n$ si et seulement si $c \mid a'$ et $c \mid n$. Ainsi, l'ensemble des diviseurs communs de a et n coïncide avec l'ensemble des diviseurs communs de a et n'. En particulier, ils ont le même plus grand commun diviseur.

Dans un second temps, il faut s'assurer que la loi de composition est bien définie, i.e. que si $[a] = [a']$ et $[b] = [b']$, alors on a $[ab] = [a'b']$. Pour ce faire, rappelons que les égalités $[a] = [a']$ et $[b] = [b']$ signifient qu'il existe $k, \ell \in \mathbb{Z}$ tels que $a' = a + nk$ et $b' = b + n\ell$. On a donc

$$a'b' - ab = (a + nk)(b + n\ell) - ab = n(a\ell + bk + nk\ell) \in n\mathbb{Z}\,,$$

ce qui implique l'égalité souhaitée $[a'b'] = [ab]$.

Dans un troisième temps, il faut vérifier que la loi est interne, i.e. que si $a, b \in \mathbb{Z}$ satisfont $\mathrm{pgcd}(a, n) = \mathrm{pgcd}(b, n) = 1$, alors on a $\mathrm{pgcd}(ab, n) = 1$. Supposons par l'absurde que $a, b \in \mathbb{Z}$ satisfont $\mathrm{pgcd}(a, n) = \mathrm{pgcd}(b, n) = 1$ mais aussi $\mathrm{pgcd}(ab, n) \geq 2$. Par le fait énoncé avant la proposition I.11, il existe un nombre premier p qui divise $\mathrm{pgcd}(ab, n)$. Par conséquent, on a $p \mid n$ et $p \mid ab$. Comme p est premier, on a donc $p \mid n$, et $p \mid a$ ou $p \mid b$; disons, sans restriction de la généralité, que p divise a. On a alors $p \mid n$ et $p \mid a$, ce qui est impossible puisque $\mathrm{pgcd}(a, n) = 1$ et $p \geq 2$. Une contradiction.

Comme la multiplication dans $\mathbb{Z}$ est associative, il en va automatiquement de même pour la loi de composition sur $(\mathbb{Z}/n\mathbb{Z})^*$:

$$[a] \cdot ([b] \cdot [c]) = [a] \cdot [bc] = [a(bc)] = [(ab)c] = [ab] \cdot [c] = ([a] \cdot [b]) \cdot [c]$$

pour tous $a, b, c \in \mathbb{Z}$. On montre de la même manière que cette loi est commutative, et admet le neutre $[1]$, qui est bien élément de $(\mathbb{Z}/n\mathbb{Z})^*$ puisque $\mathrm{pgcd}(n, 1) = 1$.

Le point restant, celui qui utilise le théorème de Bézout, est l'existence d'un inverse. Soit donc $[a]$ un élément quelconque de $(\mathbb{Z}/n\mathbb{Z})^*$, et tentons de trouver $[x] \in (\mathbb{Z}/n\mathbb{Z})^*$ tel que $[a][x] = [1]$. Comme on a $\mathrm{pgcd}(a, n) = 1$, par (une des implications de) Bézout, il existe $x, y \in \mathbb{Z}$ tels que l'égalité $ax + ny = 1$ est vérifiée dans $\mathbb{Z}$. En prenant les classes d'équivalence, on obtient l'égalité suivante dans $\mathbb{Z}/n\mathbb{Z}$:

$$[1] = [ax + ny] = [ax] = [a] \cdot [x]\,.$$

Finalement, par (l'autre implication de) Bézout, l'égalité $xa + ny = 1$ implique que $\mathrm{pgcd}(x, n) = 1$, d'où $[x] \in (\mathbb{Z}/n\mathbb{Z})^*$ comme souhaité. □

Leonard Euler (1707-1783)

Nous avons besoin d'une dernière notation et terminologie, pour une fonction qui porte le nom du plus illustre mathématicien du XVIII$^{\text{ème}}$ siècle, "l'incomparable géomètre" Leonard Euler.

Notation. Pour tout $n = 1, 2, 3, \ldots$, on note

$$\varphi(n) = \#\{a \in \{1, 2, \ldots, n\} \mid \mathrm{pgcd}(a, n) = 1\}\,.$$

C'est la *fonction* φ *d'Euler.*

Par exemple, on a $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, etc. Notons également que $\varphi(p) = p-1$ pour tout premier p.

Nous sommes finalement en mesure de donner l'application promise en théorie des nombres, publiée par EULER en 1761.

Théorème I.14: Théorème d'Euler-Fermat

Soient $n \geq 1$ et $a \in \mathbb{Z}$ tels que a et n sont premiers entre eux. Alors, l'entier $a^{\varphi(n)} - 1$ est un multiple de n.

Billet de 10 francs suisses à l'effigie d'Euler, en circulation entre 1979 et 2000

Démonstration. Pour $n \geq 1$ et $a \in \mathbb{Z}$ premiers entre eux, la classe $g \coloneqq [a]$ appartient à $G \coloneqq (\mathbb{Z}/n\mathbb{Z})^*$, qui est un groupe par la proposition I.13. Par définition du groupe G et de la fonction φ, on a $|G| = \varphi(n)$. Par le corollaire I.8 au théorème de Lagrange, on a $g^{|G|} = e_G$. Cela se traduit en l'égalité suivante dans $\mathbb{Z}/n\mathbb{Z}$:

$$[a^{\varphi(n)}] = [a]^{\varphi(n)} = g^{|G|} = e_G = [1] \in (\mathbb{Z}/n\mathbb{Z})^* \subset \mathbb{Z}/n\mathbb{Z}\,.$$

Ainsi, on a $[a^{\varphi(n)}] = [1] \in \mathbb{Z}/n\mathbb{Z}$, ce qui signifie que la diffrence $a^{\varphi(n)} - 1$ est un multiple de n. □

Le *petit théorème de Fermat*, déjà mentionné en introduction, n'est autre que le résultat ci-dessus dans le cas particulier où $n = p$ est premier.

Théorème I.15: Petit théorème de Fermat

Soient p un premier et $a \in \mathbb{Z}$ pas un multiple de p. Alors, l'entier $a^{p-1} - 1$ est un multiple de p. □

Terminons cette section par l'exploration de l'énoncé du théorème I.14 pour les premières valeurs de n.

- Pour $n = 1$, l'énoncé est trivial(ement vrai) : pour tout $a \in \mathbb{Z}$, l'entier $a - 1$ est un multiple de 1.
- Pour $n = 2$, l'énoncé est évident : pour tout $a \in \mathbb{Z}$ impair, l'entier $a - 1$ est pair.
- Ça se complique un tout petit peu pour $n = 3$, puisque l'énoncé est le suivant : si $a \in \mathbb{Z}$ n'est pas un multiple de 3, alors $a^2 - 1$ est multiple de 3.

  ⌜ Si a n'est pas un multiple de 3, alors $a + 1$ ou $a - 1$ est un multiple de 3, et donc, le produit $(a - 1)(a + 1) = a^2 - 1$ l'est aussi. ⌟

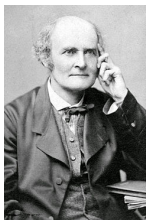
- Les cas $n = 4, 5$ constituent l'exercice 28.

I.6 Groupes symétriques

Rappelons que pour tout ensemble X non-vide, l'ensemble

$$S(X) = \{f : X \to X \mid f \text{ est une bijection}\}$$

est un groupe, appelé le *groupe symétrique* sur X. De plus, on a vu qu'à isomorphisme près, ce groupe ne dépend que du cardinal de l'ensemble X. Si ce cardinal est fini, disons $|X| = n$, alors on note $S(X) = S_n$ le *groupe symétrique de degré n*. Ses éléments sont les *permutations* de n objets.



Arthur Cayley (1821-1895)

Les groupes symétriques sont d'une importance fondamentale pour plusieurs raisons. En voici la première.

Théorème I.16: Théorème de Cayley

Tout groupe est isomorphe à un sous-groupe d'un groupe symétrique.

Démonstration. Soit donc G un groupe quelconque. Posons $X = G$, et considérons l'application

$$\varphi : G \longrightarrow S(G)\,, \quad g \longmapsto \varphi_g$$

définie par

$$\varphi_g : G \longrightarrow G\,, \quad h \longmapsto \varphi_g(h) \coloneqq gh\,.$$

Dans un premier temps, nous allons vérifier que pour tout $g \in G$, l'application $\varphi_g : G \to G$ est bijective (et donc, appartient bien à $S(G)$ comme écrit ci-dessus). Pour ce faire, fixons $h \in G$ et calculons

$$(\varphi_g \circ \varphi_{g^{-1}})(h) = (\varphi_g(\varphi_{g^{-1}}(h)) = g(g^{-1}h) = h\,,$$

d'où $\varphi_g \circ \varphi_{g^{-1}} = \mathrm{id}_G$. On vérifie de même que $\varphi_{g^{-1}} \circ \varphi_g = \mathrm{id}_G$, ce qui montre que φ_g est bijective (d'inverse $(\varphi_g)^{-1} = \varphi_{g^{-1}}$).

Dans un deuxième temps, on va montrer que $\varphi : G \to S(G)$ est un homomorphisme. Pour ce faire, fixons $g_1, g_2 \in G$, et faisons le calcul suivant dans G pour un élément $h \in G$ quelconque :

$$\varphi_{g_1 g_2}(h) = (g_1 g_2)h = (g_1(g_2 h)) = (\varphi_{g_1}(\varphi_{g_2}(h)) = (\varphi_{g_1} \circ \varphi_{g_2})(h)\,.$$

On a ainsi $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$ dans $S(G)$, ce qui montre que φ est un homomorphisme.

Finalement, vérifions que cet homomorphisme est injectif. Si $g_1, g_2 \in G$ sont tels que $\varphi_{g_1} = \varphi_{g_2} \in S(G)$, cela signifie en particulier que

$$g_1 = \varphi_{g_1}(e) = \varphi_{g_2}(e) = g_2\,,$$

et φ est bien injectif.

En conclusion, on a un homomorphisme injectif $\varphi : G \to S(G)$. Cela définit donc un homomorphisme bijectif $\varphi : G \to \mathsf{Im}(G) =: H$, d'où $G \simeq H$. Par la proposition I.1, H est un sous-groupe de $S(G)$, ce qui conclut la preuve. □

Remarque. Si le groupe G est fini, disons d'ordre $|G| = n$, alors on obtient un isomorphisme $G \simeq H < S_n$. Des exemples explicites sont traités en exercice 30.

Dès à présent et jusqu'à la fin de cette section, nous allons nous restreindre aux groupes symétriques finis $S_n = S(\{1, \dots, n\})$ avec $n \geq 1$ fixé.

Il est temps de revenir plus en détail sur la notation en "cycles" déjà brièvement abordée en section I.1.

Notation et terminologie.

- Soit r un entier avec $2 \leq r \leq n$. Une permutation $\sigma \in S_n$ est appelée un *r-cycle* s'il existe $\{x_1, \dots, x_r\} \subset \{1, \dots, n\}$ tel que

$$\sigma(y) = \begin{cases} x_{i+1} & \text{pour } y = x_i \text{ avec } i = 1, \dots, r-1\,; \\ x_1 & \text{pour } y = x_r\,; \\ y & \text{pour } y \in \{1, \dots, n\} \smallsetminus \{x_1, \dots, x_r\}. \end{cases}$$

  On notera cette permutation par

$$\sigma = (x_1, x_2, \dots, x_r) \in S_n\,.$$

- L'ensemble $\{x_1, \dots, x_r\}$ est appelé le *support* de σ. Il s'agit donc des éléments de $\{1, \dots, n\}$ qui ne sont pas fixés par la permutation σ [13].
- Un 2-cycle est appelé une *transposition*.
- Pour $\sigma, \tau \in S_n$, on notera leur composition par $\sigma\tau \coloneqq \sigma \circ \tau \in S_n$ [14].

Les "règles de calcul" suivantes vont nous être très utiles.

Proposition I.17. *Pour tout $\{x_1, \dots, x_r\} \subset \{1, \dots, n\}$, on a les égalités dans S_n :*

(i) $(x_1, x_2, \dots, x_{r-1}, x_r) = (x_2, x_3, \dots, x_r, x_1)$.

(ii) $(x_1, \dots, x_r) = (x_1, \dots, x_j)\,(x_j, \dots, x_r)$ *pour tout* $1 < j < r$.

(iii) $\tau\,(x_1, \dots, x_r)\,\tau^{-1} = (\tau(x_1), \dots, \tau(x_r))$ *pour tout* $\tau \in S_n$.

De plus :

(iv) L'ordre de $(x_1, \dots, x_r)$ *dans S_n est égal à r.*

(v) Deux cycles à supports disjoints commutent.

Démonstration. Les points (i) et (ii) découlent directement des définitions, de même que le point (v). Quant au point (iv), il découle immédiatement de l'interprétation de l'ordre vu en proposition I.2. Concentrons-nous donc sur le point (iii). Pour tout $\tau \in S_n$, la définition d'un cycle implique que la permutation $\sigma \coloneqq \tau\,(x_1, \dots, x_r)$ satisfait

$$\sigma(y) = \begin{cases} \tau(x_{i+1}) & \text{pour } y = x_i \text{ avec } i = 1, \dots, r-1\,; \\ \tau(x_1) & \text{pour } y = x_r\,; \\ \tau(y) & \text{pour } y \in \{1, \dots, n\} \smallsetminus \{x_1, \dots, x_r\}. \end{cases}$$

13. Un 1-cycle n'est autre que l'identité, au support vide, raison pour laquelle on prend $r \geq 2$.
14. On compose donc les permutations comme les applications, "de droite à gauche".

En appliquant cette même définition à la permutation $\sigma' \coloneqq (\tau(x_1), \dots, \tau(x_r))\,\tau$, on obtient

$$\sigma'(y) = \begin{cases} \tau(x_{i+1}) & \text{pour } \tau(y) = \tau(x_i) \text{ avec } i = 1, \dots, r-1\,; \\ \tau(x_1) & \text{pour } \tau(y) = \tau(x_r)\,; \\ \tau(y) & \text{pour } \tau(y) \in \{1, \dots, n\} \smallsetminus \{\tau(x_1), \dots, \tau(x_r)\}. \end{cases}$$

Comme τ est une bijection, a bien l'égalité $\sigma = \sigma'$, qui est équivalente à l'égalité $\tau\,(x_1, \dots, x_r)\,\tau^{-1} = (\tau(x_1), \dots, \tau(x_r))$. □

Le théorème suivant montre en particulier que la notation en cycles, et donc les règles de calcul associées, peuvent être appliquées à tous les éléments de S_n.

Théorème I.18

Toute permutation est composition de cycles à supports disjoints.

Démonstration. Soit donc $\sigma \in S_n$ fixé. Considérons *l'orbite*[15] de $1 \in \{1, \dots, n\}$, i.e. les éléments $1, \sigma(1), \sigma^2(1), \dots$ de $\{1, \dots, n\}$. Comme l'ensemble $\{1, \dots, n\}$ est fini et σ injectif, il existe un entier $r \geq 1$ tel que $\sigma^r(1) = 1$. Considérons le $r \geq 1$ minimal tel que $\sigma^r(1) = 1$. Par définition, σ permute cycliquement ces éléments, et on a donc un premier r-cycle

$$\sigma_1 \coloneqq \big(1, \sigma(1), \sigma^2(1), \dots, \sigma^{r-1}(1)\big)\,.$$

(Ici, on admet la possibilité d'un 1-cycle, qui n'est autre que l'identité.) Si le support de σ_1 est égal à tout l'ensemble $\{1, \dots, n\}$, on a fini puisque $\sigma = \sigma_1$. Sinon, on recommence[16] avec le plus petit élément $i \in \{1, \dots, n\} \smallsetminus \{1, \sigma(1), \dots, \sigma^{r-1}(1)\}$, d'où un second cycle

$$\sigma_2 \coloneqq \big(i, \sigma(i), \sigma^2(i), \dots, \sigma^{s-1}(i)\big)\,,$$

avec $s \geq 1$ le plus petit entier tel que $\sigma^s(i) = i$. Notons que les cycles σ_1 et σ_2 sont à supports disjoints : sinon, on aurait $k, \ell \geq 1$ tels que $\sigma^k(i) = \sigma^\ell(1)$, d'où $i = \sigma^{\ell-k}(1)$ dans le support de σ_1, une contradiction. Si les supports de σ_1 et de σ_2 recouvrent tout l'ensemble $\{1, \dots, n\}$, on a fini puisque $\sigma = \sigma_1\sigma_2$. Sinon, on recommence.

Comme l'ensemble $\{1, \dots, n\}$ est fini, cette procédure se termine, lorsque l'union des supports des cycles $\sigma_1, \sigma_2, \dots, \sigma_m$ recouvre $\{1, \dots, n\}$. On a alors

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_m \in S_n\,,$$

qui est donc bien composition de cycles à supports disjoints. Il ne reste plus qu'à ôter les éventuels 1-cycles qui ne contribuent pas à cette composition, et la preuve est terminée. □

15. Cette terminologie, que nous n'utiliserons pas dans le cadre de ce cours, vient de la théorie des *actions de groupes*, voir GÉOMÉTRIE I.

16. Comme chaque fois que les mots "on recommence" sont écrits dans une démonstration, une preuve parfaitement formelle se ferait par récurrence, ici sur $n \geq 1$.

Exemple. Considérons la permutation $\sigma \in S_6$ donnée, en notation du premier semestre, par le tableau

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 4 & 2 & 3 \end{pmatrix}.$$

En appliquant l'algorithme de la preuve du théorème I.18, on obtient un premier cycle $\sigma_1 = (1,5,2)$, un second cycle $\sigma_2 = (3,6)$, et un dernier cycle $\sigma_3 = (4)$ qui ne contribue pas, d'où

$$\sigma = (1,5,2)(3,6)\,.$$

Remarques.

1. La décomposition $\sigma = \sigma_1 \dots \sigma_m$ d'une permutation $\sigma \in S_n$ en produit de cycles à supports disjoints n'est pas unique. En effet, par les points (v) et (i) de la proposition I.17, les opérations suivantes ne changent pas σ :
   - permutation des cycles $\sigma_1, \dots, \sigma_m$;
   - permutation cyclique du support d'un des cycles $\sigma_1, \dots, \sigma_m$.

   Par exemple, la permutation $\sigma = (1,5,2)(3,6) \in S_6$ peut s'écrire

   $$\sigma = (1,5,2)(3,6) = (3,6)(1,5,2) = (6,3)(1,5,2) = (6,3)(5,2,1) = \dots$$

2. En revanche, la décomposition d'une permutation en produit de cycles à supports disjoints est unique aux deux opérations ci-dessus près. En d'autres termes, si $\sigma_1 \dots \sigma_m = \sigma'_1 \dots \sigma'_{m'}$ sont deux produits de cycles à supports disjoints, alors on a $m = m'$, et ces produits sont reliées par une suite des opérations ci-dessus.

Le théorème I.18 et la proposition I.17 permettent de calculer de façon très efficace dans S_n. Ce deux énoncés impliquent également le résultat suivant.

Corollaire I.19. *Toute permutation est produit de transpositions.*

Démonstration. Soit donc $\sigma \in S_n$ quelconque. Par le théorème I.18, on peut écrire σ comme produit de cycles. Par le point (ii) de la proposition I.17 (appliqué $r-2$ fois), chaque cycle peut être dcomposé en produit de transpositions via $(x_1, x_2, \dots, x_{r-1}, x_r) = (x_1, x_2)(x_2, x_3)\cdots(x_{r-1}, x_r)$, ce qui conclut la preuve. □

Venons-en maintenant à la signature d'une permutation.

Définition I.5

La **signature** de $\sigma \in S_n$ est

$$\varepsilon(\sigma) \coloneqq \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}\,.$$

Remarques.

1. Ainsi, la signature de $\sigma \in S_n$ est donné par un produit indexé par l'ensemble des $\binom{n}{2} = \frac{n(n-1)}{2}$ paires ordonnées (i,j) avec $i<j$ dans $\{1,\dots,n\}$.
2. De manière équivalente, on aurait pu écrire
$$\varepsilon(\sigma) = \prod_{\{i,j\}\subset\{1,\dots,n\}} \frac{\sigma(i)-\sigma(j)}{i-j}\,.$$
En effet, ce nouveau produit est sur l'ensemble des $\binom{n}{2}$ paires non-ordonnées dans $\{1,\dots,n\}$, et le facteur $\frac{\sigma(i)-\sigma(j)}{i-j}$ est inchangé si on échange les rôles de i et j.
3. Comme i,j sont distincts et σ injectif, chaque facteur $\frac{\sigma(i)-\sigma(j)}{i-j}$ est un nombre rationnel non-nul. Par conséquent, la signature définit une application $\varepsilon\colon S_n \to \mathbb{Q}^*$.

Exemples.

1. Pour $\sigma = \mathrm{id} \in S_n$, on a trivialement $\varepsilon(\mathrm{id}) = \prod \frac{i-j}{i-j} = 1$.
2. Pour $\sigma = (1,2) \in S_2$, on a $\varepsilon(\sigma) = \frac{2-1}{1-2} = -1$.
3. Pour $\sigma = (1,2,3) \in S_3$, on a $\varepsilon(\sigma) = \frac{2-3}{1-2}\cdot\frac{2-1}{1-3}\cdot\frac{3-1}{2-3} = 1$.

Comme on le voit sur ces exemples, cette définition n'est absolument pas adaptées aux calculs ! En revanche, elle mène à l'énoncé suivant, qui permet de calculer très facilement la signature d'une permutation quelconque.

Proposition I.20. *La signature définit un homomorphisme de groupes*
$$\varepsilon\colon S_n \longrightarrow \{-1,1\}$$
avec $\varepsilon(\sigma) = -1$ *pour toute transposition* σ.

Démonstration. Cette démonstration va se faire en trois étapes, et utiliser la remarque 2 ci-dessus, et donc la définition suivante de la signature :
$$\varepsilon(\sigma) = \prod_{\{i,j\}\subset\{1,\dots,n\}} \frac{\sigma(i)-\sigma(j)}{i-j}\,.$$

Dans un premier temps, nous allons vérifier que $\varepsilon\colon S_n \to \mathbb{Q}^*$ est un homomorphisme. Soient donc $\sigma,\tau \in S_n$, et calculons dans $\mathbb{Q}^*$:

$$\begin{aligned}
\varepsilon(\sigma\tau) &= \prod_{\{i,j\}\subset\{1,\dots,n\}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{i-j} = \prod_{\{i,j\}\subset\{1,\dots,n\}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)}\cdot\frac{\tau(i)-\tau(j)}{i-j} \\
&= \prod_{\{i,j\}\subset\{1,\dots,n\}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} \prod_{\{i,j\}\subset\{1,\dots,n\}} \frac{\tau(i)-\tau(j)}{i-j} \\
&= \prod_{\{k,\ell\}\subset\{1,\dots,n\}} \frac{\sigma(k)-\sigma(\ell)}{k-\ell} \prod_{\{i,j\}\subset\{1,\dots,n\}} \frac{\tau(i)-\tau(j)}{i-j} = \varepsilon(\sigma)\varepsilon(\tau)\,.
\end{aligned}$$

Dans l'avant-dernier pas, on a utilisé le fait que comme $\tau\colon\{1,\dots,n\}\to\{1,\dots,n\}$ est une bijection, cela définit une bijection dans lui-même de l'ensemble des paires non-ordonnées $\{i,j\}\subset\{1,\dots,n\}$. On a donc vérifié que $\varepsilon\colon S_n\to\mathbb{Q}^*$ est un homomorphisme.

Dans un second temps, calculons la signature d'une transposition quelconque, disons $\sigma=(u,v)\in S_n$. Pour ce faire, considérons la partition de l'ensemble des paires non-ordonnées $\{i,j\}\subset\{1,\dots,n\}$ en les trois sous-ensembles suivants : les paires $\{i,j\}$ telles que $\{i,j\}\cap\{u,v\}$ est vide ; les paires telles que $\{i,j\}\cap\{u,v\}$ compte exactement un élément ; et finalement, la paire $\{i,j\}=\{u,v\}$. Dans la définition de la signature $\varepsilon(\sigma)$, le premier sous-ensemble contribue le facteur

$$\prod_{\substack{\{i,j\}\subset\{1,\dots,n\}\\ \{i,j\}\cap\{u,v\}=\varnothing}}\frac{\sigma(i)-\sigma(j)}{i-j}=\prod_{\substack{\{i,j\}\subset\{1,\dots,n\}\\ \{i,j\}\cap\{u,v\}=\varnothing}}\frac{i-j}{i-j}=1\,.$$

Quant au second sous-ensemble, il contribue le facteur

$$\prod_{\substack{\{i,j\}\subset\{1,\dots,n\}\\ i=u,\ j\neq v}}\frac{\sigma(i)-\sigma(j)}{i-j}\prod_{\substack{\{i,j\}\subset\{1,\dots,n\}\\ i=v,\ j\neq u}}\frac{\sigma(i)-\sigma(j)}{i-j}=\prod_{j\neq u,v}\frac{v-j}{u-j}\prod_{j\neq u,v}\frac{u-j}{v-j}=1\,.$$

Finalement, le troisième sous-ensemble contribue

$$\prod_{\substack{\{i,j\}\subset\{1,\dots,n\}\\ \{i,j\}=\{u,v\}}}\frac{\sigma(i)-\sigma(j)}{i-j}=\frac{j-i}{i-j}=-1\,.$$

Ainsi, on a bien $\varepsilon(\sigma)=-1$.

En conclusion, la signature définit un homomorphisme $\varepsilon\colon S_n\to\mathbb{Q}^*$ et prend la valeur -1 pour les transpositions. Comme toute permutation σ est produit de transpositions $\sigma_1\cdots\sigma_s$ (corollaire I.19), on a donc $\varepsilon(\sigma)=\varepsilon(\sigma_1)\cdots\varepsilon(\sigma_s)=(-1)^s$. Cela conclut la preuve. □

Remarques.

1. Ainsi, on a $\varepsilon(\sigma)=+1$ (resp. $\varepsilon(\sigma)=-1$) si et seulement si σ est composition d'un nombre pair (resp. impair) de transpositions. On dit alors que $\sigma\in S_n$ est une permutation *paire* (resp. *impaire*).
2. Pour $\sigma\in S_n$, une décomposition de σ en produit de transpositions n'est pas unique : par exemple, on a $(1,3)=(2,3)(1,2)(2,3)$ et $\mathrm{id}=(1,2)(1,2)$. Mais la parité du nombre de facteurs apparaissant dans une décomposition de σ en produit de transpositions est bien définie.

Définition I.6

Le sous-ensemble de S_n formé des permutations paires s'appelle le **groupe alterné** de degré n, et est noté A_n.

Remarques.

1. Comme $A_n = \mathrm{Ker}(\varepsilon)$, c'est bien un sous-groupe de S_n (proposition I.3).
2. Pour $n \geq 2$, on a exactement 2 classes à gauche modulo A_n dans S_n : la classe à gauche de id, qui n'est autre que A_n, i.e. l'ensemble des permutations paires ; et la classe à gauche de $(1,2)$, formé de l'ensemble des permutations impaires. Par le théorème de Lagrange, on a donc

$$|A_n| = \frac{|S_n|}{[S_n : A_n]} = \frac{n!}{2}$$

pour tout $n \geq 2$.

Exemples.

1. Clairement, les groupes alternés de degrés 1 et 2 sont triviaux.
2. Pour $n = 3$, on a $A_3 = \{\mathrm{id}, (1,2,3), (1,3,2)\} < S_3$. Ainsi, le groupe alterné de degré 3 est cyclique d'ordre 3.
3. Le groupe A_4 est d'ordre $\frac{4!}{2} = 12$ et non-abélien, puisque $(1,2,3)$ et $(2,3,4)$ ne commutent pas, par exemple.
4. Par la proposition I.17 (ii), un r-cycle est produit de $r-1$ transpositions. Ainsi,
$$\varepsilon((x_1, \ldots, x_r)) = (-1)^{r-1}.$$
En particulier, les 3-cycles sont pairs.

On a une réciproque partielle à ce dernier exemple.

Proposition I.21. *Le groupe A_n est engendré par les 3-cycles.*

Démonstration. Comme tout élément de A_n est produit d'un nombre paire de transpositions, il suffit de vérifier que le produit de 2 transpositions peut être exprimé comme composition de 3-cycles. Soient donc (x_1, x_2) et (x_3, x_4) deux transpositions arbitraires dans S_n. Il y a trois cas à distinguer.

- Supposons tout d'abord que les supports $\{x_1, x_2\}$ et $\{x_3, x_4\}$ sont disjoints. Dans ce cas, on vérifie l'égalité $(x_1, x_2)(x_3, x_4) = (x_1, x_2, x_3)(x_2, x_3, x_4)$.
- Supposons dans un second temps que les supports $\{x_1, x_2\}$ et $\{x_3, x_4\}$ comptent un unique élément commun, disons $x_1 = x_3$ et $x_2 \neq x_4$ sans restreindre la généralité. Alors, on a $(x_1, x_2)(x_3, x_4) = (x_2, x_1)(x_1, x_4) = (x_2, x_1, x_4)$.
- Enfin, si $\{x_1, x_2\} = \{x_3, x_4\}$, alors on a $(x_1, x_2)(x_3, x_4) = \mathrm{id}$.

Dans chacun des cas, le produit $(x_1, x_2)(x_3, x_4)$ est composition de 3-cycles, ce qu'il fallait démontrer. □

I.7 Commutateurs, groupes résolubles

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

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

Remarques.

1. Le commutateur de g et h est trivial si et seulement si $gh = hg \in G$. On dit alors que *g et h commutent*.
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 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. Cela justifie la terminologie suivante.

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

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

Remarques.

5. Par définition, les éléments de $[G,G]$ sont les compositions de commutateurs et d'inverses de commutateurs. Mais par la remarque 3 ci-dessus, les compositions de commutateurs suffisent. Ainsi, on a $x \in [G,G]$ si et seulement s'il existe $g_1, h_1, \ldots, g_\ell, h_\ell \in G$ tel que $x = [g_1,h_1]\cdots[g_\ell,h_\ell]$.
6. Si $\varphi: G \to G$ est un homomorphisme , alors $\varphi([G,G]) = [\varphi(G),\varphi(G)]$. C'est le premier point de l'exercice 38.

Exemples (de 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 $\varepsilon([\sigma,\tau]) = [\varepsilon(\sigma),\varepsilon(\tau)] = 1$ 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, il suffit par la proposition I.21 de montrer que tout 3-cycle est un commutateur. C'est le cas, via l'égalité $(x_1,x_2,x_3) = [(x_2,x_3),(x_1,x_2)] \in S_n$. ⌟

Terminologie. Pour un groupe G, on note

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

On obtient donc une suite de sous-groupes

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

appelée la *suite dérivée* de G.

Définition I.7

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

Exemples (de groupes résolubles)**.**

0. Un groupe G est trivial si et seulement si $G^{(0)} = \{e\}$. Ainsi, un groupe trivial (par exemple, le groupe S_1) est résoluble.
1. Un groupe G est abélien si et seulement si $G^{(1)} = \{e\}$. Ainsi, un groupe abélien (par exemple, le groupe S_2) est résoluble.
2. Qu'en est-il de S_3 ? Par l'exemple 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.
3. 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 37 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.

Théorème I.22

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 connait 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. Par la proposition I.21, 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 $\ell, m \in \{1, \dots, n\}$ tels que i, j, k, ℓ, m sont tous distincts. On calcule alors, par exemple en utilisant les points (ii) et (iii) de la proposition I.17 :

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

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

Remarque. Cette discussion n'est pas sans rappeler l'introduction du cours, et ce n'est pas un hasard. En effet, par la théorie de Galois que vous verrez en ALGÈBRE II, 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 $n \leq 4$.

Plus précisément, on peut associer à tout polynôme un groupe, tel que l'équation polynomiale correspondante est résoluble par radicaux si et seulement si le groupe associé est résoluble [17]. Comme le groupe associé au polynôme général de degré n est le groupe symétrique S_n, le théorème I.22 nous donne le résultat.

I.8 Sous-groupes normaux, quotients, groupes simples

Nous commençons cette section avec le rappel de quelques notions de théorie des ensembles, d'une importance fondamentale dans le cadre de ce cours (et de bien d'autres).

- Si X est un ensemble muni d'une relation d'équivalence $\sim$, alors la *classe d'équivalence* de $x \in X$ est le sous-ensemble

$$[x] \coloneqq \{x' \in X \mid x \sim x'\}$$

de X. Les classes d'équivalence forment une partition de X : tout $x \in X$ appartient à une unique classe d'équivalence.

- On note

$$X/\!\sim \coloneqq \{[x] \mid x \in X\}$$

l'ensemble de ces classes d'équivalence, appelé *ensemble quotient*, et

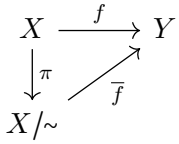
$$\pi \colon X \longrightarrow X/\!\sim, \quad x \longmapsto \pi(x) = [x]$$

l'application surjective qui associe à tout $x \in X$ sa classe d'équivalence. Cette application est appelée la *projection canonique*.

- On dit qu'une application $f \colon X \to Y$ *passe au quotient* si elle satisfait la propriété suivante pour tous $x, x' \in X$: $x \sim x' \Rightarrow f(x) = f(x')$. Si tel est le cas, on a une *application induite* bien définie sur l'ensemble quotient :

$$\overline{f} \colon X/\!\sim \longrightarrow Y, \quad [x] \longmapsto \overline{f}([x]) = f(x)\,.$$

En d'autres termes, on a l'égalité $\overline{f} \circ \pi = f$, qu'il est souvent utile de visualiser sous la forme du "diagramme commutatif" suivant :



Voyons quelques exemples triviaux mais relativement "concrets".

17. Cela justifie bien entendu cette terminologie.

Exemples.

1. Considérons l'ensemble X des habitants de la Suisse, muni de la relation d'équivalence définie par $x \sim x'$ si et seulement si x et x' ont la même date de naissance. On peut voir l'ensemble quotient $X/\sim$ comme l'ensemble des jours (où un habitant de la Suisse est né).
   Soit à présent la fonction $f\colon X \to \mathbb{N}$ donnée par $f(x)$ = l'âge de x en années. Clairement, cette application passe au quotient, puisque deux personnes nées le même jour ont le même âge. L'application induite $\overline{f}\colon X/\sim \to \mathbb{N}$ est la fonction qui calcule le nombre d'années écoulées depuis un jour donné.
   En revanche, la fonction $f\colon X \to \mathbb{N}$ donnée par $f(x)$ =le salaire mensuel de x ne passe bien évidemment *pas* au quotient : deux personnes nées le même jour n'ont en général pas le même salaire.
2. Considérons l'ensemble $X = \mathbb{Z}$ muni de la relation d'équivalence définie par $x \sim x'$ si et seulement si $x - x'$ est pair. L'ensemble quotient n'est autre que $\mathbb{Z}/2\mathbb{Z}$.
   La fonction $f\colon \mathbb{Z} \to \mathbb{Z}$ donnée par $f(x) = 0$ si x est pair et $f(x) = 1$ si x est impair passe au quotient, et induit une bijection $\overline{f}\colon \mathbb{Z}/2\mathbb{Z} \to \{0,1\}$.
   En revanche, l'application $f\colon \mathbb{Z} \to \mathbb{Z}$ donnée par $f(x) = x + 1$ ne passe *pas* au quotient : en effet, on a par exemple $0 \sim 2 \in \mathbb{Z}$ mais $f(0) = 1 \neq 3 = f(2)$.

Revenons maintenant à l'algèbre.

Dans la preuve du théorème de Lagrange, on a vu la relation d'équivalence suivante sur l'ensemble $X = G$ donné par un groupe quelconque : pour H un sous-groupe de G et $g_1, g_2 \in G$, on pose

$$g_1 \sim g_2 \quad \Leftrightarrow \quad g_2^{-1} g_1 \in H\,.$$

Rappelons que cette relation d'équivalence est une généralisation naturelle de la congruence modulo n dans $\mathbb{Z}$. Rappelons également que l'ensemble quotient correspondant n'est autre que

$$G/H = \{[g] \,|\, g \in G\} = \{gH \,|\, g \in G\}\,,$$

l'ensemble des classes à gauche dans G modulo H.

Dans le cas de la congruence modulo n dans $\mathbb{Z}$, on a vu en section I.1 que l'addition passe au quotient et défini une loi de composition sur $\mathbb{Z}/n\mathbb{Z}$, qui en fait un groupe. Cela amène naturellement à la question suivante.

Question 1. Étant donné un sous-groupe H d'un groupe $(G, \star)$, est-ce que la loi de composition

$$G \times G \longrightarrow G, \quad (g_1, g_2) \longmapsto g_1 \star g_2$$

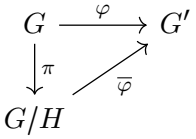
passe au quotient et induit une loi de composition

$$G/H \times G/H \longrightarrow G/H, \quad ([g_1], [g_2]) \longmapsto [g_1] \star [g_2] \coloneqq [g_1 \star g_2]\,,$$

qui donne une structure de groupe sur le quotient G/H ?

Cela amène également la question suivante :

Question 2. Si tel est le cas, quand un homomorphisme $\varphi: G \to G'$ passe-t-il au quotient pour induire un homomorphisme $\overline{\varphi}: G/H \to G'$?



Pour répondre à ces questions, la notion cruciale est la suivante.

Définition I.8

Un sous-groupe $N < G$ est dit **normal** dans G, noté $N \lhd H$, si pour tout $g \in G$, on a $gNg^{-1} = N$.

Remarque. En fait, un sous-groupe $N < G$ est normal si et seulement s'il satisfait la condition suivante, que l'on va utiliser systématiquement :

$$g \in G, x \in N \Rightarrow gxg^{-1} \in N\,.$$

⌜ En effet, si $N \lhd G$, alors on a en particulier $gNg^{-1} \subset N$ pour tout $g \in G$, ce qui est précisément la condition ci-dessus. Réciproquement, supposons que $gNg^{-1} \subset N$ pour tout $g \in G$. En appliquant cela à $g^{-1} \in G$, on obtient $g^{-1}Ng \subset N$, d'où $N \subset gNg^{-1}$. Ces deux inclusions donnent l'égalité $gNg^{-1} = N$ voulue. ⌟

Voici la réponse à la première question.

Proposition I.23. *Si N est un sous-groupe normal d'un groupe G, alors l'ensemble quotient $G/N = \{[g] \,|\, g \in G\}$ est un groupe pour la loi*

$$G/N \times G/N \longrightarrow G/N, \quad ([g_1],[g_2]) \longmapsto [g_1][g_2] \coloneqq [g_1 g_2]\,.$$

De plus, la projection canonique $\pi: G \to G/N$ est un homomorphisme surjectif de noyau $\mathrm{Ker}(\pi) = N$.

Démonstration. Le point crucial est de vérifier que la loi de composition est bien définie sur G/N, i.e. que si $g_1, h_1, g_2, h_2 \in G$ satisfont $g_1 \sim h_1$ et $g_2 \sim h_2$, alors on a $g_1 g_2 \sim h_1 h_2$. Par hypothèse et définition de la relation d'équivalence, on a $h_1^{-1} g_1 \in N$ et $h_2^{-1} g_2 \in N$. Comme N est normal dans G et contient $x = h_1^{-1} g_1$, il contient également $g_2^{-1} x g_2 = g_2^{-1}(h_1^{-1} g_1) g_2$. Comme N est un sous-groupe de G, il contient la composition

$$(h_2^{-1} g_2)(g_2^{-1} h_1^{-1} g_1 g_2) = h_2^{-1} h_1^{-1} g_1 g_2 = (h_1 h_2)^{-1} g_1 g_2\,,$$

ce qui montre qu'on a bien $g_1 g_2 \sim h_1 h_2$.

Les autres vérifications sont purement formelles. L'associativité de la loi dans G/N découle de l'associativité de la loi dans G via les égalités

$$([g][h])[k] = [gh][k] = [(gh)k] = [g(hk)] = [g][hk] = [g]([h][k]),$$

valides pour tous $g, h, k \in G$. Le neutre de G/N est bien entendu $e_{G/N} \coloneqq [e_G]$, puisqu'il satisfait

$$e_{G/N}[g] = [e_G][g] = [e_G g] = [g] = [g e_G] = [g][e_G] = [g] e_{G/N}$$

pour tout $g \in G$. L'inverse d'une classe $[g]$ fixée est donné par $[g]^{-1} \coloneqq [g^{-1}]$, puisqu'on a

$$[g]^{-1}[g] = [g^{-1}][g] = [g^{-1}g] = [e_G] = e_{G/N},$$

et similairement $[g][g]^{-1} = e_{G/N}$. On est donc bien en présence d'un groupe.

Finalement, la projection canonique $\pi : G \to G/N$ donnée par $\pi(g) = [g]$ est un homomorphisme, puisqu'elle satisfait

$$\pi(gh) = [gh] = [g][h] = \pi(g)\pi(h)$$

pour tous $g, h \in G$, et elle est surjective par définition. Un élément $g \in G$ appartient au noyau de π si et seulement s'il satisfait

$$[g] = \pi(g) = e_{G/N} = [e_G],$$

i.e. $g \sim e_G$, ce qui est équivalent à $g \in N$. Cela montre l'égalité $\mathrm{Ker}(\pi) = N$ et conclut la preuve. □

Terminologie. Si N est un sous-groupe normal d'un groupe G, alors G/N est appelé le *groupe quotient* de G par N [18].

Venons-en finalement à des exemples de sous-groupes normaux, et de groupes quotients.

Exemples (de sous-groupes normaux)**.**

1. Dans tout groupe G, le sous-groupe trivial $N = \{e\}$ est normal.

   ⌜ En effet, pour tous $g \in G$ et $x \in \{e\}$, on a $gxg^{-1} = geg^{-1} = e \in N$. ⌟

2. Dans tout groupe G, le sous-groupe $N = G$ est normal.

   ⌜ En effet, pour tous $g, x \in G$, on a $gxg^{-1} \in G$. ⌟

3. Dans un groupe G abélien, tout sous-groupe $N = H$ est normal.

   ⌜ En effet, pour tous $x \in N$ et $g \in G$, on a $gxg^{-1} = gg^{-1}x = x \in N$. ⌟

18. Intuitivement, lorsqu'on quotiente un groupe G par $N \triangleleft G$, on "tue" le sous-groupe N en identifiant tous ses éléments entre eux (et au neutre).

4. Pour tout groupe G, le centre $Z(G)$ est normal dans G : la preuve est identique à celle ci-dessus.

5. Si $\varphi: G \to G'$ est un homomorphisme, alors $\mathrm{Ker}(\varphi) \lhd G$.

   ⌜ En effet, soient $x \in \mathrm{Ker}(\varphi)$ et $g \in G$. Comme φ est un homomorphisme, on a

   $$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)e_{G'}\varphi(g)^{-1} = e_{G'},$$

   d'où $gxg^{-1} \in \mathrm{Ker}(\varphi)$. ⌟

   Réciproquement, on a vu en proposition I.23 que tout $N \lhd G$ est le noyau de l'homomorphisme $\pi: G \to G/N$. En conclusion :

Les sous-groupes normaux sont les noyaux des homomorphismes.

6. Pour tout $n \geq 1$ et $K = \mathbb{R}$ ou $\mathbb{C}$, le groupe spécial linéaire $\mathrm{SL}(n, K)$ est normal dans $\mathrm{GL}(n, K)$, puisque c'est le noyau de $\det: \mathrm{GL}(n, K) \to K^*$.

7. Pour tout $n \geq 1$, le groupe alterné A_n est normal dans le groupe symétrique S_n, puisque $A_n = \mathrm{Ker}(\varepsilon: S_n \to \{-1, 1\})$.

8. Pour tout groupe G, le groupe $\mathrm{Int}(G)$ des automorphismes intérieurs de G est normal dans $\mathrm{Aut}(G)$: c'est l'exercice 40.

9. Pour tout groupe G, le groupe dérivé $[G, G]$ est normal dans G : c'est le troisième point de l'exercice 38.

10. Tout sous-groupe d'indice 2 est normal.

    ⌜ Soit donc H un sous-groupe de G avec $[G : H] = 2$, d'où $2 = |G/H| = |H\backslash G|$. Ainsi, pour tout $g \in G \smallsetminus H$, on a une partition $G = H \sqcup gH = H \sqcup Hg$. Par conséquent, pour tout $g \in G \smallsetminus H$, on a $gH = Hg$, i.e. $gHg^{-1} = H$. D'autre part, pour tout $g \in H$, on a bien évidemment $gH = H = Hg$, d'où $gHg^{-1} = H$. En conclusion, l'égalité $gHg^{-1} = H$ vaut pour tout $g \in G$, ce qui montre $H \lhd G$. ⌟

11. Pour terminer, cherchons un exemple de sous-groupe $H < G$ qui n'est *pas* normal. Par l'exemple 3 ci-dessus, il faut que G ne soit pas abélien. Par le corollaire I.7, tout groupe d'ordre $2, 3$ ou 5 est cyclique et donc abélien. De plus, on vérifie facilement que tout groupe d'ordre 4 est abélien[19]. Ainsi, le groupe non-abélien le plus petit est d'ordre 6, et c'est $G = S_3$. Par le corollaire I.5, un sous-groupe $H < S_3$ est d'ordre 1 (et normal par l'exemple 1 ci-dessus), d'ordre 2, d'ordre 3 (et normal par l'exemple 10) ou d'ordre 6 (et normal par l'exemple 2). Ainsi, les seuls sous-groupes qui ont une chance de ne pas être normaux sont ceux d'ordre 2.
    Considérons donc $H = \{\mathrm{id}, (1,2)\} < S_3 = G$. Pour $x = (1,2) \in H$ et $g = (1,3) \in S_3$, on a $gxg^{-1} = (1,3)(1,2)(1,3) = (2,3) \notin H$. Ainsi, le sous-groupe H n'est effectivement *pas* normal dans S_3.

19. En effet, si G contient un élément d'ordre 4, alors il est cyclique, et donc abélien (isomorphe à $\mathbb{Z}/4\mathbb{Z}$). Sinon, par le corollaire I.6, tous les éléments non-triviaux de G sont d'ordre 2, ce qui implique que G est abélien (isomorphe au groupe de Klein V).

Tentons à présent de calculer quelques exemples de groupes quotients.

Exemples (de groupes quotients)**.**

1. Pour $N = \{e\} \lhd G$, la relation d'équivalence correspondante n'est autre que l'égalité, puisque $g_1 \sim g_2$ si et seulement si $g_2^{-1} g_1 \in \{e\}$, ce qui équivaut à $g_1 = g_2$. Ainsi, l'ensemble quotient correspondant est formé de singletons

$$G/\{e\} = \{\{g\} \,|\, g \in G\}\,.$$

   La projection canonique $\pi : G/\{e\} \to G$ est donc bijective, et fournit ainsi un isomorphisme $G/\{e\} \simeq G$ [20].

2. Pour $N = G \lhd G$, on a $g_1 \sim g_2$ si et seulement si $g_2^{-1} g_1 \in G$, ce qui est toujours le cas. Ainsi, l'ensemble quotient correspondant est formé d'une unique classe d'équivalence :

$$G/G = \{G\} = \{e_{G/G}\}\,,$$

   et on est en présence du groupe trivial [21] .

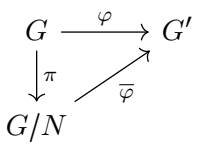
3. Pour $G = \mathbb{Z}$, tout sous-groupe est de la forme $H = n\mathbb{Z}$ par la proposition I.9, il est normal dans $\mathbb{Z}$ puisque c'est un groupe abélien, et le groupe quotient correspondant est par construction $\mathbb{Z}/n\mathbb{Z}$, le groupe des entiers modulo n.

4. Pour $N \lhd G$ d'indice 2, le groupe quotient G/N est d'ordre 2, d'où $G/N \simeq \mathbb{Z}/2\mathbb{Z}$ par l'exemple 2 en section I.3. En particulier, on a $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$.

5. Pour $N = [G, G] \lhd G$, le groupe quotient $G/[G, G]$ est abélien (exercice 46).

6. Considérons le sous-groupe normal $(\mathbb{Z}, +)$ du groupe abélien $(\mathbb{R}, +)$. La relation d'équivalence correspondante est $x \sim x' \in \mathbb{R} \Leftrightarrow x - x' \in \mathbb{Z}$. Ainsi, on identifie dans $\mathbb{R}/\mathbb{Z}$ deux réels dont la différence est un entier. On verra très prochainement l'isomorphisme $\mathbb{R}/\mathbb{Z} \simeq S^1$, dont on peut avoir une intuition géométrique en "enroulant" la droite réelle $\mathbb{R}$ autour du cercle S^1 de telle manière que deux réels distants de 1 sont envoyés sur le même point du cercle.

Tournons-nous à présent vers la seconde question : étant donné un sous-groupe normal $N \lhd G$, quand un homomorphisme $\varphi : G \to G'$ passe-t-il au quotient pour induire un homomorphisme $\overline{\varphi} : G/N \to G'$ tel que $\overline{\varphi} \circ \pi = \varphi$? Notons que si tel est le cas, on a



$$N = \mathrm{Ker}(\pi) \subset \mathrm{Ker}(\overline{\varphi} \circ \pi) = \mathrm{Ker}(\varphi)\,.$$

Comme nous allons maintenant le démontrer, cette condition nécessaire est aussi suffisante.

20. Intuitivement, "on n'a rien tué du tout".
21. Intuitivement, "on a tout tué".

Proposition I.24. *Soit N un sous-groupe normal d'un groupe G. Si $\varphi: G \to G'$ est un homomorphisme avec $N \subset \mathrm{Ker}(\varphi)$, alors il existe un unique homomorphisme $\overline{\varphi}: G/N \to G'$ tel que $\overline{\varphi} \circ \pi = \varphi$.*

Démonstration. Tout d'abord, l'application induite $\overline{\varphi}: G/N \to G'$ est uniquement déterminé par la condition $\overline{\varphi} \circ \pi = \varphi$, puisqu'on a

$$\overline{\varphi}([g]) = \overline{\varphi}(\pi(g)) = (\overline{\varphi} \circ \pi)(g) = \varphi(g)$$

pour tout $g \in G$. Le fait que $\overline{\varphi}$ est un homomorphisme est également automatique, via les égalités

$$\overline{\varphi}([g_1][g_2]) = \overline{\varphi}([g_1 g_2]) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}([g_1])\overline{\varphi}([g_2])$$

pour tous $g_1, g_2 \in G$.

Le seul point non-trivial, et celui qui utilise l'hypothèse, est le fait que φ passe au quotient, i.e. que l'application induite $\overline{\varphi}$ est bien définie. Pour le vérifier, prenons $g_1, g_2 \in G$ avec $[g_1] = [g_2] \in G/N$, et tentons de montrer que $\overline{\varphi}([g_1]) = \overline{\varphi}([g_2])$, i.e. que $\varphi(g_1) = \varphi(g_2)$. Par hypothèse, on a $g_2^{-1} g_1 \in N \subset \mathrm{Ker}(\varphi)$, d'où

$$e_{G'} = \varphi(g_2^{-1} g_1) = \varphi(g_2)^{-1}\varphi(g_1)\,,$$

ce qui montre l'égalité $\varphi(g_1) = \varphi(g_2)$ et conclut la preuve. □

Étant donné un homomorphisme de groupes $\varphi: G \to G'$, il n'est pas difficile de le rendre surjectif : il suffit pour cela de restreindre son image et de considérer l'homomorphisme $\varphi: G \to \mathsf{Im}(\varphi)$. En revanche, il n'est pas évident de le rendre injectif : pour cela, il s'agirait en effet de rendre son noyau trivial. Or c'est exactement ce que la construction du groupe quotient permet de faire.

Nous sommes maintenant en mesure de montrer le résultat correspondant, communément appelé *premier théorème d'isomorphisme*[22].

Théorème I.25: Premier théorème d'isomorphisme

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

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

Démonstration. Soit donc $\varphi: G \to G'$ un homomorphisme de groupes quelconque. Par l'exemple 5 ci-dessus, on sait que $N \coloneqq \mathrm{Ker}(\varphi)$ est normal dans G. Comme on a trivialement $N \subset \mathrm{Ker}(\varphi)$, on peut appliquer la proposition I.24, d'où un homomorphisme induit $\overline{\varphi}: G/\mathrm{Ker}(\varphi) \to G'$ tel que $\overline{\varphi} \circ \pi = \varphi$.

Comme π est surjectif, on a $\mathsf{Im}(\varphi) = \mathsf{Im}(\overline{\varphi} \circ \pi) = \mathsf{Im}(\overline{\varphi})$; par conséquent, l'homomorphisme $\overline{\varphi}: \mathrm{Ker}(\varphi) \to \mathsf{Im}(\varphi)$ est surjectif. Finalement, considérons un élément $[g] \in \mathrm{Ker}(\overline{\varphi})$: on a $e_{G'} = \overline{\varphi}([g]) = \varphi(g)$, d'où $g \in \mathrm{Ker}(\varphi) = N$, ce qui implique $[g] = [e_G] = e_{G/N}$. Ainsi, le noyau de $\overline{\varphi}$ est trivial. Par la proposition I.3, cet homomorphisme est injectif, et donc bijectif. C'est bien un isomorphisme. □

22. Il en existe deux autres, qui sont des conséquences du premier, mais que nous ne verrons pas dans le cadre de ce cours.

Exemples (d'isomorphismes induits)**.** Reprenons la liste d'homomorphismes de la section I.3, et utilisons la connaissance de leur noyau et de leur image pour analyser les isomorphismes induits correspondants.

1. L'homomorphisme $\mathrm{id}_G : G \to G$ induit l'isomorphisme connu $G/\{e\} \simeq G$.
2. Similairement, pour H un sous-groupe d'un groupe G, l'inclusion $H \to G$ induit l'isomorphisme $H/\{e\} \simeq H$.
3. L'homomorphisme trivial $G \to G'$ induit l'isomorphisme connu $G/G \simeq \{e\}$.
4. Soit $g \in G$ un élément d'un groupe quelconque. L'homomorphisme $\varphi : \mathbb{Z} \to G$ donné par $\varphi(k) = g^k$ induit les isomorphismes suivants :

   $$\mathbb{Z} = \mathbb{Z}/\{0\} \simeq \mathsf{Im}(\varphi) = \langle g \rangle$$

   si $o(g) = \infty$, et

   $$\mathbb{Z}/n\mathbb{Z} \simeq \mathsf{Im}(\varphi) = \langle g \rangle$$

   si $o(g) = n$ est fini. Cela donne une preuve immédiate du théorème I.10 de classification des groupes cycliques.
5. L'homomorphisme $\mathbb{C}^* \to \mathbb{R}_+^*,\ z \mapsto |z|$ induit l'isomorphisme $\mathbb{C}^*/S^1 \simeq \mathbb{R}_+^*$.
6. L'homomorphisme $\det : \mathrm{GL}(n, K) \to K^*$ donné par le déterminant induit l'isomorphisme $\mathrm{GL}(n, K)/\mathrm{SL}(n, K) \simeq K^*$.
7. L'homomorphisme $\exp : (\mathbb{C}, +) \to (\mathbb{C}^*, \cdot)$ donné par $z \mapsto e^{2\pi i z}$ a image $\mathbb{C}^*$ et noyau $\mathbb{Z}$, d'où l'isomorphisme $\mathbb{C}/\mathbb{Z} \simeq \mathbb{C}^*$.
   De plus, sa restriction $\exp : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ a image S^1 et noyau $\mathbb{Z}$, d'où l'isomorphisme promis $\mathbb{R}/\mathbb{Z} \simeq S^1$.
8. La signature $\varepsilon : S_n \to \{-1, 1\}$ induit l'isomorphisme connu $S_n/A_n \simeq \{-1, 1\}$.

Venons-en maintenant à la dernière notion de ce chapitre, celle de *groupe simple*.

Définition I.9

Un groupe G non-trivial est dit **simple** si les seuls sous-groupes normaux dans G sont $N = \{e\}$ ou $N = G$.

Intuitivement, les groupes simples sont aux groupes ce que les particules élémentaires sont à la matière, dans le sens que tout groupe "peut être construit" à l'aide de groupes simples. En d'autres termes, si G n'est pas simple, il admet un sous-groupe normal propre $N \triangleleft G$, et "peut être décomposé" en les groupes G/N et N, deux groupes strictement plus petits que G.

Les groupes simples *abéliens* sont faciles à classifier.

Proposition I.26. *Soit G un groupe abélien. Alors, G est simple si et seulement si $G \simeq \mathbb{Z}/p\mathbb{Z}$ avec p premier.*

Démonstration. Supposons tout d'abord que G est un groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}$ avec p premier, et vérifions qu'il est simple. Soit donc $N \triangleleft G$ un sous-groupe normal (en fait, un sous-groupe quelconque puisque G est abélien). Par le corollaire I.5, l'ordre de N divise $|G| = |\mathbb{Z}/p\mathbb{Z}| = p$. Comme p est premier, on a $|N| = 1$ ou $|N| = p$, ce qui implique $N = \{e\}$ ou $N = G$. Le groupe G est donc simple.

Supposons réciproquement que G est un groupe abélien simple. Cela signifie que les seuls sous-groupes $H < G$ sont $H = \{e\}$ et $H = G$. Comme G n'est pas trivial, il existe $g \in G \setminus \{e\}$, qui engendre un sous-groupe $H = \langle g \rangle < G$ non-trivial, d'où $G = H = \langle g \rangle$. Ainsi, G est cyclique. Par le théorème I.10, on a donc $G \simeq \mathbb{Z}/n\mathbb{Z}$ avec $n \in \{0, 1, 2, \ldots\}$. Reste à montrer que n est premier.

Si $n = 0$, on obtient $G \simeq \mathbb{Z}$ qui n'est pas simple, puisqu'il admet le sous-groupe propre $H = 2\mathbb{Z}$. Si $n = 1$, on obtient G trivial, qui n'est pas simple par définition. Enfin, si $n \geq 2$ n'est pas premier, alors il existe $n_1, n_2 \geq 2$ tel que $n = n_1 n_2$; dans ce cas, le groupe $G = \langle g \rangle$ admet le sous-groupe propre $H = \langle g^{n_1} \rangle \triangleleft \langle g \rangle = G$, et n'est donc pas simple. On a donc nécessairement n premier, ce qui conclut la preuve. □

Pour les groupes simples non-abéliens c'est une autre paire de manches, comme on le verra en section I.9. Néanmoins, nous sommes en mesure de décrire une famille infinie de tels groupes, ce qui constitue le dernier théorème de ce chapitre.

Théorème I.27

Le groupe alterné A_n est simple pour tout $n \geq 5$.

Remarques.

1. Ce résultat fournit une nouvelle preuve de l'égalité $[A_n, A_n] = A_n$ pour $n \geq 5$ vue en section I.7 (et donc, du fait que S_n n'est pas résoluble pour $n \geq 5$).

   ⌜ En effet, le sous-groupe $N \coloneqq [A_n, A_n]$ est normal dans A_n. Comme A_n est simple, on a soit $N = \{e\}$, soit $N = A_n$. Mais le premier cas implique que A_n est abélien, ce qui n'est vrai que pour $n \leq 3$. ⌟

2. Notons que A_4 n'est pas simple, puisqu'il admet le sous-groupe normal propre $[A_4, A_4]$ d'ordre 4 (exercice 37). Par ailleurs, les groupes alternés A_1 et A_2 sont triviaux, et donc pas simples, tandis que $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est simple [23].

La preuve du théorème requière le lemme suivant.

Lemme I.28. *Pour $n \geq 5$, tous les 3-cycles sont conjugués dans A_n.*

23. Mais A_3 est membre d'une autre famille infinie de groupes simples, celle des groupes cycliques $\mathbb{Z}/p\mathbb{Z}$ de la proposition I.26.

Démonstration. Soit donc $(i,j,k) \in A_n$ un 3-cycle quelconque, avec $n \geq 5$. Nous cherchons $\sigma \in A_n$ tel que $\sigma(i,j,k)\sigma^{-1} = (1,2,3)$. Soit $\sigma \in S_n$ tel que $\sigma(i) = 1$, $\sigma(j) = 2$ et $\sigma(k) = 3$. Par le troisième point de la proposition I.17, on a

$$\sigma(i,j,k)\sigma^{-1} = (\sigma(i),\sigma(j),\sigma(k)) = (1,2,3)\,.$$

Si σ appartient à A_n, on a terminé. Dans le cas contraire, on pose $\sigma' = (4,5)\sigma$, ce qui est possible puisque $n \geq 5$. Comme σ est une permutation impaire, on a bien $\sigma' \in A_n$, qui satisfait

$$\sigma'(i,j,k)(\sigma')^{-1} = (4,5)\sigma(i,j,k)\sigma^{-1}(4,5) = (4,5)(1,2,3)(4,5) = (1,2,3)\,.$$

Ainsi, tous les 3-cycles sont conjugués dans A_n au 3-cycle $(1,2,3)$. Par transitivité de la relation "être conjugué", tous les 3-cycles sont conjugués dans A_n. □

Démonstration du théorème I.27. Soit donc $N \lhd A_n$ avec $n \geq 5$ et $N \neq \{\mathrm{id}\}$; il s'agit de montrer que N coïncide avec A_n tout entier. En fait, il suffit de vérifier que N contient un 3-cycle. En effet, si tel est le cas, le lemme I.28 (que l'on peut appliquer puisque $n \geq 5$) et le fait que N est normal dans A_n impliquent que N contient tous les 3-cycles. Comme A_n est engendré par les 3-cycles (c'est la proposition I.21), cela implique bien l'égalité $N = A_n$.

Il s'agit donc de montrer que $N \lhd A_n$ avec $n \geq 5$ et $N \neq \{\mathrm{id}\}$ contient forcément un 3-cycle. Pour ce faire, prenons un élément $x \in N \setminus \{\mathrm{id}\}$ (qui existe puisque N est non-trivial). Par le théorème I.18, la permutation x admet une décomposition

$$x = \sigma_1\sigma_2\cdots\sigma_s$$

en produit de cycles à supports disjoints, avec $s \geq 1$ puisque $x \neq \mathrm{id}$. Il y a 4 cas à considérer.

Supposons dans un premier temps qu'un des cycles $\sigma_1,\dots,\sigma_s$ est d'ordre > 3, disons $\sigma_1 = (i,j,k,\ell,\dots)$ sans restreindre la généralité. Posons $y \coloneqq (i,j,k) \in A_n$. Comme $x \in N \lhd A_n$ et $y \in A_n$, on a $yx^{-1}y^{-1} \in N$; comme N est un sous-groupe qui contient x, il contient également la composition $xyx^{-1}y^{-1}$. Calculons cette permutation en utilisant successivement les points (iii), (i) et (ii) de la proposition I.17 :

$$\begin{aligned} xyx^{-1}y^{-1} &= x(i,j,k)x^{-1}(k,j,i) = (x(i),x(j),x(k))(k,j,i) = (j,k,\ell)(k,j,i) \\ &= (\ell,j,k)(k,j,i) = (\ell,j)(j,k)(k,j)(j,i) = (\ell,j)(j,i) = (\ell,j,i)\,. \end{aligned}$$

Le sous-groupe N contient donc bien un 3-cycle, et ce cas est réglé[24].

Supposons dans un second temps que parmi les cycles $\sigma_1,\dots,\sigma_s$, il y a un 3-cycle, disons $\sigma_1 = (i,j,k)$, et une transposition ou un autre 3-cycle, disons σ_2 tel que $\sigma_2(\ell) = m$. Posons alors $z \coloneqq (i,j,\ell) \in A_n$. Exactement comme au cas précédent, le sous-groupe normal N contient $xzx^{-1}z^{-1}$, que l'on peut calculer explicitement via

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

24. Bien entendu, la deuxième ligne du calcul ci-dessus peut se faire plus directement, mais le résultat découle formellement des règles de calcul vues en proposition I.17.

Ainsi, le sous-groupe N contient un cycle d'ordre 5, et l'on se retrouve dans l'hypothèse du premier cas, déjà traité.

Supposons maintenant que les cycles $\sigma_1, \dots, \sigma_s$ consistent en exactement un cycle, qui est d'ordre 3. Alors, $x \in N$ lui-même est ce 3-cycle, et il n'y a rien à montrer.

Le dernier cas possible est celui où tous les cycles $\sigma, \dots, \sigma_s$ sont des transpositions. Comme x est non-trivial et pair, il y a au moins deux transpositions, disons $\sigma_1 = (i, j)$ et $\sigma_2 = (k, \ell)$. Posons alors $w := (i, k, m) \in A_n$ avec $m \notin \{i, j, k, \ell\}$, ce qui est possible puisque $n \geq 5$. Comme aux deux premiers cas, le sous-groupe normal N contient la permutation $xwx^{-1}w^{-1}$, et l'on calcule

$$xwx^{-1}w^{-1} = (x(i), x(k), x(m))(m, k, i) = (j, \ell, x(m))(m, k, i)\,.$$

Si $x(m) \neq m$, alors on a le produit de deux 3-cycles à supports disjoints, et l'on se retrouve dans l'hypothèse du second cas, déjà traité. Si $x(m) = m$, alors on obtient la permutation (j, ℓ, m, k, i), et l'on se retrouve dans l'hypothèse du premier cas, ce qui conclut la preuve. □

I.9 Classification des groupes finis

Nous concluons ce chapitre sur les groupes avec une dernière section moins formelle sur la classification des groupes finis. Cette discussion est proposée "pour votre culture", et ne fait pas partie du champ de l'examen.

Dans le cas des groupes abéliens finis, la classification est relativement aisée. En effet, on verra une preuve du résultat suivant [25] au chapitre III.

Théorème I.29: 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 de nombres premiers (pas forcément distincts), suite unique à l'ordre près, telle que

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

Remarques.

1. On verra au chapitre II que si m et n sont premiers entre eux, alors on a un isomorphisme $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$. C'est l'objet du *théorème chinois*, le théorème II.14.
2. Si l'on souhaite donner la liste des groupes abéliens d'ordre m fixé à isomorphisme près, il suffit 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 et $\nu_1, \dots, \nu_n \geq 1$.

25. Pour être précis, on verra en théorème III.15 une preuve de l'existence de la décomposition, mais pas de l'unicité.

Exemples.

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 corollaire I.7 et le théorème I.10, 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'on savait déjà par la note 19 de bas de page, sans l'hypothèse de commutativité).
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 la remarque 1 ci-dessus, on a $\mathbb{Z}/36\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, par exemple. Le groupe cyclique d'ordre 36 fait donc bien partie de cette liste, comme il se doit.

Si on laisse tomber l'hypothèse de commutativité, on change de monde, et cela devient incomparablement plus difficile. Néanmoins, la classification des "particules élémentaires" a été achevée relativement récemment, et constitue ce qu'on appelle communément le *théorème énorme*.

Théorème I.30: Classification des groupes finis simples

Tout groupe fini simple est de l'un des types suivants :

- cyclique d'ordre p premier [a],
- alterné de degré $n \geq 5$ [b],
- membre d'une des 16 familles de "groupes de type de Lie" [c],
- un des 27 "groupes sporadiques" [d].

a. Ce sont les groupes simples abéliens, comme on l'a vu en proposition I.26.
b. Voir théorème I.27.
c. Typiquement, ce sont des groupes de matrices sur un corps fini.
d. Le plus petit est d'ordre 7920, et le plus grand, le *groupe Monstre*, d'ordre $\sim 8 \cdot 10^{53}$.

Pour se rendre compte de l'énormité du théorème et de sa preuve, mentionnons que 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.

Exercices

1. Les ensembles et lois de composition $(G, \star)$ suivants forment-ils des groupes ?
   (a) $G = \mathbb{Z}$ avec $x \star y = x - y$.
   (b) $G = \{1, 2, \ldots\}$ avec $\star$ le produit usuel des entiers.
   (c) $G = \mathbb{R}$ avec $x \star y = (x^n + y^n)^{1/n}$, où n est un entier impair.
   (d) G l'ensemble des nombres rationnels avec dénominateur impair, avec $\star$ l'addition usuelle des rationnels.
   (e) $G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \middle| \, a \in \mathbb{R},\ b \in \mathbb{R}^* \right\}$ avec $\star$ la multiplication usuelle des matrices.

2. Pour tous éléments g, h, x d'un groupe G arbitraire, démontrer les "règles de calcul" suivantes :
   (i) Si $xg = xh$ ou $gx = hx$, alors $g = h$.
   (ii) $(g^{-1})^{-1} = g$ et $(gh)^{-1} = h^{-1}g^{-1}$.
   (iii) $g^n g^m = g^{n+m}$ et $(g^n)^m = g^{nm}$ pour tous $n, m \in \mathbb{Z}$.

3. Soit G un groupe quelconque.
   (i) Montrer que $(gh)^n = g^n h^n$ pour tous $g, h \in G$ et $n \in \mathbb{Z}$ si et seulement si G est abélien. Comment cette égalité s'écrit-elle en notation additive ?
   (ii) Montrer qu'en fait, $(gh)^2 = g^2 h^2$ pour tous $g, h \in G$ si et seulement si G est abélien.
   (iii) En déduire que si G est tel que $g^2 = e$ pour tout $g \in G$, alors G est abélien.

4. Soit G un groupe abélien fini, et $g_1, \ldots, g_n$ ses éléments. Montrer que le produit $g_1 \cdots g_n$ est un élément de G dont le carré est le neutre.

5. Soit X un ensemble quelconque. Montrer que l'ensemble $\mathscr{P}(X)$ des parties de X muni de la *différence symétrique*

$$A \Delta B := (A \cup B) \setminus (A \cap B)$$

   est un groupe abélien.

6. Soit G un ensemble muni d'une loi de composition associative satisfaisant les conditions suivantes :
   (i) Il existe $e \in G$ tel que $eg = g$ pour tout $g \in G$.
   (ii) Pour tout $g \in G$, il existe $g' \in G$ tel que $g'g = e$.
   Montrer qu'alors, G est un groupe.

7. Tenter d'appliquer l'exercice 6 à

$$G = \{ f : X \to X \mid f \text{ est injective} \},$$

   où X est un ensemble quelconque. Est-ce effectivement un groupe ?

8. Montrer à l'aide d'un exemple que la conclusion de l'exercice 6 est fausse si l'on remplace les conditions (i) et (ii) par :
   (i)' Il existe $e \in G$ tel que $eg = g$ pour tout $g \in G$.

(ii)' Pour tout $g \in G$, il existe $g' \in G$ tel que $gg' = e$.

9. Soient X un ensemble et $(G, \star)$ un groupe. Montrer que l'ensemble des applications $G^X = \{f : X \to G\}$ est un groupe pour la loi de composition définie par

$$(f \cdot g)(x) = f(x) \star g(x)$$

pour $f, g \in G^X$ et $x \in X$.

10. Soient $(G_1, \star)$ et $(G_2, \bullet)$ deux groupes. Montrer que le produit cartésien $G_1 \times G_2$ est un groupe pour la loi de composition définie par

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 \star h_1, g_2 \bullet h_2) \quad \text{pour } g_1, h_1 \in G_1 \text{ et } g_2, h_2 \in G_2\,.$$

11. Soient X un ensemble, $(G, \cdot)$ un groupe, et $f : X \to G$ une application bijective. Pour tout $x, y \in X$, on pose

$$x \star y = f^{-1}(f(x) \cdot f(y)).$$

Montrer que $(X, \star)$ est un groupe.

12. Vérifier que pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ des multiples de n forme un sous-groupe de $\mathbb{Z}$.

13. Déterminer le centre du groupe S_3 ainsi que le centralisateur de chacun de ses éléments.

14. (i) Démontrer que l'intersection de deux sous-groupes d'un groupe G est à nouveau un sous-groupe de G.
    (ii) Dans le cas de $G = \mathbb{Z}$, quel est le sous-groupe formé par l'intersection de $n\mathbb{Z}$ et de $m\mathbb{Z}$?
    (iii) L'union de deux sous-groupes est-elle aussi un sous-groupe ?

15. Déterminer l'ordre de tous les éléments des groupes suivants :

$$\mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/5\mathbb{Z}, \quad S_3\,.$$

16. Montrer que l'image d'un homomorphisme $\varphi : G \to G'$ est un sous-groupe de G', et qu'il coïncide avec G' si et seulement si φ est surjectif.

17. Soit G un groupe. Quand l'application $\varphi : G \to G$ donnée par $\varphi(g) = g^{-1}$ est-elle un homomorphisme ?

18. Montrer les énoncés suivants :
    (i) Si $\varphi : G \to G'$ est un isomorphisme, alors $o(g) = o(\varphi(g))$ pour tout $g \in G$.
    (ii) Si G et G' sont isomorphes, alors G contient exactement 45 éléments d'ordre 5 si et seulement si G' contient exactement 45 éléments d'ordre 5.

19. Vérifier que tous les groupes d'ordre 3 sont isomorphes.

20. À quel groupe (plus connu) le groupe défini en exercice 1 (c) est-il isomorphe ?

21. Le groupe $(X, \star)$ de l'exercice 11 est-il isomorphe à $(G, \cdot)$?

22. Montrer qu'une bijection $f: X \to Y$ entre deux ensembles définit un isomorphisme $\varphi: S(X) \to S(Y)$ par $\varphi(\sigma) = f \circ \sigma \circ f^{-1}$.

23. On l'a vu en exemple 6, l'exponentielle définit un isomorphisme entre $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \cdot)$. Existe-t-il un isomorphisme entre $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \cdot)$?

24. Soit $H \subset G$ un sous-ensemble non-vide d'un groupe. Montrer que les énoncés suivants sont équivalents.
    (i) H est un sous-groupe de G.
    (ii) $HH \subset H$ et $H^{-1} \subset H$.
    (iii) $HH^{-1} \subset H$.

25. (i) Montrer que toute classe modulo $\mathbb{Z}$ dans $\mathbb{R}$ possède un unique représentant x avec $0 \leq x < 1$.
    (ii) Montrer que toute classe modulo $\mathbb{R}_+^*$ dans $\mathbb{C}^*$ possède une unique représentant de module 1.

26. Déterminer les classes à gauche et à droite modulo $H = \langle (1,2) \rangle$ dans $G = S_3$, et vérifier le théorème de Lagrange dans ce cas.

27. Vérifier que tout sous-groupe d'un groupe cyclique est lui-même cyclique, de même que tout quotient d'un groupe cyclique.

28. Donner une preuve élémentaire des cas $n = 4, 5$ du théorème I.14 d'Euler.

29. En s'inspirant du cas de $\mathbb{Z}$ traité en cours, montrer que pour tout $n \geq 1$, le groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.

30. Identifier l'homomorphisme injectif $G \to S_n$ du théorème de Cayley (où $|G| = n$) pour les groupes suivants :
    (i) $G = \mathbb{Z}/n\mathbb{Z}$.
    (ii) $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
    (iii) $G = S_3$.

31. Déterminer la décomposition en cycles à supports disjoints de toutes les puissances du cycle $(1, 2, \ldots, 6) \in S_6$.

32. Déterminer l'ordre d'une permutation en fonction de sa décomposition en cycles à supports disjoints.

33. Deux éléments x, y d'un groupe G sont dits *conjugués* s'il existe $g \in G$ tel que $y = gxg^{-1}$.
    (i) Montrer que "être conjugués" définit une relation d'équivalence sur G (dont les classes d'équivalence sont appelées les *classes de conjugaison*).
    (ii) Déterminer les classes de conjugaison dans un groupe abélien.
    (iii) À l'aide de la proposition I.17 et du théorème I.18 du cours, déterminer les classes de conjugaison dans S_n.
    (iv) Quel est le nombre $p(n)$ de classes de conjugaison dans S_n pour $n = 1, 2, 3, 4, 5$.

34. Déterminer le groupe des automorphismes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ainsi que celui de S_3. Quelle conclusion peut-on en tirer ?

35. Calculer la signature de $(1,2)(3,4) \in S_4$ à partir de sa définition.

36. Montrer que S_n est engendré par $(1,2)$ et $(1,2,\ldots,n)$.

    Indication : Commencer par les transpositions de la forme $(i, i+1)$, puis toutes les transpositions.

37. Montrer que le sous-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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

38. Montrer les énoncés suivants.
    (i) Si $\varphi: G \to G'$ est un homomorphisme, alors $\varphi([G,G]) = [\varphi(G), \varphi(G)]$.
    (ii) Si G_1, G_2 sont deux groupes, alors $[G_1 \times G_2, G_1 \times G_2] = [G_1, G_1] \times [G_2, G_2]$.
    (iii) Pour tout groupe G, le sous-groupe $[G,G]$ est normal dans G.

39. Montrer que si N est un sous-groupe normal de S_n qui contient une transposition, alors $N = S_n$.

40. Démontrer que le sous-groupe $\mathrm{Int}(G)$ des automorphismes intérieurs est normal dans $\mathrm{Aut}(G)$.

41. 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 $\varphi: G \to A$ avec A abélien est trivial.
    (iii) Si $\varphi: G \to G'$ 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 un exemple (tiré du cours) d'une famille infinie de groupes parfaits.

42. (i) Vérifier que la relation "est un sous-groupe de" est une relation d'ordre sur l'ensemble des sous-groupes d'un groupe G fixé.
    (ii) Montrer que la relation "est un sous-groupe normal de" est une relation réflexive et antisymétrique sur l'ensemble des sous-groupes de G.
    (iii) Soient N_1 le sous-groupe de A_4 engendré par un élément d'ordre 2, et N_2 le sous-groupe de A_4 formé de tous les éléments d'ordre 2. Montrer que $N_1 \lhd N_2$ et $N_2 \lhd A_4$ mais que N_1 n'est pas normal dans A_4. En déduire que la relation $\lhd$ n'est pas une relation d'ordre.

43. Soit H un sous-groupe d'un groupe G. Montrer que le sous-ensemble

$$N(H) = \{g \in G \mid gHg^{-1} = H\}$$

    est un sous-groupe de G, qui contient H comme sous-groupe normal.

44. Montrer que si G est un groupe fini et H est le seul sous-groupe de G d'ordre $|H|$, alors H est normal dans G.

45. Soit $\varphi : G \to G'$ un homomorphisme de groupes. Montrer les énoncés suivants :
    (i) Si N' est un sous-groupe normal de G', alors $\varphi^{-1}(N')$ est normal dans G.
    (ii) Si φ est surjectif et N normal dans G, alors $\varphi(N)$ est normal dans G'.

46. On a vu que le sous-groupe dérivé $[G, G]$ est normal dans G.
    (i) Vérifier que le groupe quotient $G/[G, G]$ est abélien (c'est *l'abélianisé* de G).
    (ii) Quel est l'abélianisé d'un groupe abélien ? Quel est l'abélianisé de S_n ?

47. Soient $m, n \in \mathbb{Z}$ des entiers quelconques. À quelle condition sur m, n la projection canonique $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ passe-t-elle au quotient pour définir un homomorphisme $\overline{\varphi} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$?

48. Soit $\varphi : G \to G'$ un homomorphisme de noyau H. Montrer que si G est fini, alors
$$|G| = |\mathsf{Im}(\varphi)| \cdot |H| .$$

49. Soit $\mu(\mathbb{C})$ l'ensemble de toutes les racines de l'unité dans le plan complexe
$$\mu(\mathbb{C}) = \{z \in \mathbb{C} \mid z^n = 1 \text{ pour un } n \in \mathbb{Z}\} .$$
    (i) Vérifier que $\mu(\mathbb{C})$ est un sous-groupe de $\mathbb{C}^*$.
    (ii) Montrer que ce groupe est isomorphe à $\mathbb{Q}/\mathbb{Z}$.

50. Soit $H = 2\pi\mathbb{Z}$ le sous-groupe de $\mathbb{R}$ formé des multiples de 2π. Montrer que l'application $(r, \theta) \mapsto re^{i\theta}$ induit un isomorphisme $\mathbb{R}_+^* \times \mathbb{R}/H \simeq \mathbb{C}^*$.

Chapitre II: Anneaux

Dans le cours de LOGIQUE ET THÉORIE DES ENSEMBLES, vous avez vu les rudiments de *l'arithmétique sur* $\mathbb{Z}$, dont certains concepts ont également été repris en section I.5 :

- La notion de *divisibilité* : pour $a, b \in \mathbb{Z}$, on dit que a divise b dans $\mathbb{Z}$, noté $a \mid b$, s'il existe $q \in \mathbb{Z}$ tel que $aq = b$.
- La notion de *plus grand commun diviseur* de $a, b \in \mathbb{Z}$: $d = \operatorname{pgcd}(a, b) \geq 0$ satisfait $d \mid a$ et $d \mid b$, et si $c \in \mathbb{Z}$ est tel que $c \mid a$ et $c \mid b$, alors $c \mid d$.
- La *division euclidienne* : étant donnés $a, b \in \mathbb{Z}$ avec $b > 0$, il existe une unique paire $q, r \in \mathbb{Z}$ avec $a = bq + r$ et $0 \leq r < b$.
- La notion de *nombre premier* : un entier $p \geq 2$ est premier si, lorsque $p \mid ab$ avec $a, b \in \mathbb{Z}$, alors $p \mid a$ ou $p \mid b$.
- Le *théorème fondamental de l'arithmétique* : tout entier $n > 1$ s'écrit comme produit de nombres premiers de manière unique à l'ordre des facteurs près.

DAVID HILBERT (1862-1943)

Toutes ces notions se placent naturellement dans le cadre abstrait de la *théorie des anneaux*, que l'on peut donc voir comme une généralisation et une formalisation de l'arithmétique sur $\mathbb{Z}$. Ainsi, l'exemple prototypique d'anneau est donné par les entiers $\mathbb{Z}$, même si une multitude d'autres anneaux intéressants existent, comme $\mathbb{Z}[i], \mathbb{C}[X], \ldots$ On étudiera donc les anneaux dans ce chapitre II.

EMIL ARTIN (1898-1962)

D'autre part, certains anneaux bien particuliers, appelés *corps*, généralisent les ensembles de nombres $\mathbb{R}, \mathbb{C}$, et il est possible de développer la théorie de l'algèbre linéaire vue en ALGÈBRE I AUTOMNE sur un corps quelconque : ça sera l'objet du chapitre III.

II.1 Anneaux : axiomes et exemples

Voici la définition d'un anneau.

Définition II.1

Soit A un ensemble muni de deux lois de composition $A \times A \to A$ notées

$$(a, b) \longmapsto a + b \qquad \text{et} \qquad (a, b) \longmapsto a \cdot b\,.$$

On dit que A est un **anneau** s'il satisfait les axiomes suivants :

$(A1)$ $(A,+)$ est un groupe abélien.

$(A2)$ $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ pour tous $a,b,c\in A$.

$(A3)$ Il existe $1\in A$ tel que $1\cdot a=a\cdot 1=a$ pour tout $a\in A$.

$(A4)$ $(a+b)\cdot c=a\cdot c+b\cdot c$ et $c\cdot(a+b)=c\cdot a+c\cdot b$ pour tous $a,b,c\in A$.

Un anneau est dit **commutatif** si on a de plus $a\cdot b=b\cdot a$ pour tous $a,b\in A$.

Remarques et terminologie.

1. La loi notée + est appelée *l'addition*. Comme d'habitude, on notera $0=0_A$ le neutre et $-a$ l'inverse de a dans le groupe abélien $(A,+)$.

2. La loi $\cdot$ est appelée *la multiplication*. On notera souvent $a\cdot b=:ab$. Les axiomes $(A2)$ et $(A3)$ disent que $(A,\cdot)$ est un monoïde. Comme on l'a vu en section I.1, le neutre $1=1_A$ de $(A,\cdot)$ est nécessairement unique.

3. L'axiome $(A4)$ est un axiome de *distributivité*. Formellement, on aurait du écrire
$$(a+b)\cdot c=(a\cdot c)+(b\cdot c)\,,$$
pour ne pas confondre le côté droit avec $a\cdot(c+b)\cdot c$. Mais on applique la convention usuelle que "la multiplication l'emporte sur l'addition".

4. On a les règles de calcul suivantes, valides pour tous $a,b\in A$:
   (i) $a\cdot 0=0\cdot a=0$

   ⌜ Cela découle du calcul
   $$a\cdot 0\overset{(A1)}{=}a\cdot(0+0)\overset{(A4)}{=}a\cdot 0+a\cdot 0\overset{(A1)}{\Rightarrow}a\cdot 0=0\,,$$
   où dans la dernière implication, on utilise l'existence d'un inverse additif à $a\cdot 0$. La preuve de $0\cdot a=0$ est similaire. ⌟

   (ii) $a(-b)=(-a)b=-(ab)$

   ⌜ On calcule
   $$ab+a(-b)\overset{(A4)}{=}a\cdot(b-b)\overset{(A1)}{=}a\cdot 0\overset{(i)}{=}0\overset{(A1)}{\Rightarrow}a(-b)=-(ab)\,,$$
   et similairement pour $(-a)b=-(ab)$. ⌟

   (iii) $(-a)(-b)=ab$

   ⌜ En appliquant le point (ii) deux fois, on obtient
   $$(-a)(-b)\overset{(ii)}{=}-(a(-b))\overset{(ii)}{=}-(-(ab))\overset{(A1)}{=}ab\,,$$
   où au dernier pas, on a utilisé l'identité $-(-x)=x$ valide pour tout élément x d'un groupe abélien. ⌟

   En remplaçant (a,b) par $(1,-a)$ ou $(-a,1)$ dans (iii), on trouve :

(iv) $(-1)a = -a = a(-1)$.

Finalement, en posant $a = -1$ dans cette égalité, on obtient :

(v) $(-1)(-1) = 1$.

5. Comme $(A, +)$ est un groupe, on a bien-sûr également la règle de calcul suivante : si $a + b = a + c$, alors $b = c$.
   En revanche, on n'a en général *pas* l'implication $ab = ac \Rightarrow b = c$. Par exemple, on a $0 \cdot b = 0 \cdot c = 0$ pour tous $b, c \in A$ par le point (i) [1].

6. L'ensemble $A = \{0\}$ est un anneau, appelé *l'anneau nul*, et noté $A = 0$.
   Remarquons que A est l'anneau nul si et seulement si $0 = 1 \in A$.

   ⌜ Si $A = \{0\}$, alors on a forcément $1 = 0$. Réciproquement, si $1 = 0 \in A$, alors tout $a \in A$ est égal à $a \overset{(A3)}{=} a \cdot 1 = a \cdot 0 \overset{(i)}{=} 0$. ⌟

7. Pour $n \in \mathbb{Z}$ et $a \in A$, on note comme d'habitude

$$n \cdot a = \begin{cases} a + \cdots + a \quad (n \text{ fois}) & \text{si } n > 0, \\ 0 & \text{si } n = 0, \\ (-a) + \cdots + (-a) \quad (|n| \text{ fois}) & \text{si } n < 0. \end{cases}$$

   Par les règles de calcul vues en section I.1, on a

$$(n + m) \cdot a = n \cdot a + m \cdot a, \quad (nm) \cdot a = n \cdot (m \cdot a), \quad n \cdot (a + b) = n \cdot a + n \cdot b$$

   pour tous $n, m \in \mathbb{Z}$ et $a, b \in A$.
   De plus, l'axiome de distributivité implique les égalités

$$n \cdot (ab) = (n \cdot a)b = a(n \cdot b)$$

   pour tous $n \in \mathbb{Z}$ et $a, b \in A$.

   ⌜ Cela découle du point (i) pour $n = 0$. Pour $n > 0$, on a

$$n \cdot (ab) = \overbrace{ab + \cdots + ab}^{n} \overset{(A4)}{=} a(\overbrace{b + \cdots + b}^{n}) = a(n \cdot b),$$

   et similairement pour les autres cas. ⌟

Voici enfin une liste d'exemples.

Exemples (d'anneaux)**.**

1. L'ensemble $A = \mathbb{Z}$ muni de l'addition et de la multiplication standards est un anneau commutatif, de même que $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.

1. Comme on le verra, c'est le seul contre-exemple dans un anneau intègre.

2. Pour $K = \mathbb{R}$ ou $\mathbb{C}$ et $n \geq 1$, l'ensemble $A = \mathscr{M}_n(K)$ des matrices carrées de taille n à coefficients dans K est un anneau pour l'addition et de la multiplication matricielles. Cela découle de résultats vus en algèbre linéaire.
Pour $n = 1$, l'anneau $\mathscr{M}_1(K) = K$ est commutatif.
Pour $n \geq 2$, l'anneau $\mathscr{M}_n(K)$ n'est pas commutatif.

3. Considérons l'ensemble $A = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ est continue}\}$ muni des lois suivantes : pour $f, g \in A$ et $x \in \mathbb{R}$, on définit
$$(f+g)(x) = f(x) + g(x) \quad \text{et} \quad (f \cdot g)(x) = f(x)g(x)\,.$$
C'est un anneau : cela découle de résultats vus en analyse, par exemple le fait que le produits et la somme de deux fonctions continues est également continue. Notons que le neutre additif 0_A est la fonction identiquement nulle, tandis que le neutre multiplicatif 1_A est la fonction identiquement égale à 1.
Il en va de même pour l'ensemble $B = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ est dérivable}\} \subset A$.

4. Soient $(G, +)$ un groupe abélien, et $\mathrm{End}(G)$ l'ensemble des *endomorphismes* de G, c'est-à-dire des homomorphismes de groupes $\varphi : G \to G$. Comme on le verra en exercice 3, c'est un anneau pour l'addition et la multiplication suivantes :
$$(\varphi + \psi)(g) = \varphi(g) + \psi(g) \quad \text{et} \quad (\varphi \cdot \psi)(g) = \varphi(\psi(g))$$
pour tous $\varphi, \psi \in \mathrm{End}(G)$ et $g \in G$.

5. Pour tout $n \geq 1$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif pour les lois héritées de $\mathbb{Z}$, à savoir
$$[a] + [b] \coloneqq [a+b] \quad \text{et} \quad [a] \cdot [b] = [ab]$$
pour tous $a, b \in \mathbb{Z}$.

⌜ Le fait que l'addition est bien définie et fait de $(\mathbb{Z}/n\mathbb{Z}, +)$ un groupe abélien a été montré en exemple 7 de la section I.1. De même, le fait que la multiplication est bien définie et satisfait les axiomes $(A2)$, $(A3)$ ainsi que la commutativité a été vu dans la preuve de la proposition I.13. Finalement, la distributivité dans $\mathbb{Z}/n\mathbb{Z}$ découle directement de la distributivité dans $\mathbb{Z}$, via
$$([a] + [b])[c] = [a+b][c] = [(a+b)c] = [ac + bc] = [ac] + [bc] = [a][c] + [b][c]$$
pour tous $a, b, c \in \mathbb{Z}$, et similairement pour $[c]([a] + [b]) = [c][a] + [c][b]$. ⌟

6. Soient A_1, A_2 deux anneaux. Alors, le produit cartésien $A_1 \times A_2$ est muni d'une structure d'anneau via
$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \quad \text{et} \quad (a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2)$$
pour tout $a_1, b_1 \in A_1$ et $a_2, b_2 \in A_2$. C'est le sujet de l'exercice 1.
On parle de *l'anneau produit*.

7. Pour tout anneau A et ensemble X, on vérifie que l'ensemble

$$A^X \coloneqq \{f\colon X \to A\}$$

est un anneau pour les lois

$$(f+g)(x) = f(x) + g(x) \quad \text{et} \quad (f \cdot g)(x) = f(x)g(x)$$

pour $f, g \in A^X$ et $x \in X$.

Terminologie. Soit A un anneau.

- Un *sous-anneau* B de A est un sous-ensemble $B \subset A$ qui contient 1_A, et tel que

$$a, b \in B \Rightarrow -a, a+b, a \cdot b \in B\,.$$

Notons que $(B, +)$ est un sous-groupe de $(A, +)$, et que B est un anneau pour la restriction des lois de A à B.

- Un élément $a \in A \smallsetminus \{0\}$ est un *diviseur de zéro* s'il existe $b \in A \smallsetminus \{0\}$ tel que $ab = 0$ ou $ba = 0$.

- L'anneau A est *intègre* si A est non-nul, commutatif, et sans diviseur de zéro. Cette dernière condition est équivalente à l'implication suivante : pour tous $a, b \in A$,

$$ab = 0 \quad \Rightarrow \quad a = 0 \ \text{ ou } \ b = 0\,.$$

Notons que dans un anneau intègre, on a la règle de calcul suivante : pour tous $a, b, c \in A$,

$$ab = ac,\ a \neq 0 \quad \Rightarrow \quad b = c\,.$$

⌜ Supposons donc $a, b, c \in A$ avec $ab = ac$ et $a \neq 0$. On a alors

$$0 = ab - ac \overset{(A4)}{=} a(b-c) \overset{A \text{ int.}}{\Rightarrow} a = 0 \ \text{ ou } \ b - c = 0 \overset{a \neq 0}{\Rightarrow} b - c = 0\,,$$

ce qui est équivalent à $b = c$. ⌟

- On note

$$A^* = \{a \in A \,|\, \text{il existe } a' \in A \text{ tel que } aa' = a'a = 1\}$$

l'ensemble des *unités* de A. L'inverse multiplicatif de $a \in A^*$ est habituellement noté a^{-1}. Par définition, $(A^*, \cdot)$ est un groupe ; en particulier, l'inverse multiplicatif de $a \in A^*$ est unique.

⌜ Si $a, b \in A^*$ admettent les inverses multiplicatifs a^{-1} et b^{-1}, respectivement, alors ab admet l'inverse $b^{-1}a^{-1}$; on a donc bien $ab \in A^*$. La vérification des axiomes de groupe est immédiate. ⌟

De plus, si A est non-nul, alors on a $A^* \subset A \smallsetminus \{0\}$.

⌜ Comme $0 \cdot b \overset{(i)}{=} 0 \overset{A \neq 0}{\neq} 1$ pour tout $b \in A$, le neutre additif 0 n'est pas une unité. ⌟

Définition II.2

Un **corps** est un anneau commutatif non nul K tel que $K^* = K \setminus \{0\}$.

Remarques.

1. Ainsi, un corps est un anneau commutatif non-nul tel que pour tout $a \in K$ avec $a \neq 0$, il existe $a^{-1} \in K$ tel que $a^{-1}a = 1$.
2. Un corps est un anneau intègre.

   ⌜ Par définition, un corps K est un anneau commutatif non-nul. Reste donc à voir qu'il n'a pas de diviseur de zéro. Soient $a, b \in K$ avec $ab = 0$ et $a \neq 0$. Par définition, l'élément $a \neq 0$ admet un inverse a^{-1}, d'où

   $$b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0\,.$$

   On a donc bien $b = 0$. ⌟

Étudions ces notions en reprenant notre liste d'exemples d'anneaux.

Exemples.

1. Les ensembles de nombres $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ forment une suite de sous-anneaux intègres.
   Le groupe des unités de $\mathbb{Z}$ est $\mathbb{Z}^* = \{-1, 1\}$. Ainsi, l'anneau $\mathbb{Z}$ est un anneau intègre qui n'est *pas* un corps.
   D'autre part, on a $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ et $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, ce qui justifie la notation, et montre que $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

2. Pour $K = \mathbb{R}$ ou $\mathbb{C}$ et $n \geq 1$ fixé, considérons l'anneau $A = \mathscr{M}_n(K)$.
   Pour $n = 1$, l'anneau $A = \mathscr{M}_1(K) = K$ est un corps.
   Pour $n \geq 2$, l'anneau A n'est pas commutatif, et a des diviseurs de zéro : par exemple, les matrices $a = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \neq 0$ et $b = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \neq 0$ satisfont $ab = 0 \in A$.
   Le groupe des unités de A n'est autre que

   $$\mathscr{M}_n(K)^* = \{M \in \mathscr{M}_n(K) \,|\, \exists N \in \mathscr{M}_n(K) \text{ t.q. } MN = NM = I\} = \mathrm{GL}(n, K)\,,$$

   le groupe général linéaire de degré n de K.

3. L'anneau $B = \{f : \mathbb{R} \to \mathbb{R} \,|\, f \text{ est dérivable}\}$ est un sous-anneau de $A = \{f : \mathbb{R} \to \mathbb{R} \,|\, f \text{ est continue}\}$, puisque toute fonction dérivable est continue [2].
   Ces deux anneaux ne sont pas intègres : par exemple, on a $fg = 0_A$ pour les fonctions $f \neq 0_A$ et $g \neq 0_A$ données par les graphes ci-dessous.

2. De plus, l'anneau A est un sous-anneau de $\mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}\}$.

De plus, on a

$$\begin{aligned} A^* &= \{f\colon \mathbb{R} \to \mathbb{R} \,|\, f \text{ est continue et il existe } g\colon \mathbb{R} \to \mathbb{R} \text{ avec } fg = 1_A\} \\ &= \{f\colon \mathbb{R} \to \mathbb{R}^* \,|\, f \text{ est continue}\}\,, \end{aligned}$$

puisque toute fonction $f\colon \mathbb{R} \to \mathbb{R}$ avec $f(x) \neq 0$ pour tout $x \in \mathbb{R}$ satisfait que $\frac{1}{f}$ est continue. Similairement, on a $B^* = \{f\colon \mathbb{R} \to \mathbb{R}^* \,|\, f \text{ est dérivable}\}$.

4. Étant donné un groupe abélien $(G, +)$ quelconque, l'anneau $A = \mathrm{End}(G)$ peut avoir des diviseurs de zéros (exercice 3). De plus, le groupe des unités n'est autre que $\mathrm{End}(G)^* = \mathrm{Aut}(G)$, le groupe des automorphismes de G.

5. Venons-en à l'exemple fondamental de $A = \mathbb{Z}/n\mathbb{Z}$ avec $n \geq 2$, qui est un anneau commutatif non-nul. Montrons tout d'abord que son groupe des unités n'est autre que

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z} \,|\, \mathrm{pgcd}(a, n) = 1\}\,,$$

ce qui justifie la notation employée en section I.5.

⌜ Par définition du groupe des unités, on a

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z} \,|\, \text{il existe } [b] \in \mathbb{Z}/n\mathbb{Z} \text{ tel que } [a][b] = [1] \in \mathbb{Z}/n\mathbb{Z}\}\,.$$

Or, cette dernière égalité est équivalente à l'existence de $k \in \mathbb{Z}$ tels que $ab + kn = 1$, ce qui par le théorème de Bézout est équivalent à $\mathrm{pgcd}(a, n) = 1$. ⌟

Quand l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il intègre ? Nous allons montrer que les trois conditions suivantes sont équivalentes :

(i) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre.

(ii) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.

(iii) L'entier n est premier.

⌜ Pour vérifier cela, nous allons montrer les implications (iii) ⇒ (ii) ⇒ (i) ⇒ (iii). Pour commencer, supposons donc $n = p$ premier, et vérifions que $\mathbb{Z}/p\mathbb{Z}$ est un corps. Par l'égalité ci-dessus, on a

$$(\mathbb{Z}/p\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z} \,|\, \mathrm{pgcd}(a, p) = 1\} = \{[1], [2], \ldots, [p-1]\} = \mathbb{Z}/p\mathbb{Z} \smallsetminus \{[0]\}\,,$$

ce qui montre que $\mathbb{Z}/p\mathbb{Z}$ est bien un corps. Comme un corps est toujours intègre, la seconde implication est triviale. Venons-en donc à la troisième, que l'on montre par la contraposée : supposons n pas premier, et tentons de trouver des diviseurs de zéro pour montrer que $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. Comme $n \geq 2$ n'est pas premier,

il existe des entiers $1 < r, s < n$ tels que $rs = n$; considérons leurs classes $a = [r]$ et $b = [s]$ dans $\mathbb{Z}/n\mathbb{Z}$. Ce sont des diviseurs de zéro puisque $a \neq 0$ et $b \neq 0$ mais

$$ab = [r][s] = [rs] = [n] = [0] \in \mathbb{Z}/n\mathbb{Z}\,.$$

Cela conclut la preuve de l'équivalence de ces trois conditions. ⌟

Ainsi, pour tout nombre premier p, on a un corps $\mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z}$ d'ordre p. En particulier, on retrouve le corps $\mathbb{F}_2 = \{0, 1\}$ vu en LOGIQUE ET THÉORIE DES ENSEMBLES.

6. Si A_1 et A_2 sont deux anneaux non-nuls , alors l'anneau produit $A_1 \times A_2$ n'est pas intègre, et on a $(A_1 \times A_2)^* = A_1^* \times A_2^*$. C'est le second point de l'exercice 1.

7. Si X un ensemble de cardinalité $|X| > 1$ et A un anneau quelconque, alors l'anneau $A^X = \{f : X \to A\}$ n'est pas intègre.

   ⌜ Si $A = 0$, alors A^X est également l'anneau nul, et n'est ainsi pas intègre ; supposons donc A non-nul. Comme $|X| > 1$, il existe deux éléments différents $x_1 \neq x_2 \in X$. Soient $f_1, f_2 : X \to A$ définis par $f_1(x) = 1$ si $x = x_1$ et $f_1(x) = 0$ sinon, et similairement pour f_2 avec x_2. Comme A est non-nul, on a $f_1 \neq 0$ et $f_2 \neq 0$; néanmoins, comme $x_1 \neq x_2$, on a $(f_1 \cdot f_2)(x) = f_1(x)f_2(x) = 0$ pour tout $x \in X$, i.e. $f_1 \cdot f_2 = 0$. Ainsi, l'anneau A^X admet des diviseurs de zéro, et n'est donc pas intègre. ⌟

   Finalement, on vérifie facilement que $\left(A^X\right)^* = (A^*)^X$.

Remarque. On montrera en exercice 6 qu'un anneau intègre fini est un corps, ce qui fournit une preuve alternative de (i)⇒(ii) dans l'exemple 5 ci-dessus. C'est bien entendu faux en général, puisque l'anneau intègre $\mathbb{Z}$ n'est pas un corps.

Ces notions sont tout à fait élémentaires mais étonnamment, elles permettent déjà de démontrer un résultat non-trivial de théorie des nombre. Pour l'énoncer, calculons la classe modulo n de $(n-1)!$ pour les premières valeurs de $n \geq 2$.

n	2	3	4	5	6	7	8	9	10	11
$(n-1)!$	1	2	6	24	120	720	5040	40320	362880	3628800
$(n-1)! \bmod n$	1	2	2	4	0	6	0	0	0	10

JOHN WILSON (1741-1793)

Théorème II.1: Théorème de Wilson

Un nombre entier $n \geq 2$ est premier si et seulement si $(n-1)! \equiv -1 \pmod{n}$.

Démonstration. Supposons pour commencer que $n \geq 2$ satisfait $(n-1)! \equiv -1 \pmod{n}$, et tentons de vérifier que n est premier. Pour ce faire, considérons

un diviseur d de n avec $1 \leq d < n$, et montrons que $d = 1$. Par hypothèse, on a $(n-1)! + 1 \equiv 0 \pmod{n}$, ce qui signifie que n divise $(n-1)! + 1$. Comme d divise n, on obtient que d divise $(n-1)!+1$. Par ailleurs, les inégalités $1 \leq d \leq n-1$ impliquent que d divise également $(n-1)!$. Par conséquent, l'entier d divise aussi la différence entre ces deux nombres, à savoir $(n-1)! + 1 - (n-1)! = 1$, ce qui n'est possible que si $d = 1$ [3].

Supposons à présent $n = p$ premier. Comme la relation $(n-1)! \equiv -1 \pmod{n}$ est trivialement satisfaite pour $p = 2$, on peut supposer $p > 2$. Il s'agit donc de calculer

$$[(p-1)!] = [1][2]\cdots[p-1] \in \mathbb{Z}/p\mathbb{Z}\,,$$

et de montrer que le résultat est $[-1]$. Comme p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps (voir exemple 5). Ainsi, le produit ci-dessus est en fait la multiplication de tous les éléments du groupe des unités $(\mathbb{Z}/p\mathbb{Z})^* = \{[1], [2], \ldots, [p-1]\}$. Comme il s'agit d'un groupe, chaque $a \in (\mathbb{Z}/p\mathbb{Z})^*$ admet un inverse $a^{-1} \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $aa^{-1} = 1$. Par conséquent, dans le produit ci-dessus, chaque $a \in (\mathbb{Z}/p\mathbb{Z})^*$ se simplifie avec son inverse, sauf les éléments a tels que $a = a^{-1}$. On a donc

$$[(p-1)!] = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^*} a = \prod_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^* \\ a = a^{-1}}} a\,.$$

Quels sont les éléments $a \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $a = a^{-1}$? Cette équation est équivalente à $a^2 = 1$ dans le groupe $(\mathbb{Z}/p\mathbb{Z})^*$, ou à $a^2 - 1 = 0$ dans l'anneau $\mathbb{Z}/p\mathbb{Z}$, qui se factorise en $(a-1)(a+1) = 0$. Comme $\mathbb{Z}/p\mathbb{Z}$ est intègre (puisque p est premier), on a nécessairement $a - 1 = 0$ ou $a + 1 = 0$, donc $a = 1$ ou $a = -1$. En conclusion, les éléments $a \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $a = a^{-1}$ sont $a = 1$ et $a = -1$, qui sont distincts puisque $p > 2$. Le produit ci-dessus est donc égal à

$$[(p-1)!] = \prod_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^* \\ a = a^{-1}}} a = 1(-1) = -1 \in \mathbb{Z}/p\mathbb{Z}\,,$$

ce qui conclut la preuve. □

II.2 Homomorphismes d'anneaux

Définition II.3

Une application $\varphi : A \to A'$ entre deux anneaux est appelée un **homomorphisme d'anneaux** si elle satisfait

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{et} \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

pour tous $a, b \in A$, ainsi que $\varphi(1_A) = 1_{A'}$.

3. On montrera en exercice 7 qu'en fait, si $n > 4$ n'est pas premier, alors $(n-1)! \equiv 0 \pmod{n}$, comme la table ci-dessus le laissait présager.

Remarques et terminologie.

1. La première condition signifie que $\varphi\colon (A,+) \to (A',+)$ est un homomorphisme de groupes. Comme on l'a vu en section I.3, cela implique les égalités $\varphi(0_A) = 0_{A'}$ et $\varphi(-a) = -\varphi(a)$ pour tout $a \in A$.

2. La seconde condition signifie que φ préserve la multiplication [4].

   Les deux premières conditions n'impliquent en général *pas* la troisième (voir néanmoins l'exercice 11). Par exemple, l'application identiquement nulle $\varphi\colon A \to A'$ donnée par $\varphi(a) = 0_{A'}$ pour tout $a \in A$ satisfait trivialement les deux premières conditions, mais pas la troisième si $A' \neq 0$ puisque $\varphi(1_A) = 0_{A'} \neq 1_{A'}$. Un exemple moins trivial est donné en exercice 9.

3. La restriction d'un homomorphisme d'anneaux $\varphi\colon A \to A'$ aux unités de A définit un homomorphisme de groupes $\varphi|_{A^*}\colon (A^*,\cdot) \to ((A')^*,\cdot)$.

   ⌜ En effet, pour tout $a \in A^*$, il existe $b \in A$ tel que $ab = ba = 1_A$, d'où

   $$1_{A'} = \varphi(1_A) = \varphi(ab) = \varphi(a)\varphi(b) \quad \text{et} \quad 1_{A'} = \varphi(1_A) = \varphi(ba) = \varphi(b)\varphi(a)\,.$$

   Ainsi, on a bien $\varphi(a) \in (A')^*$ d'inverse $\varphi(b)$. Le fait que c'est un homomorphisme de groupe est assuré par la seconde condition. ⌟

4. On vérifie facilement que la composition de deux homomorphismes d'anneaux est encore un homomorphisme d'anneaux.

5. Naturellement, on définit le *noyau* et *l'image* de $\varphi\colon A \to A'$ via

   $$\mathrm{Ker}(\varphi) \coloneqq \{a \in A \,|\, \varphi(A) = 0_{A'}\} \quad \text{et} \quad \mathsf{Im}(\varphi) \coloneqq \varphi(A) = \{\varphi(a) \in A' \,|\, a \in A\}\,.$$

   Par la proposition I.3, le noyau $\mathrm{Ker}(\varphi)$ est un sous-groupe de $(A,+)$, qui est trivial si et seulement si φ est injectif, tandis que $\mathsf{Im}(\varphi)$ est un sous-groupe de $(A',+)$.
   En fait, il s'avère que $\mathsf{Im}(\varphi)$ est un sous-anneau de A'.

   ⌜ On a déjà $\mathsf{Im}(\varphi) < (A',+)$, et donc les implications $a', b' \in \mathsf{Im}(\varphi) \Rightarrow -a', a'+b' \in \mathsf{Im}(\varphi)$. De plus, on a bien $1_{A'} = \varphi(1_A) \in \mathsf{Im}(\varphi)$. Finalement, tous $a', b' \in \mathsf{Im}(\varphi)$ sont de la forme $a' = \varphi(a)$ et $b' = \varphi(b)$, d'où $a'b' = \varphi(a)\varphi(b) = \varphi(ab) \in \mathsf{Im}(\varphi)$. ⌟

   En revanche, le noyau $\mathrm{Ker}(\varphi)$ n'est jamais un sous-anneau de A si A' est non-nul, puisqu'il ne contient pas 1_A. On reviendra sur la nature exacte du noyau en section II.3.

6. Un *isomorphisme d'anneaux* est un homomorphisme d'anneaux $\varphi\colon A \to A'$ tel qu'il existe un homomorphisme d'anneaux $\psi\colon A' \to A$ avec $\varphi \circ \psi = \mathrm{id}_{A'}$ et $\psi \circ \varphi = \mathrm{id}_A$. S'il existe un tel isomorphisme, on dit que A et A' sont *isomorphes*, ce qui est noté $A \simeq A'$.

4. En termes techniques, c'est un homomorphisme de monoïdes $\varphi\colon (A,\cdot) \to (A',\cdot)$.

Comme en section I.3, on vérifie qu'un homomorphisme d'anneaux est un isomorphisme si et seulement s'il est bijectif. En d'autres termes, l'inverse d'un homomorphisme d'anneaux est toujours un homomorphisme d'anneaux.

Par la remarque 3 ci-dessus, un isomorphisme d'anneaux $\varphi: A \to A'$ définit un isomorphisme de groupes $\varphi|_{A^*}: (A^*, \cdot) \to ((A')^*, \cdot)$.

Toutes les remarques de la section I.3 sur les isomorphismes de groupes se transposent *verbatim* aux isomorphismes d'anneaux.

Exemples (d'homomorphismes d'anneaux)**.**

1. Pour tout anneau A, l'identité $\mathrm{id}_A: A \to A$ est un homomorphisme d'anneaux, qui est un isomorphisme.
2. Si $B \subset A$ est un sous-anneau, alors l'inclusion $i: B \to A$ est un homomorphisme d'anneaux injectif d'image B. En particulier, les inclusions
$$\mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{R} \longrightarrow \mathbb{C}$$
sont des homomorphismes d'anneaux.
3. Pour $A = \{f: \mathbb{R} \to \mathbb{R} \mid f \text{ continue}\}$ et $x_0 \in \mathbb{R}$ fixé, l'application d'évaluation en x_0 donnée par $\varphi: A \to \mathbb{R}$, $f \mapsto f(x_0)$ est un homomorphisme d'anneaux.

   ⌜ En effet, pour tous $f, g \in A$, on a par définition
   $$\varphi(f+g) = (f+g)(x_0) = f(x_0) + g(x_0) = \varphi(f) + \varphi(g)\,,$$
   $$\varphi(f \cdot g) = (f \cdot g)(x_0) = f(x_0)g(x_0) = \varphi(f)\varphi(g)\,,$$
   et $\varphi(1_A) = 1_A(x_0) = 1$ puisque la fonction 1_A est identiquement égale à $1 \in \mathbb{R}$. ⌟
4. Pour $A = \mathscr{M}_n(K)$ avec $n \geq 1$ et $K = \mathbb{R}$ ou $\mathbb{C}$, et $P \in \mathrm{GL}(n, K)$ fixé, l'application $\varphi: A \to A$ donnée par $\varphi(M) = PMP^{-1}$ est un isomorphisme d'anneaux. (On parle d'*automorphisme d'anneaux.*) C'est l'exercice 10.
5. Pour tout $n \geq 1$, la projection canonique $\pi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto [a]$ est un homomorphisme d'anneaux surjectif de noyau $n\mathbb{Z}$. Cela découle directement des définitions.

Proposition II.2. *Pour tout anneau A, il existe un unique homomorphisme d'anneaux $\mathbb{Z} \to A$.*

Démonstration. Soit donc $\varphi: \mathbb{Z} \to A$ un homomorphisme d'anneaux. Pour tout $n > 0$, on a
$$\varphi(n) = \varphi(\overbrace{1 + \cdots + 1}^{n}) = \overbrace{\varphi(1) + \cdots + \varphi(1)}^{n} = \overbrace{1_A + \cdots + 1_A}^{n} = n \cdot 1_A\,,$$

ou la dernière égalité n'est que la notation additive de $n^{\text{ième}}$ puissance de 1_A. Pour tout $n < 0$, on a similairement

$$\varphi(n) = \varphi(\overbrace{(-1) + \cdots + (-1)}^{|n|}) = \overbrace{\varphi(-1) + \cdots + \varphi(-1)}^{|n|} = \overbrace{(-1_A) + \cdots + (-1_A)}^{|n|} = n \cdot 1_A.$$

Finalement, on a également $\varphi(0) = 0_A = 0 \cdot 1_A$. En conclusion, tout homomorphisme d'anneaux $\varphi\colon \mathbb{Z} \to A$ est donné par $\varphi(n) = n \cdot 1_A$. Il y a donc au plus un homomorphisme d'anneaux $\mathbb{Z} \to A$.

Reste à vérifier que l'application $\varphi\colon \mathbb{Z} \to A$ donné par $\varphi(n) = n \cdot 1_A$ est bien un tel homomorphisme. Cela repose sur la remarque 6 de la section II.1 au sujet des règles de calcul pour $n \cdot a$ avec $n \in \mathbb{Z}$ et $a \in A$. En effet, pour tous $n, m \in \mathbb{Z}$, on a

$$\varphi(n+m) = (n+m) \cdot 1_A = n \cdot 1_A + m \cdot 1_A = \varphi(n) + \varphi(m)$$

et

$$\varphi(nm) = (nm) \cdot 1_A = n \cdot (m \cdot 1_A) = n \cdot \varphi(m) = n \cdot (1_A \varphi(m)) = (n \cdot 1_A)\varphi(m) = \varphi(n)\varphi(m)\,.$$

Finalement, on a $\varphi(1) = 1 \cdot 1_A = 1_A$ par définition, ce qui conclut la preuve. □

Ainsi, pour tout anneau A, il existe un unique homomorphisme d'anneaux de $\mathbb{Z}$ dans A, que l'on note $\epsilon\colon \mathbb{Z} \to A$. Cela définit donc un sous-groupe $\mathrm{Ker}(\epsilon)$ qui est un sous-groupe de $\mathbb{Z}$. Par la proposition I.9, il existe un unique entier $n \geq 0$ tel que $\mathrm{Ker}(\epsilon) = n\mathbb{Z}$.

Terminologie. Cet entier n est appelé la *caractéristique* de A, noté $\mathrm{car}(A)$.

Remarque. De manière plus concrète, on a :

- Si $\mathrm{car}(A) = 0$, alors $n \cdot 1_A \neq 0_A$ pour tout $n > 0$.
- Si $\mathrm{car}(A)$ est positif, alors c'est le plus petit entier $n > 0$ tel que $n \cdot 1_A = 0_A$.

⌜ On a $\mathrm{car}(A) = 0$ si et seulement si $\mathrm{Ker}(\epsilon) = \{0\}$, ce qui est équivalent à $n \cdot 1_A \neq 0_A$ pour tout $n \neq 0$. (Notons que c'est également équivalent à $\epsilon\colon \mathbb{Z} \to A$ injectif, ce qui implique que A admet le sous-anneau $\epsilon(\mathbb{Z}) \subset A$ isomorphe à $\mathbb{Z}$.)

Supposons à présent $\mathrm{car}(A)$ positif. Si n est un entier positif tel que $n \cdot 1_A = 0_A$, on a $n \in \mathrm{Ker}(\epsilon) = \mathrm{car}(A)\mathbb{Z}$. Ainsi, comme n et $\mathrm{car}(A)$ sont tous deux positifs, il existe $k \geq 1$ tel que $n = \mathrm{car}(A)k$. Cela implique $n \geq \mathrm{car}(A)$. ⌟

Exemples (de caractéristique)**.**

1. Les anneaux $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique nulle.
2. Un anneau A est de caractéristique $\mathrm{car}(A) = 1$ si et seulement si $A = 0$.
3. Pour tout $n \geq 1$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n [5].

Proposition II.3. *Si un anneau est intègre, alors sa caractéristique est soit nulle, soit un nombre premier.*

5. On verra des exemples d'anneaux infinis de caractéristique positive en section II.6, comme l'anneau des polynômes à coefficients dans $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. Supposons donc A intègre avec $\mathrm{car}(A) = n > 0$, et supposons par l'absurde que n n'est pas premier. Si $n = 1$, cela signifie que A est l'anneau nul, ce qui contredit l'hypothèse. Si $n \geq 2$, il existe des entiers r, s avec $1 < r, s < n$ tels que $rs = n$. Considérons les éléments $a = r \cdot 1_A$ et $b = s \cdot 1_A$ de A. Par minimalité de $n = \mathrm{car}(A)$, on a $a \neq 0_A$ et $b \neq 0_A$. Néanmoins, on a

$$ab = (r \cdot 1_A)(s \cdot 1_A) = (\overbrace{1_A + \cdots + 1_A}^{r})(\overbrace{1_A + \cdots + 1_A}^{s}) = \overbrace{1_A + \cdots + 1_A}^{rs=n} = n \cdot 1_A = 0_A\,.$$

Ainsi, l'anneau A admet des diviseurs de zéro, ce qui est une contradiction. □

Comme un corps est un anneau intègre, on obtient immédiatement le corollaire suivant.

Corollaire II.4. *La caractéristique d'un corps est soit nulle, soit un nombre premier.* □

Concluons cette section avec une dernière proposition.

Proposition II.5. *S'il existe un homomorphisme d'anneaux $A \to A'$, alors la caractéristique de A' divise celle de A dans $\mathbb{Z}$.*

Démonstration. Soit donc $\varphi\colon A \to A'$ un homomorphisme d'anneaux, et considérons les deux homomorphismes $\epsilon\colon \mathbb{Z} \to A$ et $\epsilon'\colon \mathbb{Z} \to A'$ de la proposition II.2. Comme la composition $\varphi \circ \epsilon\colon \mathbb{Z} \to A$ est un homomorphisme d'anneaux, on a $\varphi \circ \epsilon = \epsilon'$ par unicité. En notant $n = \mathrm{car}(A)$ et $n' = \mathrm{car}(A')$, on a donc

$$n\mathbb{Z} = \mathrm{Ker}(\epsilon) \subset \mathrm{Ker}(\varphi \circ \epsilon) = \mathrm{Ker}(\epsilon') = n'\mathbb{Z}\,,$$

ce qui implique que n' divise n. □

Corollaire II.6. *Deux anneaux isomorphes ont la même caractéristique.*

Démonstration. Par la proposition II.5, si A et A' sont isomorphes, on a $\mathrm{car}(A)$ divise $\mathrm{car}(A')$ et $\mathrm{car}(A')$ divise $\mathrm{car}(A)$. Cela implique qu'ils sont égaux au signe près. Comme ces deux entiers sont non-négatifs, ils sont égaux. □

II.3 Idéaux et anneaux quotients

En section I.8, nous avons vu la notion cruciale de *sous-groupe normal* : si N est un sous-groupe normal de G, alors il est possible de construire le groupe quotient G/N. De plus, un sous-ensemble d'un groupe G est un sous-groupe normal de G si et seulement si c'est le noyau d'un homomorphisme de groupes $\varphi\colon G \to G'$. Finalement, tout homomorphisme $\varphi\colon G \to G'$ induit un isomorphisme de groupes $\overline{\varphi}\colon G/\mathrm{Ker}(\varphi) \to \mathsf{Im}(\varphi)$.

Le but de cette section est d'adapter cette discussion aux anneaux, ce qui généralise le cas de l'anneau $\mathbb{Z}/n\mathbb{Z}$ vu en section II.1. Pour dégager la notion correcte, tentons de comprendre les propriétés des noyaux des homomorphismes d'anneaux.

Lemme II.7. *Si $\varphi\colon A \to A'$ est un homomorphisme d'anneaux, alors* $\mathrm{Ker}(\varphi) =: I$ *satisfait les deux propriétés suivantes :*

(i) I est un sous-groupe de $(A,+)$.

(ii) Pour tout $x \in I$ et $a \in A$, on a $xa \in I$ et $ax \in I$.

Démonstration. Comme nous l'avons déjà observé, le premier point découle du fait que $\varphi\colon (A,+) \to (A',+)$ est un homomorphisme de groupes, et de la proposition I.3. Pour vérifier le second point, fixons $x \in I = \mathrm{Ker}(\varphi)$ et $a \in A$; on calcule

$$\varphi(xa) = \varphi(x)\varphi(a) = 0 \cdot \varphi(a) = 0\,,$$

ce qui montre que xa appartient bien à $\mathrm{Ker}(\varphi) = I$. La preuve pour ax est similaire. □

Ce résultat motive la définition suivante.

Définition II.4

Un sous-ensemble I d'un anneau A est appelé un **idéal** de A s'il satisfait les deux propriétés suivantes :

(i) I est un sous-groupe de $(A,+)$ [a].

(ii) Pour tout $x \in I$ et $a \in A$, on a $xa \in I$ et $ax \in I$.

a. Rappelons que par la proposition I.1, il suffit de vérifier que I contient le neutre 0 et satisfait $x, y \in I \Rightarrow x - y \in I$.

Exemples (d'idéaux)**.**

1. Tout anneau $A \neq 0$ admet les deux idéaux $I = \{0\}$ et $I = A$.
   (On verra en exercice 17 qu'un anneau commutatif $A \neq 0$ est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A. En particulier, la théorie des idéaux est essentiellement triviale dans un corps.)
2. Pour tout $n \in \mathbb{Z}$, le sous-ensemble $I = n\mathbb{Z}$ est un idéal de l'anneau $A = \mathbb{Z}$. (Par la proposition I.9, ce sont les seuls idéaux de $\mathbb{Z}$.)
3. Soit x un élément fixé d'un anneau commutatif A. Considérons l'ensemble

   $$(x) \coloneqq xA = \{xa \,|\, a \in A\}$$

   des multiples de x dans A. Il s'agit d'un idéal de A.

   ⌜ En effet, notons d'abord que comme $0 = x \cdot 0$, le neutre additif est bien un élément de $(x) = xA$. De plus, la différence de deux éléments quelconques de (x) est de la forme $xa - xb$ avec $a, b \in A$. En utilisant la règle de calcul (ii) et l'axiome $(A4)$, on obtient

   $$xa - xb = xa + x(-b) = x(a-b)\,,$$

qui appartient bien à (x) puisque $a-b \in A$. Cela montre que (x) est un sous-groupe de $(A,+)$. Pour vérifier le second point, fixons $xa \in (x)$ et $a' \in A$. Comme A est commutatif, on obtient

$$a'(xa) = (xa)a' = x(aa')\,,$$

qui appartient bien à (x) puisque $aa' \in A$.

⌟

On parle de *l'idéal principal* engendré par $x \in A$.

Par exemple, on a $(0) = \{0\}$ et $(1) = A$, ce qui redonne l'exemple 1 ci-dessus.

Dans $A = \mathbb{Z}$, le choix $x = n \in \mathbb{Z}$ mène à $(x) = n\mathbb{Z}$, ce qui redonne l'exemple 2.

4. Si $\varphi\colon A \to A'$ est un homomorphisme d'anneaux, alors $\mathrm{Ker}(\varphi)$ est un idéal de A par le lemme II.7.

Remarques (sur les notions d'idéal et de sous-anneau)**.**

1. Un sous-ensemble d'un anneau A qui est à la fois un idéal et un sous-anneau de A coïncide avec A.

   ⌜ En effet, si $B \subset A$ est un sous-anneau, il contient le neutre multiplicatif 1. Si B est également un idéal, alors pour tout $a \in A$, il contient $a \cdot 1 = a$. On a ainsi $A \subset B$, d'où l'égalité $B = A$.

   ⌟

   Par conséquent, un idéal $I \subsetneq A$ n'est jamais un sous-anneau de A, et un sous-anneau $B \subsetneq A$ n'est jamais un idéal de A. Par exemple, $I = 2\mathbb{Z} \subset \mathbb{Z}$ est un idéal mais pas un sous-anneau de $\mathbb{Z}$, tandis que $B = \mathbb{Z} \subset \mathbb{Q}$ est un sous-anneau mais pas un idéal de $\mathbb{Q}$.

2. Les sous-anneaux de A coïncident avec les images des homomorphismes d'anneaux $\varphi\colon A' \to A$, tandis que les idéaux de A coïncident avec les noyaux des homomorphismes d'anneaux $\varphi\colon A \to A'$.

   ⌜ On a déjà vu en section II.2 que l'image d'un homomorphisme d'anneaux $\varphi\colon A' \to A$, est un sous-anneau de A. Réciproquement, tout sous-anneau $B \subset A$ est l'image de l'homomorphisme d'anneaux $\varphi\colon B \to A$ donné par l'inclusion. Par le lemme II.7, le noyau d'un homomorphisme d'anneaux $\varphi\colon A \to A'$ est un idéal de A. Finalement, la réciproque découle de la proposition II.8 à venir.

   ⌟

3. En conséquence de ces deux points, l'image d'un homomorphisme d'anneaux $\varphi\colon A' \to A$ n'est pas un idéal de A sauf si φ est surjectif, tandis que le noyau de $\varphi\colon A \to A'$ n'est pas un sous-anneau de A sauf si $A' = 0$.

Venons-en à présent aux anneaux quotients. Comme un idéal I d'un anneau A est en particulier un sous-groupe du groupe abélien $(A,+)$, c'est un sous-groupe normal, et l'on peut considérer le groupe quotient formé des classes d'équivalence

$$A/I = \{[a] \,|\, a \in A\}$$

pour la relation d'équivalence $a \sim b \Leftrightarrow a - b \in I$. Par la proposition I.23, c'est un groupe abélien pour l'addition $[a] + [b] \coloneqq [a+b]$.

Comme I est un idéal, ce quotient est en fait un anneau.

Proposition II.8. *Si $I \subset A$ est un idéal, alors A/I est un anneau pour les lois*

$$[a] + [b] \coloneqq [a+b] \quad \textit{et} \quad [a][b] \coloneqq [ab]\,.$$

De plus, la projection canonique $\pi\colon A \to A/I$ est un homomorphisme d'anneaux de noyau I.

Démonstration. Comme mentionné ci-dessus, la proposition I.23 nous dit d'ores et déjà que cette addition est bien définie sur A/I et le munit d'une structure de groupe (abélien puisque $(A,+)$ est abélien), tel que $\pi\colon A \to A/I$ est un homomorphisme de groupes de noyau I. Cela donne en particulier l'axiome $(A1)$.

Le point crucial qui reste à vérifier est que la multiplication est bien définie sur A/I. Pour ce faire, fixons $a, a', b, b' \in A$ tels que $[a] = [a']$ et $[b] = [b']$, et vérifions que $[ab] = [a'b']$. Par hypothèse, il existe $x, y \in I$ tels que $a' - a = x$ et $b' - b = y$. Calculons la différence

$$a'b' - ab = (a+x)(b+y) - ab \overset{(A4)}{=} ab + ay + xb + xy - ab = ay + xb + xy\,.$$

Comme on a $x, y \in I$, la seconde propriété dans la définition d'un idéal implique que les trois termes ci-dessus appartiennent à I. Par la première propriété dans la définition d'un idéal, leur somme est aussi dans I, ce qui montre que $a'b' - ab \in I$, et donc l'égalité voulue $[ab] = [a'b']$.

Les axiomes $(A2) - (A4)$ pour A/I découlent automatiquement des axiomes correspondants pour A. Par exemple, on a $1_{A/I} = [1_A]$ puisque

$$[1_A] \cdot [a] = [1_A \cdot a] = [a] = [a \cdot 1_A] = [a][1_A]$$

pour tout $a \in A$.

Finalement, on sait déjà que la projection canonique $\pi\colon A \to A/I$ est un homomorphisme de groupes, et donc satisfait la première condition d'un homomorphisme d'anneaux. Les deux autres conditions sont elles aussi automatiques, puisque

$$\pi(ab) = [ab] = [a][b] = \pi(a)\pi(b)$$

pour tous $a, b \in A$, et

$$\pi(1_A) = [1_A] = 1_{A/I}\,.$$

Cela conclut la preuve. □

Exemples (d'anneaux quotients)**.**

1. Pour $I = \{0\} \subset A$, la relation d'équivalence correspondante est l'égalité. Ainsi, l'anneau quotient est formé des singletons $A/\{0\} = \{\{a\} \mid a \in A\}$. La projection canonique $\pi\colon A/\{0\} \to A$ est donc bijective, et fournit ainsi un isomorphisme d'anneaux $A/\{0\} \simeq A$.

2. Pour $I = A \subset A$, l'ensemble quotient correspondant est formé d'une unique classe d'équivalence $A/A = \{A\} = \{[0_A]\}$, et on est en présence de l'anneau nul $A/A = 0$.

3. Pour tout $n \in \mathbb{Z}$, le choix de l'idéal $I = n\mathbb{Z}$ dans $A = \mathbb{Z}$ donne l'anneau quotient $A/I = \mathbb{Z}/n\mathbb{Z}$ vu en section II.1.
4. Plus généralement, pour x un élément fixé d'un anneau commutatif A, on a l'anneau quotient $A/(x) = \{[a] \,|\, a \in A\}$ pour la relation d'équivalence $a \sim b \Leftrightarrow a - b \in (x) = xA$.

Continuons à adapter les résultats de la section I.8 aux anneaux.

Proposition II.9. *Soit I un idéal d'un anneau A. Si $\varphi: A \to A'$ est un homomorphisme d'anneaux avec $I \subset \mathrm{Ker}(\varphi)$, alors il existe un unique homomorphisme d'anneaux $\overline{\varphi}: A/I \to A'$ tel que $\overline{\varphi} \circ \pi = \varphi$.*

Démonstration. Par hypothèse, la proposition I.24 peut être appliquée, d'où l'existence d'un unique homomorphisme de groupes $\overline{\varphi}: (A/I, +) \to (A', +)$ tel que $\overline{\varphi} \circ \pi = \varphi$, i.e. avec $\overline{\varphi}([a]) = \varphi(a)$ pour tout $a \in A$. Il reste juste à vérifier que c'est un homomorphisme d'anneaux. C'est automatique puisque

$$\overline{\varphi}([a][b]) = \overline{\varphi}([ab]) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}([a])\overline{\varphi}([b])$$

pour tous $a, b \in A$, tandis que

$$\overline{\varphi}(1_{A/I}) = \overline{\varphi}([1_A]) = \varphi(1_A) = 1_{A'}\,.$$

Cela conclut la preuve. □

Nous sommes finalement en mesure de montrer le *premier théorème d'isomorphisme* pour les anneaux.

Théorème II.10: Théorème d'isomorphisme pour les anneaux

Tout homomorphisme d'anneaux $\varphi: A \to A'$ induit un isomorphisme d'anneaux

$$\overline{\varphi}: A/\mathrm{Ker}(\varphi) \xrightarrow{\simeq} \mathsf{Im}(\varphi)\,.$$

Démonstration. Par le théorème I.25, l'homorphisme de groupes $\varphi: (A, +) \to (A', +)$ induit un isomorphisme de groupes $\overline{\varphi}: A/\mathrm{Ker}(\varphi) \to \mathsf{Im}(\varphi)$, qui est un homomorphisme d'anneaux par la proposition II.9. Ainsi, c'est un homomorphisme d'anneaux bijectif, et donc un isomorphisme d'anneaux. □

Exemple. Soit A un anneau quelconque, et soit $\epsilon: \mathbb{Z} \to A$ l'unique homomorphisme de la proposition II.2. Par définition, on a $\mathrm{Ker}(\epsilon) = n\mathbb{Z}$ avec $n = \mathrm{car}(A)$. Par le théorème II.10, l'homomophisme ϵ induit un isomorphisme d'anneaux

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\simeq} \mathsf{Im}(\epsilon) \subset A\,.$$

Ainsi, l'anneau A contient un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$, où $n = \mathrm{car}(A)$.

II.4 Anneaux euclidiens

EUCLIDE
(~300 av.J.C.)

Dans cette section, nous allons nous intéresser à une classe particulière d'anneaux qui contient $\mathbb{Z}$, les corps, ainsi que les entiers de Gauss (voir section II.5) et les anneaux de polynômes à coefficients dans un corps (section II.6).

L'idée est de formaliser la notion de division euclidienne dans $\mathbb{Z}$. La difficulté réside dans le fait que dans $\mathbb{Z}$, on demande que le reste $r \in \mathbb{Z}$ de la division de $a \in \mathbb{Z}$ par $b \in \mathbb{Z} \setminus \{0\}$ satisfasse $0 \leq r < |b|$. En clair, on utilise de façon cruciale l'ordre naturel sur $\mathbb{Z}$. Voici la solution.

Définition II.5

Un anneau intègre A est un **anneau euclidien** s'il existe une application $f : A \setminus \{0\} \to \{1, 2, \ldots\}$ satisfaisant les conditions suivantes :

1. Pour tous $a, b \in A \setminus \{0\}$, on a $f(a) \leq f(ab)$.
2. Pour tous $a \in A$ et $b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que $a = qb + r$ et soit $r = 0$ soit $f(r) < f(b)$.

Remarques.

1. Intuitivement, l'application f mesure la "taille" d'un élément non-nul de A, à la façon de la valeur absolue sur $\mathbb{Z}$.
2. Cette application f n'est pas nécessairement unique (voir l'exemple 2 ci-dessous) : c'est l'existence d'au moins une telle application qui fait de A un anneau euclidien.
3. Étant donnés $a \in A$ et $b \in A \setminus \{0\}$, la paire d'éléments (q, r) de A telle que $a = qb + r$ n'est en général pas unique (voir l'exemple 1).
4. On verra en exercice 26 que la seconde condition suffit, dans le sens suivant : si A est un anneau intègre muni d'une application $g : A \setminus \{0\} \to \{1, 2, \ldots\}$ satisfaisant la seconde condition, alors l'anneau A est euclidien via l'application $f : A \setminus \{0\} \to \{1, 2, \ldots\}$ définie par $f(a) = \min_{x \in A \setminus \{0\}} g(xa)$.

Exemples (d'anneaux euclidiens)**.**

1. L'anneau des entiers $A = \mathbb{Z}$ est euclidien via $f : \mathbb{Z} \setminus \{0\} \to \{1, 2, \ldots\}$ donnée par $f(a) = |a|$.

   ⌜ Pour tous $a, b \in \mathbb{Z} \setminus \{0\}$, on a bien $f(a) = |a| \leq |a||b| = |ab| = f(ab)$ puisque $|b| \geq 1$. De plus, la division eulidienne assure que pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$, il existe $q, r \in \mathbb{Z}$ avec $a = qb + r$ et $0 \leq r < |b|$: on a bien soit $r = 0$, soit $f(r) < f(b)$. ⌟

   Mais cette paire (q, r) n'est pas unique, puisque $(a, b) = (1, 2)$ mène aux solutions $(q, r) = (0, 1)$ et $(1, -1)$, par exemple. En revanche, si l'on demande de plus que $r \geq 0$, alors cette paire est unique : c'est la forme habituelle de la division euclidienne.

2. Tout corps $A = K$ est un anneau euclidien via $f : K \setminus \{0\} \to \{1, 2, \ldots\}$ donnée par n'importe quelle application constante.

   ⌜ Pour tous $a \in K$ et $b \in K \setminus \{0\} = K^*$, on peut poser $q = ab^{-1}$ et $r = 0$, qui satisfont bien l'égalité $qb + r = a$, et donc la seconde condition. Comme on a toujours $r = 0$, l'application f n'intervient pas dans cette seconde condition, et peut ainsi être choisie arbitrairement, pour autant qu'elle satisfasse la première condition. En particulier, toute application constante fait l'affaire. ⌟

La division euclidienne avait été utilisée en proposition I.9 pour caractériser les sous-groupes de $\mathbb{Z}$. Voici une généralisation de ce résultat aux anneaux euclidiens, avec presque exactement la même preuve.

Proposition II.11. *Si I est un idéal d'un anneau euclidien A, alors il existe $x \in A$ tel que $I = (x) = \{xa \,|\, a \in A\}$, l'idéal principal engendré par x.*

Démonstration. Si $I = \{0\}$, alors on a bien $I = (x)$ pour $x = 0$ et l'énoncé est vérifié ; on peut donc supposer $I \neq \{0\}$. Comme l'ensemble $I \setminus \{0\}$ est non-vide, il existe $x \in I \setminus \{0\}$ qui minimise f sur cet ensemble ; en d'autres termes, on choisit $x \in I \setminus \{0\}$ tel que

$$f(x) \leq f(r) \quad \text{pour tout } r \in I \setminus \{0\}\,.$$

Nous allons maintenant vérifier l'égalité $I = (x)$, ce qui montrera la proposition.

L'inclusion $(x) \subset I$ est immédiate : comme x appartient à I qui est un idéal, il doit nécesairement contenir les multiples de x, d'où $(x) = \{xa \,|\, a \in A\} \subset I$. Pour montrer l'autre inclusion, prenons $y \in I$. Comme A est euclidien et x non-nul, il existe $q, r \in A$ tels que $y = qx + r$ et soit $r = 0$ soit $f(r) < f(x)$. Si $r = 0$, alors on a $y = qx \in (x)$, ce qu'on voulait démontrer. Dans le cas contraire, on aurait $r \neq 0$ et $r = y - qx$ avec $f(r) < f(x)$. Comme x, y sont des éléments de I qui est un idéal, on a $r = y - qx \in I$. On aurait donc $r \in I \setminus \{0\}$ avec $f(r) < f(x)$, ce qui contredit la minimalité de x en exergue ci-dessus. □

Remarques.

1. L'élément x qui engendre I n'est pas unique, mais on comprend parfaitement comment sont reliés deux tels éléments : c'est l'objet de la proposition II.12 ci-dessous.
2. Un anneau intègre dans lequel tous les idéaux sont principaux est appelé un *anneau principal*. On vient donc de montrer que tout anneau euclidien est un anneau principal [6].

Le but de la suite de cette section est d'étendre aux anneaux euclidiens les notions d'arithmétique suivantes, vues sur $\mathbb{Z}$: la divisibilité, le plus grand commun diviseur, et les éléments premiers.

6. La réciproque est fausse : il existe des anneaux principaux qui ne sont pas euclidiens, par exemple $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$, mais cela dépasse le cadre de ce cours.

A. Divisibilité

L'extension de cette notion est parfaitement naturelle.

Terminologie. Soit A un anneau commutatif, et soient $a, b \in A$. On dit que a *divise* b dans A, noté $a \mid b$, s'il existe $c \in A$ tel que $b = ac$. Dans le cas contraire, on note $a \nmid b$.

Exemples (de divisibilité)**.**

1. Dans $\mathbb{Z}$, on a $2 \nmid 3$ puisqu'il n'existe pas d'entier $c \in \mathbb{Z}$ tel que $3 = 2c$. En revanche, on a $2 \mid 3$ dans $\mathbb{Q}$, puisque le rationnel $c = \frac{2}{3} \in \mathbb{Q}$ satisfait $3 = 2c$.
2. Dans un corps K, tout $a \neq 0$ divise tout $b \in K$, puisque l'élément $c = a^{-1}b \in K$ satisfait $b = ac$. Ainsi, l'étude de la divisibilité dans un corps est essentiellement triviale.

Remarque. On vérifie en exercice 22 les énoncés suivants, valides pour tous a, b, c dans un anneau commutatif A :

1. Si $a \mid b$ et $b \mid c$, alors $a \mid c$.
2. Si $a \mid b$ et $a \mid c$, alors $a \mid (b + c)$.
3. Si $a \mid b$, alors $a \mid bx$ pour tout $x \in A$.
4. Si $a \mid b$, alors $au \mid b$ pour toute unité $u \in A^*$.
5. On a $a \mid b$ si et seulement si $(b) \subset (a)$.

Proposition II.12. *Pour tous a, b dans un anneau intègre A, sont équivalents :*

(i) $a \mid b$ *et* $b \mid a$ *;*

(ii) $(a) = (b)$ *;*

(iii) il existe $u \in A^*$ *tel que* $b = au$*.*

Démonstration. L'équivalence entre les deux premières conditions découle du point 5 de la remarque ci-dessus (et est donc valide sans hypothèse sur A autre que la commutativité). Supposons à présent que $a, b \in A$ satisfont la condition (iii) : il existe $u \in A^*$ tel que $b = au$. Dans ce cas, on a $a \mid b$ par définition, et comme $a \mid a$, on a également $b = au \mid a$ par la remarque 4 ci-dessus.

Le seul point non-trivial, et le seul à invoquer l'hypothèse d'intégrité de A, est l'implication (i)⇒(iii). Supposons donc que $a, b \in A$ satisfont $a \mid b$ et $b \mid a$. Par définition, il existe $c, d \in A$ tels que $b = ac$ et $a = bd$, d'où $a = acd$. En utilisant une règle de calcul et la distributivité, on obtient

$$0 = a - acd = a + a(-cd) = a(1 - cd)\,.$$

Comme A est intègre, soit $a = 0$, soit $1 - cd = 0$. Dans le premier cas, on a $a = 0$ et $b = 0 \cdot c = 0$: le point (iii) est satisfait en posant $u = 1 \in A^*$, puisque $0 = 0 \cdot 1$. Dans le second cas, on a $cd = 1$ d'où $c \in A^*$, et le point (iii) est satisfait en posant $u = c \in A^*$, puisque $b = ac$. □

Terminologie. Si deux éléments a, b d'un anneau intègre A satisfont l'une des conditions de la proposition II.12, on dit qu'ils sont *associés* dans A.

On verra en exercice 23 qu'il s'agit d'une relation d'équivalence, et que la divisibilité définit une relation d'ordre sur les classes d'équivalence correspondantes.

Exemples (d'éléments associés)**.**

1. Dans $A = \mathbb{Z}$, on a $\mathbb{Z}^* = \{-1, 1\}$. Ainsi, deux entiers sont associés si et seulement s'ils sont égaux au signe près. On aura naturellement tendance à choisir l'unique représentant non-négatif dans la classe d'équivalence correspondante.
2. Dans un corps K, on a $K^* = K \setminus \{0\}$. Ainsi, deux éléments a, b sont associés si et seulement s'ils sont tous les deux nuls, ou tous les deux non-nuls. Il y a donc deux classes d'équivalence, données par $\{0\}$ et $K \setminus \{0\}$, qui possèdent les représentants naturels 0 et 1, respectivement.

B. Plus grand commun diviseur et théorème des restes chinois

La définition de plus grand commun diviseur dans $\mathbb{Z}$ donnée en section I.5 se généralise facilement, à un détail près qui sera discuté ci-dessous.

Terminologie. Soit A un anneau commutatif, et soient $a, b \in A$. Un élément d de A est appelé un *plus grand commun diviseur* de a et b dans A, noté $\mathrm{pgcd}(a, b)$, s'il satisfait les deux propriétés suivantes :

— $d \mid a$ et $d \mid b$,

— si $c \in A$ est tel que $c \mid a$ et $c \mid b$, alors $c \mid d$.

On dit que a et b sont *premiers entre eux*[7] dans A si 1 est un plus grand commun diviseur de a et b dans A.

Si la définition du plus grand commun diviseur se généralise de manière presque immédiate, se posent les questions de l'existence et de l'unicité de cet élément. L'unicité est traitée dans les remarques ci-dessous.

Remarques.

1. Si $d \in A$ est un pgcd de a et b dans A et $u \in A^*$ une unité, alors du est également un pgcd de a et b. Ainsi, "dans le meilleur des cas", le pgcd est unique à association près, i.e. à multiplication par une unité près.

   ⌜ Si d est un pgcd de a et b, alors $d \mid a$ et $d \mid b$. Par la remarque 4 ci-dessus, on a également $du \mid a$ et $du \mid b$. De plus, si $c \in A$ est tel que $c \mid a$ et $c \mid b$, alors $c \mid d$, ce qui implique que $c \mid du$ par la remarque 3. ⌟

2. Réciproquement, si A est intègre et d, d' sont deux pgcd de a et b dans A, alors ils sont associés : il existe $u \in A^*$ tel que $d' = du$.

   ⌜ Par la première condition dans la définition de pgcd, on a $d \mid a, d \mid b$, et $d' \mid a, d' \mid b$. Par la seconde condition, cela implique $d \mid d'$ et $d' \mid d$. Par la proposition II.12, qui peut être appliquée puisque A est intègre, il existe $u \in A^*$ tel que $d' = du$. ⌟

7. On vérifie facilement que deux éléments sont premiers entre eux si et seulement si leurs diviseurs communs coïncident avec les unités de A.

Exemples (de plus grands communs diviseurs)**.**

1. Dans $A = \mathbb{Z}$, si d est un pgcd de $a, b \in \mathbb{Z}$, alors $-d$ en est aussi un. Dans cet anneau, on peut définir le pgcd de a et b comme l'unique $\text{pgcd}(a, b) \geq 0$. Mais cet exemple, bien que très naturel, est tout à fait particulier à cet égard et ne doit pas faire oublier qu'en général, un pgcd n'est défini qu'à association près.
2. Dans $A = K$ un corps, on a $\text{pgcd}(0, 0) = 0$, tandis que si $(a, b) \neq (0, 0)$, alors $\text{pgcd}(a, b)$ est donné par n'importe quel élément de K^* (exercice 25). Ainsi, tous les éléments de K sont premiers entre eux, à l'exception de $(0, 0)$.

On a donc répondu à la question de l'unicité du pgcd, dans le cadre très général des anneaux intègres. Qu'en est-il de l'existence ? C'est ici qu'il est nécessaire de se restreindre aux anneaux euclidiens [8].

Proposition II.13. *Si A est un anneau euclidien, alors tous $a, b \in A$ admettent un plus grand commun diviseur $d \in A$, et il existe $r, s \in A$ tels que $d = ra + sb$.*

Démonstration. Étant donnés a, b deux éléments d'un anneau euclidien A, considérons le sous-ensemble

$$I = \{ra + sb \,|\, r, s \in A\} \subset A\,.$$

Il s'agit d'un idéal de A. En effet, il contient $0 = 0 \cdot a + 0 \cdot b$, et si $ra + sb$ et $r'a + s'b$ sont deux éléments de I, alors leur différence en est aussi un puisqu'on a

$$(ra + sb) - (r'a + s'b) = (r - r')a + (s - s')b \in I\,.$$

Finalement, pour $ra + sb \in I$ et $x \in A$, on a $x(ra + sb) = (xr)a + (xs)b \in I$, qui est donc bien un idéal de A.

Par la proposition II.11, que l'on peut appliquer puisque A est euclidien, il existe $d \in A$ tel que $I = (d) = dA$. Il reste à vérifier que d satisfait les deux conditions d'un pgcd de a et b.

Notons tout d'abord que $a = 1 \cdot a + 0 \cdot b$ est un élément de $I = (d)$, ce qui signifie que $d \mid a$. De même, on a $b = 0 \cdot a + 1 \cdot b \in I = (d)$, d'où $d \mid b$. De plus, si $c \in A$ est tel que $c \mid a$ et $c \mid b$, alors par les remarques 2 et 3 sur la divisibilité, on a $c \mid (ra + sb)$ pour tous $r, s \in A$. Ainsi, on a $c \mid x$ pour tout $x \in I$. Comme d est élément de I, on a en particulier $c \mid d$, ce qui montre que d satisfait la seconde condition d'un pgcd de a et b.

Enfin, comme d est élément de I, il existe $r, s \in A$ tels que $d = ra + sb$. □

Ainsi, c'est la théorie des idéaux qui permet de construire les plus grands communs diviseurs dans les anneaux euclidiens.

8. Comme le montre la preuve de la proposition II.13, le cadre plus général des anneaux principaux conviendrait tout aussi bien. Cette preuve est à comparer à celle de la proposition I.11, qu'elle généralise.

Avant de passer aux éléments premiers, nous allons faire un petit détour par le plus petit commun multiple, ce qui nous permettra de démontrer un résultat remarquable appelé le "théorème des restes chinois".

Terminologie. Soit A un anneau commutatif, et soient $a, b \in A$. Un élément c de A est appelé un *plus petit commun multiple* de a et b dans A, noté $\mathrm{ppcm}(a, b)$, s'il satisfait les deux propriétés suivantes :

— $a \mid c$ et $b \mid c$,

— si $x \in A$ est tel que $a \mid x$ et $b \mid x$, alors $c \mid x$.

La théorie développée ci-dessus pour le pgcd s'adapte facilement, et mène aux résultats suivants qui seront vus en exercice 27 :

1. Pour a, b deux éléments fixés d'un anneau intègre A, deux plus petit communs multiples de a et b sont associés.
2. Si A est un anneau euclidien, alors tous $a, b \in A$ admettent un plus petit commun multiple $c \in A$, donné par $(a) \cap (b) = (c)$.

De plus, le pgcd et le ppcm sont liés par la relation suivante, qui sera également vue en exercice 27 :

3. Si A est un anneau intègre et si d (resp. c) est un pgcd (resp. un ppcm) de a et b dans A, alors cd et ab sont associés dans A.

L'énoncé du théorème nécessite encore une convention : pour $a \in A$, on notera $[x]_a \in A/(a)$ la classe d'équivalence de $x \in A$ modulo l'idéal principal $(a) \subset A$.

Théorème II.14: Théorème des restes chinois

Soient A un anneau euclidien, et $a, b \in A$ premiers entre eux. Alors, l'application

$$A/(ab) \longrightarrow A/(a) \times A/(b)\,, \quad [x]_{ab} \longmapsto ([x]_a, [x]_b)$$

est un isomorphisme d'anneaux.

Exemple. Pour $A = \mathbb{Z}$ (qui est bien euclidien), on obtient l'énoncé suivant : si $m, n \in \mathbb{Z}$ sont premiers entre eux, alors on a un isomorphisme d'anneaux

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\,, \quad [x]_{mn} \longmapsto ([x]_m, [x]_n)\,.$$

En particulier, on a un isomorphisme de groupes abéliens $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, comme promis en section I.9.

Par conséquent, l'application décrite ci-dessus étant une bijection, on obtient le résultat suivant : si $m, n \in \mathbb{Z}$ sont premiers entre eux, alors pour tous $y, z \in \mathbb{Z}$, le système

$$\begin{aligned} x &\equiv y \pmod{m} \\ x &\equiv z \pmod{n} \end{aligned}$$

admet une solution $x \in \mathbb{Z}$, solution unique à addition d'un multiple de mn près.

Remarque. Une multitude de généralisations de ce théorème existe, par exemple dans les anneaux principaux (avec la même preuve), mais aussi pour un nombre arbitraire d'éléments deux à deux premiers entre eux.

Démonstration du théorème II.14. Soient donc a, b deux éléments premiers entre eux dans un anneau euclidien A, et soit

$$\varphi\colon A \longrightarrow A/(a) \times A/(b)$$

l'application donnée par

$$\varphi(x) = ([x]_a, [x]_b) =: (\pi_a(x), \pi_b(x)) \,.$$

Comme les projections canoniques $\pi_a\colon A \to A/(a)$ et $\pi_b\colon A \to A/(b)$ sont des homomorphismes d'anneaux, il en va de même pour φ. Tentons à présent de déterminer son noyau et son image.

Par définition de φ et la proposition II.8, on a

$$\mathrm{Ker}(\varphi) = \{x \in A \,|\, \pi_a(x) = \pi_b(x) = 0\} = \mathrm{Ker}(\pi_a) \cap \mathrm{Ker}(\pi_b) = (a) \cap (b) \,.$$

De plus, par les résultats 2 et 3 ci-dessus sur le ppcm et le fait que a, b sont premiers entre eux, on obtient

$$(a) \cap (b) = (\mathrm{ppcm}(a, b)) = (\mathrm{ppcm}(a, b) \cdot \mathrm{pgcd}(a, b)) = (ab) \ .$$

Ainsi, le noyau de φ est l'idéal (ab).

Nous allons maintenant montrer que φ est surjectif. Comme a, b sont premiers entre eux, la proposition II.13 implique qu'il existe $r, s \in A$ tels que $ra + sb = 1$. Ainsi, on a les égalités $[sb]_a = [1]_a$ et $[ra]_b = [1]_b$. Pour un élément quelconque $([y]_a, [z]_b)$ de $A/(a) \times A/(b)$, considérons $x = sby + raz \in A$. On a

$$\varphi(x) = ([sby]_a, [raz]_b) = ([sb]_a \cdot [y]_a, [ra]_b \cdot [z]_b) = ([y]_a, [z]_b) \ ,$$

ce qui montre que φ est bien surjective.

Il ne reste plus qu'à appliquer le théorème II.10, i.e. le théorème d'isomorphisme pour les anneaux : l'homomorphisme $\varphi\colon A \to A/(a) \times A/(b)$ induit un isomorphisme $\overline{\varphi}\colon A/(ab) \to A/(a) \times A/(b)$ donné par $[x]_{ab} \mapsto ([x]_a, [x]_b)$. Cela conclut la preuve du théorème des restes chinois. □

C. Décomposition en éléments irréductibles et premiers

La difficulté ici est que la notion de nombre premier dans $\mathbb{Z}$ admet deux généralisations aux anneaux intègres, qui ne coïncident en général pas. Comme on le verra ci-dessous, elles coïncident bel et bien dans le cas des anneaux euclidiens, ce qui suffira à notre bonheur. En particulier, cela nous permettra de démontrer une extension du théorème fondamental de l'arithmétique de $\mathbb{Z}$ aux anneaux euclidiens.

Terminologie. Soit A un anneau intègre, et soit $p \in A \setminus \{0\}$ tel que $p \notin A^*$:

- p est dit *irréductible* dans A si, pour tous $a, b \in A$ tels que $p = ab$, on a $a \in A^*$ ou $b \in A^*$ [9].
- p est dit *premier* dans A si, pour tous $a, b \in A$ tels que $p \mid ab$, on a $p \mid a$ ou $p \mid b$.

Exemples (d'éléments premiers et irréductibles)**.**

1. Dans un corps K, il n'y a aucun élément premier et aucun élément irréductible, puisque $K^* \cup \{0\} = K$.
2. Dans l'anneau $\mathbb{Z}$ des entiers, on verra ci-dessous que p est premier si et seulement si p est irréductible, ce qui signifie que les seuls diviseurs de p sont ± 1 et $\pm p$. C'est équivalent à la condition que les seuls diviseurs positifs de p sont 1 et p, la définition habituelle d'un nombre premier.

   Ainsi, on retrouve bien la notion usuelle de nombre premier, à cela près que les nombres négatifs sont aussi admis : $\ldots, -11, -7, -5, -3, -2, 2, 3, 5, 7, 11, \ldots$

Proposition II.15. *Dans un anneau intègre, tout élément premier est irréductible. Dans un anneau euclidien, tout élément irréductible est premier.*

Démonstration. Soit donc p premier dans un anneau intègre A, et soient $a, b \in A$ tels que $p = ab$. Il s'agit de montrer que a ou b est une unité de A. Comme $p \mid p = ab$ et p est premier, on a $p \mid a$ ou $p \mid b$; supposons sans restreindre la généralité que $p \mid a$. Ainsi, il existe $c \in A$ tel que $a = pc$. On a donc $p = ab = pcb$, ce qui implique $1 = cb$ puisque A est intègre et p non-nul. On a donc bien que b est une unité.

Soit à présent p irréductible dans un anneau euclidien A, et soient $a, b \in A$ tels que $p \mid ab$. Il s'agit de montrer que $p \mid a$ ou $p \mid b$. Supposons que $p \nmid a$, et vérifions que $p \mid b$.

Dans un premier temps, nous allons voir que p et a sont premiers entre eux. En effet, soit $d \in A$ un diviseur de a et de p. Il existe donc $c \in A$ tel que $p = dc$. Comme p est irréductible, on a $d \in A^*$ ou $c \in A^*$. Dans le second cas, on aurait $p = dc$ avec $c \in A^*$, d'où $p \mid d$; comme on a $d \mid a$, cela impliquerait $p \mid a$, une contradiction. On a donc qu'un diviseur commun d de a et p est une unité. En particulier, un pgcd de p et a est une unité, ce qui signifie que p et a sont bien premiers entre eux.

Par la proposition II.13, qu'on peut appliquer puisque A est euclidien, il existe $r, s \in A$ tels que $ra + sp = 1$. Par hypothèse, on a $p \mid ab$, d'où $p \mid rab$. Par définition, on a également $p \mid spb$. Ainsi, p divise $rab + spb = (ra + sp)b = b$, ce qu'il fallait démontrer. □

Remarques.

1. Ce résultat se généralise aux anneaux principaux, avec la même preuve.
2. Il existe néanmoins des anneaux intègres (mais pas principaux) où ce résultat n'est pas valide. Par exemple, on verra en exercice 31 que l'élément 3 est irréductible mais pas premier dans l'anneau $\mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}\}$.

9. De manière équivalente, si $a \mid p$ dans A, alors a est une unité ou a est associé à p.

Voici enfin la généralisation aux anneaux euclidiens du théorème fondamental de l'arithmétique.

Théorème II.16

Soit A un anneau euclidien, et soit $a \in A \setminus \{0\}$ avec $a \notin A^*$. Alors, il existe des éléments irréductibles $p_1, \dots, p_n \in A$ tels que $a = p_1 \cdots p_n$. De plus, si $a = p_1 \cdots p_n = q_1 \cdots q_m$ sont deux telles factorisations, alors on a $m = n$ et il existe une permutation $\sigma \in S_n$ telle que p_i est associé à $q_{\sigma(i)}$ pour tout $i = 1, \dots, n$.

De façon moins formelle mais peut-être plus claire, on a donc : tout élément de $A \setminus (A^* \cup \{0\})$ se décompose en produit d'irréductibles, et cette décomposition est unique à l'ordre des facteurs près, et à multiplication par des unités près.

Exemples.

1. Pour $A = \mathbb{Z}$, on peut toujours choisir les irréductibles (ou premiers) positifs, ce qui donne donc bien le *théorème fondamental de l'arithmétique* : tout entier $n > 1$ se décompose en produit de nombres premiers positifs, et cette décomposition est unique à l'ordre des facteurs près.

   Notons néanmoins qu'en général, si on ne suppose pas les premiers positifs, on peut avoir par exemple $6 = 2 \cdot 3 = (-2)(-3)$.
2. Pour $A = K$ un corps, l'énoncé de ce théorème est bien entendu correct, mais totalement vide puisque $K \setminus (K^* \cup \{0\}) = \varnothing$.

La preuve de ce théorème repose sur le lemme suivant, qu'on va démontrer dans un premier temps.

Lemme II.17. *Dans un anneau euclidien, une application $f : A \setminus \{0\} \to \{1, 2, \dots\}$ comme dans la définition II.5 satisfait $f(a) < f(ab)$ pour tous $a \neq 0$ et $b \neq 0$ avec $b \notin A^*$.*

Démonstration. Soit donc A un anneau euclidien, soit $f : A \setminus \{0\} \to \{1, 2, \dots\}$ une application satisfaisant les deux conditions de la définition II.5, et soient $a \neq 0$ et $b \neq 0$ avec $b \notin A^*$. Par définition, on a $f(a) \leq f(ab)$, et l'on veut voir l'inégalité stricte $f(a) < f(ab)$. Supposons par l'absurde $f(a) = f(ab)$, et tentons d'obtenir la contradiction $b \in A^*$. Si on avait $f(a) = f(ab)$, on aurait alors

$$f(ab) = f(a) = \min\{f(y) \mid y \in (a) \setminus \{0\}\}.$$

En effet, pour tout $y \in (a) \setminus \{0\}$, il existe $x \in A \setminus \{0\}$ tel que $y = xa$, d'où $f(y) = f(xa) \geq f(a)$; comme a appartient à $(a) \setminus \{0\}$, on a bien l'égalité ci-dessus.

Par la preuve de la proposition II.11, le fait que $x = ab$ minimise la valeur de f sur l'ensemble $I \setminus \{0\} = (a) \setminus \{0\}$ implique que l'idéal $I = (a)$ est engendré par $x = ab$. On a donc $a \in (a) = (ab)$, d'où l'existence de $c \in A$ tel que $a = abc$. Comme A est intègre et a non-nul, on a $1 = bc$, et b est une unité de A. □

Nous sommes maintenant en mesure de démontrer le théorème II.16.

Démonstration du théorème II.16. L'existence de la décomposition en produit d'irréductibles découle immédiatement de l'affirmation suivante : *tout* $a \in A \setminus \{0\}$ *est soit une unité, soit le produit d'un nombre fini d'irréductibles.*

La preuve de cette affirmation se fait par induction sur $f(a) \in \{1, 2, \ldots\}$:

- Si $f(a) = 1$, alors a est une unité de A : par la contraposée, si a n'est pas dans A^*, alors le lemme II.17 implique $f(a) = f(1 \cdot a) > f(1) \geq 1$, d'où $f(a) > 1$.
- Soit à présent $a \in A \setminus \{0\}$ avec $f(a) > 1$, et supposons l'affirmation vérifiée pour tout $x \in A \setminus \{0\}$ avec $f(x) < f(a)$. Si a est une unité ou un élément irréductible, l'affirmation est trivialement vraie. Supposons donc $a \notin A^*$ et non irréductible : en d'autres termes, on peut écrire $a = bc$ avec $b, c \in A$ qui ne sont pas des unités. Par le lemme II.17, on a $f(b) < f(bc) = f(a)$ puisque $c \notin A^*$, et $f(c) < f(bc) = f(a)$, puisque $b \notin A^*$. Par hypothèse de récurrence, les éléments b et c sont produits d'un nombre fini d'irréductibles. Il en va donc de même pour leur produit $bc = a$, ce qui conclut la preuve de l'affirmation.

Venons-en à la preuve de l'unicité de la décomposition. Soient donc $a = p_1 \cdots p_n = q_1 \cdots q_m$ avec $p_1, \ldots, p_n, q_1, \ldots, q_m$ irréductibles, et supposons sans restreindre la généralité $n \leq m$. Comme A est euclidien, la proposition II.15 nous garantit que ces éléments sont également premiers. Comme $p_1 \mid p_1 \cdots p_n = q_1 \cdots q_m$ et p_1 est premier, il existe $j \in \{1, \ldots, m\}$ tel que $p_1 \mid q_j$; il existe donc $u_1 \in A$ tel que $q_j = u_1 p_1$. Comme q_j est irréductible, on a soit $p_1 \in A^*$, ce qui est impossible puisque p_1 est irréductible, soit $u_1 \in A^*$, ce qui est donc le cas. En conclusion, p_1 est associé à q_j, que l'on notera $q_{\sigma(1)}$.

Comme $q_j = u_1 p_1$, on peut écrire $p_1 p_2 \cdots p_n = q_1 \cdots q_{j-1}(u_1 p_1) q_{j+1} \cdots q_m$. Comme A est intègre et p_1 non-nul, cela implique l'égalité $p_2 \cdots p_n = u_1 q_1 \cdots q_{j-1} q_{j+1} \cdots q_m$, à laquelle on peut appliquer le même argument : il existe $\sigma(2) \in \{1, \ldots, m\} \setminus \{\sigma(1)\}$ et $u_2 \in A^*$ tels que $q_{\sigma(2)} = u_2 p_2$, et on recommence. En utilisant n fois ce raisonnement, on obtient une application injective $\sigma : \{1, \ldots, n\} \to \{1, \ldots, m\}$ et une égalité de la forme

$$1 = u_1 u_2 \cdots u_n q_{j_1} \cdots q_{j_{m-n}} ,$$

avec $u_1, \ldots, u_n$ des unités et $\{j_1, \ldots, j_{m-n}\} = \{1, \ldots, m\} \setminus \mathsf{Im}(\sigma)$. Cela implique que le produit d'irréductibles $q_{j_1} \cdots q_{j_{m-n}}$ est lui-même une unité, ce qui est impossible sauf si ce produit est vide. Ainsi, on a $m = n$ et σ est bien une bijection, i.e. un élément de S_n. Cela conclut la preuve. □

Remarques.

1. Un anneau intègre pour lequel l'énoncé du théorème II.16 est valide est appelé un *anneau factoriel*. On a donc montré qu'un anneau euclidien est factoriel.
2. En fait, on peut montrer le résultat plus général suivant : tout anneau principal est factoriel [10]. On a donc les implications suivantes pour les anneaux :

$$\text{corps} \Rightarrow \text{euclidien} \Rightarrow \text{principal} \Rightarrow \text{factoriel} \Rightarrow \text{intègre} .$$

10. La preuve est à peine plus difficile que dans le cas euclidien.

II.5 Entiers de Gauss et théorème des deux carrés

C'est bien beau d'avoir toute une théorie sur les anneaux euclidiens, mais les seuls exemples que nous avons sont l'anneau des entiers $\mathbb{Z}$, pour lequel la plupart de ces résultats sont connus, et les corps, pour lesquels tous ces résultats sont triviaux.

Carl Friedrich Gauss (1777-1855)

Billet de 10 Deutsche Mark à l'effigie de Gauss, en circulation entre 1991 et 2001

Le but de cette section est de présenter un autre exemple d'anneau eucidien, et d'appliquer la théorie de la section II.4 pour démontrer le *théorème des deux carrés* de Fermat. L'anneau en question porte le nom du plus illustre mathématicien de son temps, Carl Friedrich Gauss.

Considérons le sous-ensemble suivant des nombres complexes :

$$\mathbb{Z}[i] \coloneqq \{x + iy \,|\, x, y \in \mathbb{Z}\} \subset \mathbb{C}\,.$$

On vérifie très facilement qu'il s'agit d'un sous-anneau de $\mathbb{C}$, et donc d'un anneau intègre, dont le groupe des unités est donné par $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$. C'est l'anneau des *entiers de Gauss*.

Proposition II.18. *L'anneau $\mathbb{Z}[i]$ est un anneau euclidien.*

Démonstration. Comme on l'a vu, $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ et donc un anneau intègre. Définissons l'application $f\colon \mathbb{Z}[i] \to \mathbb{N}$ via $f(x+iy) = x^2 + y^2$, qui n'est autre que la restriction à $\mathbb{Z}[i]$ de l'application $z \mapsto |z|^2$. Notons que pour $x + iy \neq 0$, on a bien $f(x+iy) \in \{1, 2, \ldots\}$. De plus, pour $a, b \in \mathbb{Z}[i] \setminus \{0\}$,

$$f(ab) = |ab|^2 = |a|^2|b|^2 = f(a)f(b) \geq f(a)$$

puisque $f(b) \geq 1$. Reste donc à montrer que f satisfait la seconde condition dans la définition II.5.

Pour ce faire, fixons $a \in \mathbb{Z}[i]$ et $b \in \mathbb{Z}[i] \setminus \{0\}$, et tentons de trouver $q, r \in \mathbb{Z}[i]$ tels que $a = qb + r$, avec r satisfaisant $r = 0$ ou $f(r) < f(b)$. Notons que comme l'application f est définie sur $\mathbb{Z}[i]$ tout entier et satisfait $f(r) = 0 \Leftrightarrow r = 0$, cette condition sur r peut simplement s'écrire $f(r) < f(b)$. Comme a, b sont des nombres complexes non-nuls, on peut considérer leur quotient $\frac{a}{b} \in \mathbb{C}$, qui s'écrit donc $\frac{a}{b} = u + iv$ avec $u, v \in \mathbb{R}$. Il s'agit maintenant d'approximer au mieux ces réels avec des entiers : choisissons $x, y \in \mathbb{Z}$ tels que $|u - x| \leq \frac{1}{2}$ et $|v - y| \leq \frac{1}{2}$. Posons à présent $q \coloneqq x + iy \in \mathbb{Z}[i]$ et $r \coloneqq a - qb \in \mathbb{Z}[i]$, qui satisfont bien $a = qb + r$ par construction. De plus, on a

$$r = a - qb = b\left(\frac{a}{b} - q\right) = b\left((u+iv) - (x+iy)\right) = b\left((u-x) + i(v-y)\right)\,,$$

ce qui implique

$$f(r) = |r|^2 = |b|^2\left(|u-x|^2 + |v-y|^2\right) \leq |b|^2 \cdot \frac{1}{2} = \frac{f(b)}{2} < f(b)$$

puisque $|u - x| \leq \frac{1}{2}, |v - y| \leq \frac{1}{2}$ et $0 < f(b)$. Cela conclut la preuve. □

Ainsi, nous sommes maintenant en mesure d'appliquer les résultats de la section II.4 à l'anneau $A = \mathbb{Z}[i]$. Pour le théorème promis de théorie des nombres, nous aurons besoin du lemme suivant.

Lemme II.19. *Si p est un premier positif congru à 1 modulo 4, alors il existe $m \in \mathbb{Z}$ tel que $m^2 \equiv -1 \pmod{p}$.*

Démonstration. Soit p un nombre premier avec $p \equiv 1 \pmod 4$, et posons $m = \left(\frac{p-1}{2}\right)!$. Par hypothèse, l'entier $\frac{p-1}{2}$ est pair, d'où $(-1)^{\frac{p-1}{2}} = 1$. En utilisant ce fait et l'égalité $-k \equiv p - k \pmod p$, on obtient la congruence modulo p suivante :

$$\begin{aligned} m^2 &= 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)(-1)(-2)\cdots\left(-\frac{p-1}{2}\right) \\ &\equiv 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)(p-1)(p-2)\cdots(p-\frac{p-1}{2}) \\ &= 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\cdots(p-2)(p-1) = (p-1)!\,. \end{aligned}$$

La conclusion découle maintenant du théorème de Wilson. □

Voici enfin le résultat promis.

Théorème II.20: Théorème des deux carrés de Fermat

Un nombre premier $p > 2$ est somme de deux carrés si et seulement s'il est congru à 1 modulo 4.

RICHARD DEDEKIND (1831-1916)

Par exemple, ce théorème nous dit que les nombres premiers $3, 7, 11, 19, 23$ ne sont pas sommes de deux carrés, tandis que $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$, etc... le sont.

Il existe de très nombreuses preuves de ce résultat [11]. Celle que nous présentons ici date de 1894, et est due à l'un des fondateurs de la théorie algébrique des nombres, le mathématicien allemand RICHARD DEDEKIND.

Démonstration. Le fait qu'un nombre (premier) impair somme de deux carrés est congru à 1 modulo 4 est immédiat, et laissé en exercice 30.

Réciproquement, fixons p premier avec $p \equiv 1 \pmod 4$, et tentons de trouver $x, y \in \mathbb{Z}$ tels que $p = x^2 + y^2$. Par le lemme II.19, il existe $m \in \mathbb{Z}$ tel que $m^2 \equiv -1 \pmod p$. En d'autres termes, on a $p \mid (m^2 + 1)$ dans $\mathbb{Z} \subset \mathbb{Z}[i]$, d'où $p \mid (m^2 + 1) = (m + i)(m - i)$ dans $\mathbb{Z}[i]$. En revanche, on a $p \nmid m \pm i$ dans $\mathbb{Z}[i]$: sinon, on aurait $x + iy \in \mathbb{Z}[i]$ tel que $m \pm i = p(x + iy)$, d'où $y \in \mathbb{Z}$ avec $py = \pm 1$, ce qui est impossible car $p \neq \pm 1$. Comme p divise $(m + i)(m - i)$ mais ne divise pas $m \pm i$, cet entier n'est *pas* premier dans $\mathbb{Z}[i]$. Par la proposition II.18, cet anneau est euclidien ; la proposition II.15 peut donc être appliquée et implique que p n'est *pas* irréductible dans $\mathbb{Z}[i]$. Comme p n'est visiblement ni le zéro ni une unité de l'anneau euclidien $\mathbb{Z}[i]$, le théorème II.16 nous dit qu'il

11. Une preuve particulièrement remarquable est due à DON ZAGIER.

existe des irréductibles $p_1, \dots, p_n \in \mathbb{Z}[i]$ avec $n \geq 2$ et $p = p_1 \cdots p_n$. Cela implique l'égalité suivante dans $\mathbb{Z}$:

$$p^2 = f(p) = f(p_1 \cdots p_n) = f(p_1) \cdots f(p_n) \in \mathbb{Z}\,.$$

Notons que $f(p_j) > 1$ pour tout $j = 1, \dots, n$, car $f(a) = 1$ si et seulement si $a \in \mathbb{Z}[i]^*$ et p_j est irréductible. Appliquons à nouveau le théorème II.16, mais cette fois à l'élément p^2 de l'anneau euclidien $\mathbb{Z}$: l'unicité de la décomposition en irréductibles et le fait que $f(p_j) > 1$ pour tout j impliquent l'inégalité $n \leq 2$. En conclusion, on a $n = 2$, i.e. $p = p_1 p_2$ et $f(p_1) = f(p_2) = p$. En écrivant $p_1 = x + iy \in \mathbb{Z}[i]$, on a donc $x, y \in \mathbb{Z}$ avec $p = f(p_1) = f(x + iy) = x^2 + y^2$. □

II.6 Anneaux de polynômes

Le but de cette section est de présenter une famille importante d'anneaux (parfois euclidiens), appelés les anneaux de polynômes. La définition parfaitement formelle [12] se fait au détriment de la compréhensibilité, raison pour laquelle nous optons pour une définition semi-formelle.

Dans toute cette section, A désigne un anneau commutatif. On notera $A[X]$ l'ensemble des expressions de la forme

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

avec $n \geq 0$ et $a_0, a_1, \dots, a_n \in A$. On la notera $P = \sum_{i=0}^{n} a_i X^i = \sum_{i \geq 0} a_i X^i$, où il est entendu que $a_i = 0$ pour tout $i > n$. Deux telles expressions $P = \sum_{i \geq 0} a_i X^i$ et $Q = \sum_{i \geq 0} b_i X^i$ représentent le même élément de $A[X]$ si on a $a_i = b_i$ pour tout $i \geq 0$.

Pour $P = \sum_{i \geq 0} a_i X^i$ et $Q = \sum_{i \geq 0} b_i X^i$ dans $A[X]$, posons $P + Q = \sum_{i \geq 0} c_i X^i$ avec $c_i = a_i + b_i$ pour tout $i \geq 0$, ce qui définit bien un élément $P + Q$ de $A[X]$. Comme $(A, +)$ est un groupe abélien, on vérifie facilement qu'il en va de même pour $(A[X], +)$. En particulier, le neutre est donné par $0_{A[X]} = \sum_{i \geq 0} 0_A X^i$, appelé le *polynôme nul*.

Pour $P = \sum_{i \geq 0} a_i X^i$ et $Q = \sum_{j \geq 0} b_j X^j$ dans $A[X]$, posons $PQ = \sum_{k \geq 0} c_k X^k$ avec $c_k = \sum_{i+j=k} a_i b_j$ pour tout $k \geq 0$. Cela définit bien un élément $PQ \in A[X]$ [13]. On vérifie facilement que $(A[X], +, \cdot)$ est un anneau commutatif. En particulier, le neutre multiplicatif est donné par $1_{A[X]} = 1_A = \sum_{i \geq 0} a_i X^i$ avec $a_0 = 1_A$ et $a_i = 0$ pour $i > 0$.

Définition II.6

L'anneau $A[X]$ est **l'anneau des polynômes** (en la variable X) à coefficients dans A.

12. Une telle définition revient par exemple à considérer l'ensemble $A^{(\mathbb{N})}$ formé des suites $\{(a_i)_{i \geq 0} \mid a_i \in A$ pour tout $i \geq 0$ et il existe $n \geq 0$ tel que $a_i = 0$ pour tout $i > n\}$.

13. Cela fait également écho au *produit de Cauchy* défini dans le contexte des séries infinies.

Terminologie. Tout $P \in A[X] \setminus \{0\}$ peut s'écrire $P = a_0 + a_1X + \cdots + a_nX^n$ avec $a_n \neq 0$. L'entier $n \geq 0$ est appelé le *degré* de P, noté $\deg(P)$, et $a_n \in A \setminus \{0\}$ est le *coefficent dominant* de P. Par convention, le degré du polynôme nul est $-\infty$.

Remarques.

1. Notons que $A[X]$ contient le sous-anneau A, formé des polynômes de degré ≤ 0. Par conséquent, le groupe des unités $A[X]^*$ contient le sous-groupe A^*. Ces deux groupes sont-ils égaux ?

   Une autre conséquence est que si $A[X]$ est intègre, alors A est intègre. La réciproque est-elle valide ?
2. On a clairement l'inégalité $\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}$. Ce n'est pas une égalité en général : par exemple si $P = 1$ et $Q = -1$.
3. On vérifie facilement l'inégalité $\deg(PQ) \leq \deg(P) + \deg(Q)$. Là encore, ce n'est pas une égalité en toute généralité, mais un contre-exemple est moins évident : on peut considérer $P = Q = [2] \in \mathbb{Z}/4\mathbb{Z} \subset \mathbb{Z}/4\mathbb{Z}[X]$ qui satisfont $PQ = 0$, d'où $\deg(PQ) = -\infty < 0 + 0 = \deg(P) + \deg(Q)$.

   Existe-t-il une classe d'anneaux pour lesquels cette inégalité est un égalité ?

La proposition suivante répond quasi-simultanément aux trois questions ci-dessus.

Proposition II.21. *Si A est un anneau intègre, alors :*

(i) $A[X]^* = A^*$,

(ii) $A[X]$ *est intègre,*

(iii) $\deg(PQ) = \deg(P) + \deg(Q)$ *pour tous* $P, Q \in A[X]$.

Démonstration. Nous allons commencer par montrer le troisième point. Comme l'égalité est trivialement vraie si $P = 0$ ou $Q = 0$, on peut supposer P et Q non-nuls. Ils peuvent donc s'écrire $P = \sum_i a_i X^i$ avec coefficient dominant $a_n \neq 0$ et $Q = \sum_j b_j X^j$ avec coefficient dominant $b_m \neq 0$. On a alors $\sum_{i+j=k} a_i b_j = 0$ pour tout $k > m + n$ et $\sum_{i+j=m+n} a_i b_j = a_n b_m \neq 0$ puisque A est intègre. Ainsi, on a bien $\deg(PQ) = n + m = \deg(P) + \deg(Q)$.

Passons au second point. Comme A est intègre, c'est un anneau commutatif et non-nul, et il en va donc de même pour $A[X]$. Reste à voir que $A[X]$ n'a pas de diviseur de zéro. Supposons donc $P, Q \in A[X]$ non-nuls. On a donc $\deg(P) \geq 0$ et $\deg(Q) \geq 0$; par le troisième point, on a $\deg(PQ) = \deg(P) + \deg(Q) \geq 0$, et donc $PQ \neq 0$.

Pour montrer le premier point, rappelons que l'inclusion $A^* \subset A[X]^*$ est toujours valide ; il s'agit donc de vérifier l'autre inclusion. Considérons donc $P \in A[X]^*$. Par définition, il existe $Q \in A[X]$ tel que $PQ = 1_{A[X]} = 1_A$. Comme il s'agit d'un polynôme de degré zéro, le troisième point donne $\deg(P) + \deg(Q) = 0$. Comme P, Q sont non-nuls, on a forcément $\deg(P) = \deg(Q) = 0$. Ainsi, les polynômes P, Q sont des éléments du sous-anneau A qui satisfont $PQ = 1_A$, i.e. des éléments de A^*. □

Exemples.

1. Si $A = \mathbb{Z}$, alors $\mathbb{Z}[X]^* = \mathbb{Z}^* = \{\pm 1\}$. Ainsi, deux éléments de $\mathbb{Z}[X]$ sont associés si et seulement s'ils sont égaux au signe près. Il est donc naturel de choisir l'unique représentant à coefficient dominant positif dans la classe d'équivalence correspondante.
2. Si $A = K$ est un corps, alors $K[X]^* = K^* = K \setminus \{0\}$: les unités de $K[X]$ sont précisément les polynômes de degré 0. Ainsi, tout élément non-nul de $K[X]$ est associé à un unique polynôme de coefficient dominant 1.

Remarque. Tous les polynômes de degré 1 sont irréductibles dans $K[X]$.

⌜ En effet, considérons $P \in K[X]$ de degré 1. Cela nous assure déjà que P n'est ni nul ni une unité. Supposons $Q, T \in K[X]$ tels que $P = QT$. Comme $1 = \deg(P) = \deg(Q) + \deg(T)$, on a forcément $\deg(Q) = 0$ ou $\deg(T) = 0$, i.e. $Q \in K[X]^*$ ou $T \in K[X]^*$. Cela montre que P est irréductible. ⌟

Notons que cet énoncé est faux en général dans un anneau intègre : par exemple, le polynôme de degré 1 donné par $6X \in \mathbb{Z}[X]$ n'est pas irréductible, puisqu'il peut s'écrire comme le produit des polynômes 2 et $3X$ qui ne sont pas des unités de $\mathbb{Z}[X]$.

Tous les anneaux de polynômes ne sont pas euclidiens, mais c'est le cas si l'anneau de coefficients est un corps. C'est l'objet de l'énoncé suivant.

Théorème II.22

Si K est un corps, alors $K[X]$ est un anneau euclidien pour l'application [a] $\deg : K[X] \setminus \{0\} \to \{0, 1 \ldots\}$.

a. Au sens stricte, on voudrait une application à valeurs dans $\{1, 2, \ldots\}$, sans le zéro. Cela n'a aucune importance pour la théorie de la section II.4, mais pour ceux que cela chiffonne, il suffit de poser $f(P) = 2^{\deg(P)}$, qui a de plus le bon goût de satisfaire $f(0) = 0$ et $f(PQ) = f(P)f(Q)$.

Démonstration. Puisque K est un corps, c'est un anneau intègre et la proposition II.21 peut être appliquée : l'anneau $K[X]$ est bien intègre et pour tous $P, Q \in K[X] \setminus \{0\}$, on a $\deg(PQ) = \deg(P) + \deg(Q) \geq \deg(P)$. Cela montre que le degré satisfait la première condition dans la définition II.5.

Pour vérifier la seconde, considérons $P \in K[X]$ et $Q \in K[X] \setminus \{0\}$, et tentons de trouver $T, R \in K[X]$ tels que $P = TQ + R$ avec $R = 0$ ou $\deg(R) < \deg(Q)$. Pour fixer les notations, écrivons $Q = \sum_{j=0}^{m} b_j X^j$ avec $b_m \neq 0$, d'où $\deg(Q) = m$. Si $m = 0$, on a $Q = b_0 \in K^* = K[X]^*$, d'où l'existence de $Q^{-1} \in K[X]$: on pose alors $T = PQ^{-1}$ et $R = 0$, qui satisfont bien $TQ + R = PQ^{-1}Q + 0 = P$.

Supposons donc $m > 0$, et procédons par récurrence sur $\deg(P) =: n$.

- Pour $n < m$, on pose $T = 0$ et $R = P$, qui satisfont bien $TQ + R = 0 \cdot Q + P = P$ et $\deg(R) = \deg(P) = n < m = \deg(Q)$. Comme on a $m > 0$, cela donne le départ de la récurrence, en particulier les cas $n = -\infty$ et $n = 0$.

- Soit à présent $P = \sum_{i=1}^{n} a_i X^i$ avec $a_n \neq 0$ et $n \geq m$, et supposons l'énoncé vrai pour tout P_1 avec $\deg(P_1) < n$. L'idée est de soustraire de P le multiple de Q permettant d'éliminer le coefficient dominant de P, et donc de réduire son degré. Formellement, on pose

$$P_1 \coloneqq P - a_n b_m^{-1} X^{n-m} Q \in K[X]\,,$$

où l'on note que $b_m^{-1} \in K$ existe puisque b_m est non-nul et K est un corps [14], tandis que X^{n-m} est bien un élément de $K[X]$ car on a supposé $n \geq m$. Comme promis, le coefficient de degré n est $a_n - a_n b_m^{-1} b_m = 0$, d'où $\deg(P_1) < \deg(P)$. Par hypothèse de récurrence, il existe $T_1, R \in K[X]$ tels que $P_1 = T_1 Q + R$ avec $R = 0$ ou $\deg(R) < \deg(Q)$. On a donc

$$P = P_1 + a_n b_m^{-1} X^{n-m} Q = T_1 Q + R + a_n b_m^{-1} X^{n-m} Q = (\underbrace{T_1 + a_n b_m^{-1} X^{n-m}}_{=:T}) Q + R\,,$$

ce qui fournit $T, R \in K[X]$ tels que $P = TQ + R$.

Cela conclut la preuve. □

Exemple. En appliquant l'algorithme de division euclidienne donné par cette preuve pour les polynômes $P = X^5+3X^4+X^3-6X^2-X+1$ et $Q = X^3+2X^2+X-1$ dans $\mathbb{Q}[X]$, on obtient $T = X^2 + X - 2$ et $R = -2X^2 + 2X - 1$.

Remarques.

1. Il est à noter que la preuve ci-dessus fournit un algorithme explicite pour la division euclidienne, avec une unique solution.
2. On montrera en exercice 34 que l'anneau $\mathbb{Z}[X]$ n'est pas euclidien (en fait, pas principal). Ainsi, l'hypothèse que A est un corps est nécessaire.
3. En revanche, la preuve ci-dessus nous montre que la division euclidienne de P par Q est réalisable dans $A[X]$ avec A intègre pour autant que le coefficient dominant de Q soit une unité de A.

Ainsi, toute la théorie de la section II.4 s'applique aux anneaux $K[X]$ avec K un corps. En particulier, le théorème II.16 nous dit que tout polynôme de degré ≥ 1 se décompose en le produit de son coefficient dominant et d'irréductibles avec coefficents dominants égaux à 1, de manière unique à l'ordre près. Pour comprendre cette factorisation, il est utile de considérer la notion de *racine* d'un polynôme.

Pour ce faire, rappelons que pour tout anneau A et ensemble Y, l'ensemble $A^Y = \{f : Y \to A\}$ est un anneau pour les lois $(f+g)(x) = f(x) + g(x)$ et $(f \cdot g)(x) = f(x)g(x)$ pour $f, g \in A^Y$ et $x \in Y$. En particulier, on a l'anneau $A^A = \{f : A \to A\}$.

14. Voir la remarque 3 ci-dessous.

Notons encore que tout polynôme $P = \sum_{i=1}^{n} a_i X^i \in A[X]$ définit une *application polynomiale* $\overline{P}: A \to A$ via $\overline{P}(x) = \sum_{i=1}^{n} a_i x^i$, qui est donc un élément de l'anneau A^A. Finalement, on vérifie facilement que l'application

$$\varphi: A[X] \longrightarrow A^A, \quad P \longmapsto \overline{P}$$

est un homomorphisme d'anneaux [15].

Terminologie. Un élément $a \in A$ est une *racine* de $P \in A[X]$ si $\overline{P}(a) = 0$.

Proposition II.23. *Soit A un anneau intègre. Un élément $a \in A$ est une racine de $P \in A[X]$ si et seulement si $X - a$ divise P dans $A[X]$.*

Démonstration. Supposons tout d'abord que $P \in A[X]$ est tel que $(X - a) \mid P$ dans $A[X]$. Il existe donc $T \in A[X]$ tel que $P = (X - a)T$ dans $A[X]$. Comme l'application $A[X] \to A^A, P \mapsto \overline{P}$ ci-dessus est un homomorphisme d'anneaux, on obtient $\overline{P} = \overline{(X-a)T} = \overline{(X-a)} \cdot \overline{T}$ dans A^A. L'évaluation en $a \in A$ donne ainsi

$$\overline{P}(a) = (a - a) \cdot \overline{T}(a) = 0 \cdot \overline{T}(a) = 0\,,$$

et $a \in A$ est donc bien une racine de P.

Supposons réciproquement que $a \in A$ est une racine de $P \in A[X]$, et posons $Q = X - a \in A[X]$. Comme le coefficient dominant de Q est une unité de A (en l'occurrence 1), il est possible d'effectuer la division euclidienne de P par Q dans $A[X]$ comme expliqué en remarque 3 ci-dessus : il existe donc $T, R \in A[X]$ tels que $P = TQ + R$ et $\deg(R) < \deg(Q)$. Comme $\deg(Q) = 1$, le reste R est un élément du sous-anneau $A \subset A[X]$ formé des polynômes de degré ≤ 0 ; en particulier, l'application $\overline{R} \in A^A$ associée est une application constante (égale à $R \in A$). Via l'homomorphisme d'anneaux $A[X] \to A^A, P \mapsto \overline{P}$, on obtient l'égalité $\overline{P} = \overline{T} \cdot \overline{Q} + \overline{R}$ dans A^A. Comme $\overline{P}(a) = 0$ par hypothèse et $\overline{Q}(a) = 0$ par construction, l'évaluation en $a \in A$ donne

$$0 = \overline{P}(a) = \overline{T}(a) \cdot \overline{Q}(a) + \overline{R}(a) = \overline{R}(a) = R\,.$$

Le reste R étant zéro, on a donc $P = TQ$, d'où $Q = X - a$ divise P dans $A[X]$. □

Pour terminer ce chapitre, appliquons ces résultats à l'anneau $A = \mathbb{C}[X]$.

Exemple. Un polynôme dans $\mathbb{C}[X]$ est irréductible si et seulement s'il est de degré 1.

⌜ Le fait que tout polynôme de degré 1 est irréductible est vrai dans tout $K[X]$ avec K un corps, comme nous l'avons vu dans la remarque après la proposition II.21. Pour la réciproque, supposons par la contraposée que $P \in \mathbb{C}[X]$ est de degré $\deg(P) \neq 1$, et montrons qu'il n'est pas irréductible.

- Si $\deg(P) = -\infty$, alors $P = 0$, qui n'est pas irréductible par définition.

15. Notons néanmoins que cet homomorphisme n'est en général pas injectif (par exemple, dans le cas d'un anneau A fini, puisque $A[X]$ est infini et A^A fini), raison pour laquelle on ne peut pas assimiler un polynôme à l'application polynomiale associée.

- Si $\deg(P) = 0$, alors P est une unité par la remarque après la proposition II.21, et n'est donc pas irréductible.
- Si $\deg(P) \geq 2$, alors par le *théorème fondamental de l'algèbre*[16], le polynôme P possède une racine $\lambda \in \mathbb{C}$. Par la proposition II.23, on a $(X - \lambda) \mid P$ dans $\mathbb{C}[X]$, d'où $P = (X - \lambda)T$ avec $T \in \mathbb{C}[X]$ de degré $\deg(T) = \deg(P) - 1 \geq 1$, et donc pas une unité. Ainsi, P n'est pas irréductible dans $\mathbb{C}[X]$.

On a donc bien que P n'est jamais irréductible si son degré n'est pas 1. ⌟

Jean Le Rond d'Alembert (1717-1783)

Ainsi, tout polynôme irréductible dans $\mathbb{C}[X]$ est associé à un unique polynôme de la forme $X - \lambda$ avec $\lambda \in \mathbb{C}$.

⌜ Tout polynôme irréductible est de degré 1, et donc de la forme $P = a_0 + a_1 X$ avec $a_1 \neq 0$.

On a donc $P = u(X - \lambda)$ avec $\lambda = -a_0 a_1^{-1} \in \mathbb{C}$ et $u = a_1 \in \mathbb{C}^* = \mathbb{C}[X]^*$. ⌟

Par conséquent, le théorème II.16 appliqué à l'anneau euclidien $\mathbb{C}[X]$ donne l'énoncé suivant :

Tout polynôme $P \in \mathbb{C}[X]$ de degré $d \geq 1$ se décompose en

$$P = a(X - \lambda_1)\cdots(X - \lambda_d)\,,$$

de manière unique à l'ordre près, où $a \in \mathbb{C}^*$ est le coefficient dominant de P et $\lambda, \ldots, \lambda_d \in \mathbb{C}$ ses racines (pas forcément distinctes).

Exercices

1. Soient A_1, A_2 deux anneaux. On définit une addition et une multiplication sur le produit cartésien $A_1 \times A_2$ via

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \quad \text{et} \quad (a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2)$$

   pour tous $a_1, b_1 \in A_1$ et $a_2, b_2 \in A_2$.
   (i) Vérifier que $(A_1 \times A_2, +, \cdot)$ est un anneau. Quand est-il commutatif ?
   (ii) Montrer que $(A_1 \times A_2)^* = A_1^* \times A_2^*$.
   (iii) Montrer que si A_1 et A_2 sont non-nuls, alors $A_1 \times A_2$ a des diviseurs de zéro.

2. Soit A l'ensemble des nombres réels de la forme $a + b\sqrt{5}$ avec a, b rationnels. Montrer que A est un anneau. Est-ce un corps ?

3. Soient $(G, +)$ un groupe abélien, et $\mathrm{End}(G)$ l'ensemble des *endomorphismes* de G, c'est-à-dire des homomorphismes $\varphi : G \to G$. On définit une addition et une multiplication sur $\mathrm{End}(G)$ via

$$(\varphi + \psi)(g) = \varphi(g) + \psi(g) \quad \text{et} \quad (\varphi \cdot \psi)(g) = \varphi(\psi(g))$$

   pour tout $g \in G$.

16. Ce théorème a été énoncé par d'Alembert en 1746. Les premières preuves complètes ont été données par Gauss en 1799, 1815, 1816, 1849,...

(i) Vérifier que $(\mathrm{End}(G), +, \cdot)$ est un anneau.

(ii) Déterminer le groupe $\mathrm{End}(G)^*$ des unités de cet anneau.

(iii) Soit $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. L'anneau $\mathrm{End}(G)$ est-il commutatif ? Possède-t-il des diviseurs de zéro ?

4. Soit B un sous-anneau non-nul d'un anneau A. Parmi les affirmations suivantes, déterminer lesquelles sont vraies (donner une preuve) et lesquelles sont fausses (donner un contre-exemple).

(i) Le groupe des unités B^* est un sous-groupe de A^*.

(ii) Si A est intègre, alors B est intègre.

(iii) Si A est un corps, alors B est un corps.

(iv) Si B est intègre, alors A est intègre.

(v) Si B est un corps, alors A est un corps.

5. Pour tout anneau A, montrer que

$$Z = \{a \in A \mid ax = xa \text{ pour tout } x \in A\}$$

est un sous-anneau de A.

6. (i) Soit A un anneau intègre, et $a \neq 0 \in A$. Vérifier que l'application $A \to A$ donnée par $b \mapsto ab$ est injective.

(ii) À l'aide du point précédent, montrer qu'un anneau intègre fini est un corps.

7. Comme complément au théorème de Wilson, montrer que si $n > 4$ n'est pas un nombre premier, alors $(n-1)! \equiv 0 \pmod{n}$.

8. Soit A un anneau commutatif non-nul. Démontrer que A est un corps si et seulement si pour tous $a, b \in A$ avec $a \neq 0$, il existe un unique $x \in A$ avec $ax + b = 0$.

9. Donner un exemple d'une application $\varphi : \mathbb{Z} \to \mathscr{M}_2(\mathbb{R})$ non-triviale qui préserve l'addition et la multiplication mais n'est pas un homomorphisme d'anneaux.

10. Soit $A = \mathscr{M}_n(K)$ avec $K = \mathbb{R}$ ou $\mathbb{C}$ et $n \geq 1$. Montrer que pour toute matrice inversible $P \in \mathrm{GL}(n, K)$, l'application $\varphi : A \to A$ donnée par $\varphi(M) = PMP^{-1}$ est un isomorphisme d'anneaux.

11. Soit $\varphi : A \to A'$ une application entre deux anneaux telle que

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{et} \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

pour tout $a, b \in A$. Montrer que φ satisfait $\varphi(1_A) = 1_{A'}$ (et donc, est un homomorphisme d'anneaux) si l'une des deux conditions suivantes est satisfaite :

(i) φ est surjective,

(ii) A' est intègre et il existe $a \in A$ tel que $\varphi(a) \neq 0$.

12. Soient $\varphi : A \to A'$ un homomorphisme d'anneaux, et B' un sous-anneau de A'. Montrer que $\varphi^{-1}(B')$ est un sous-anneau de A.

13. À quels anneaux connus les anneaux $\mathrm{End}(\mathbb{Z})$ et $\mathrm{End}(\mathbb{Z}/n\mathbb{Z})$ sont-ils isomorphes ?

14. Soient A et A' deux anneaux de caractéristique n et n', respectivement. Quelle est la caractéristique de l'anneau $A \times A'$?

15. On sait que si A est un anneau de caractéristique nulle, il contient un sous-anneau isomorphe à $\mathbb{Z}$. En déduire que si K est un corps de caractéristique nulle, il contient un sous-anneau isomorphe à $\mathbb{Q}$. (Comme K et $\mathbb{Q}$ sont des corps, on parle de *sous-corps*.)

    Indication : Considérer l'application $\varphi\colon \mathbb{Q} \to K$ donnée par $\varphi(\frac{m}{n}) = \epsilon(m)\epsilon(n)^{-1}$, avec ϵ l'unique homomorphisme $\epsilon\colon \mathbb{Z} \to K$.

16. Montrer que l'intersection de deux idéaux est un idéal. Est-ce toujours le cas pour l'intersection d'une famille quelconque d'idéaux ?

17. Montrer qu'un anneau commutatif A non-nul est un corps si et seulement si les seuls idéaux $I \subset A$ sont $I = \{0\}$ et $I = A$.

18. Montrer que si $\varphi\colon A \to A'$ est un homomorphisme d'anneaux avec A un corps et A' non-nul, alors φ est injectif.

19. Soient $\varphi\colon A \to A'$ un homomorphisme d'anneaux, et I un idéal de A'. Montrer que $\varphi^{-1}(I)$ est un idéal de A.

20. Soient A un anneau commutatif et I un idéal de A. Posons

$$r(I) = \{a \in A \,|\, \text{il existe } n \in \mathbb{N} \text{ tel que } a^n \in I\}\,.$$

    Montrer que $r(I)$ est un idéal de A qui contient I, et que $r(r(I)) = r(I)$.

21. Soit A un anneau quelconque, et $\epsilon\colon \mathbb{Z} \to A$ l'homomorphisme d'anneaux associé. Pour quels $m \in \mathbb{Z}$ cet homomorphisme passe-t-il au quotient pour définir un homomorphisme $\bar{\epsilon}\colon \mathbb{Z}/m\mathbb{Z} \to A$?

22. Soit A un anneau commutatif. Vérifier les énoncés suivants, pour tous $a, b, c \in A$:
    (i) Si $a \mid b$ et $b \mid c$, alors $a \mid c$.
    (ii) Si $a \mid b$ et $a \mid c$, alors $a \mid (b + c)$.
    (iii) Si $a \mid b$, alors $a \mid bx$ pour tout $x \in A$.
    (iv) Si $a \mid b$, alors $au \mid b$ pour toute unité $u \in A^*$.
    (v) On a $a \mid b$ si et seulement si $(b) \subset (a)$.

23. Deux éléments a, b d'un anneau commutatif A sont dits *associés* s'il existe une unité $u \in A^*$ telle que $b = au$.
    (i) Montrer qu'il s'agit d'une relation d'équivalence sur A.
    (ii) Montrer que dans le cas d'un anneau intègre, la relation "a divise b" définit une relation d'ordre sur l'ensemble des classes d'équivalence correspondantes.

24. Montrer que dans un anneau commutatif quelconque, le seul plus grand commun diviseur de $a = 0$ et $b = 0$ est donné par $\mathrm{pgcd}(0, 0) = 0$.

25. Donner deux preuves de l'affirmation ci-dessous, l'une en utilisant les définitions, l'autre au moyen de la proposition II.13 et de l'exercice 17 :
    Dans un corps K, un plus grand commun diviseur de a et b est donné par 0 *si $a = b = 0$, et par tout élément de $K \setminus \{0\}$ sinon.*

26. Soit A un anneau intègre muni d'une application $g\colon A\setminus\{0\}\to\{1,2,\ldots\}$ satisfaisant la condition de la division euclidienne (seconde condition dans la définition II.5). Montrer qu'alors, l'anneau A est euclidien via l'application $f\colon A\setminus\{0\}\to\{1,2,\ldots\}$ définie par
$$f(a)=\min_{x\in A\setminus\{0\}} g(xa)\,.$$
Indication : Pour vérifier que f satisfait la seconde condition, fixer $a,b\in A\setminus\{0\}$, considérer $c\in A\setminus\{0\}$ tel que $f(b)=g(cb)$, et appliquer l'hypothèse sur g aux éléments ac et bc.

27. Rappelons qu'un *plus petit commun multiple* de a et b dans un anneau A est un élément $c\in A$ tel que $a\mid c$ et $b\mid c$, et si $a\mid x$ et $b\mid x$ pour un $x\in A$, alors $c\mid x$.
    (i) Vérifier que si A est intègre, alors deux plus petits communs multiples de a et b sont associés.
    (ii) Montrer que si A est euclidien, un plus petit commun multiple de a et b existe et est donné par un générateur de l'idéal $(a)\cap(b)$.
    (iii) Montrer que si d est un plus grand commun diviseur et c un plus petit commun multiple de a et b dans A euclidien (ou plus généralement, dans A intègre), alors cd et ab sont associés.
    (iv) Calculer le plus petit commun multiple de deux éléments d'un corps.

28. Dans un anneau euclidien, montrer que les éléments $a\in A\setminus\{0\}$ qui minimisent la fonction $f\colon A\setminus\{0\}\to\{1,2,\ldots\}$ sont précisément les unités de A.
    En supposant que f satisfait $f(ab)=f(a)f(b)$, montrer que cette valeur minimale est 1.

29. Soient p un nombre premier et I un idéal de $\mathbb{Z}$ tel que $p\mathbb{Z}\subset I\subset\mathbb{Z}$. Montrer que $I=p\mathbb{Z}$ ou $I=\mathbb{Z}$.

30. Démontrer la réciproque du théorème des deux carrés de Fermat : si p est un nombre (premier) impair qui est somme de deux carrés, alors p est congru à 1 modulo 4.

31. (i) Vérifier que pour tout $d\in\mathbb{N}$,
$$\mathbb{Z}[\sqrt{-d}]:=\{x+y\sqrt{-d}\,|\,x,y\in\mathbb{Z}\}$$
est un sous-anneau de $\mathbb{C}$, et donc un anneau intègre.
    (ii) Montrer que les unités de cet anneau sont les éléments $z=x+y\sqrt{-d}$ tels que $N(z):=x^2+dy^2=1$.
    (iii) Dans le cas $d=5$, montrer (à l'aide de la fonction N) que l'élément 3 est irréductible dans $\mathbb{Z}[\sqrt{-5}]$.
    (iv) À l'aide de la factorisation $6=(1-\sqrt{-5})(1+\sqrt{-5})$, montrer que 3 n'est pas premier dans $\mathbb{Z}[\sqrt{-5}]$.
    (v) En déduire que $\mathbb{Z}[\sqrt{-5}]$ n'est pas un anneau euclidien.

32. En s'inspirant du cas $d=1$ vu en proposition II.18, démontrer que l'anneau
$$\mathbb{Z}[\sqrt{-d}]:=\{x+y\sqrt{-d}\,|\,x,y\in\mathbb{Z}\}$$
est aussi euclidien pour $d=2$.

33. Soient K un corps et $P \in K[X]$ un polynôme de degré 3. Montrer que si P n'est pas irréductible, alors il possède une racine dans K.

34. Dans $A = \mathbb{Z}[X]$, considérons l'ensemble $I = \{2P + XQ \mid P, Q \in A\}$.
    (i) Vérifier qu'il s'agit d'un idéal de A qui ne coïncide pas avec A tout entier.
    (ii) Démontrer que I n'est pas de la forme $(x) = xA$ pour un $x \in A$.
    (iii) En conclure que A n'est pas un anneau euclidien.

35. Le but de cet exercice est d'étudier *l'algorithme d'Euclide* dans le cadre d'un anneau euclidien A arbitraire.
    (i) Étant donnés $a \in A$ et $b \in A \setminus \{0\}$, montrer que si l'on applique successivement la division euclidienne

$$\begin{aligned} a &= q_1 b + r_1, \quad \text{avec} \quad f(r_1) < f(b) \\ b &= q_2 r_1 + r_2, \quad \text{avec} \quad f(r_2) < f(r_1) \\ r_1 &= q_3 r_2 + r_3, \quad \text{avec} \quad f(r_3) < f(r_2) \\ &\cdots \end{aligned}$$

    on doit finir par obtenir $r_n = 0$
    (ii) Montrer que r_{n-1} est alors un plus grand commun diviseur de a et b.
    (iii) Utiliser cet algorithme pour écrire ce plus grand commun diviseur comme combinaison de a et b.
    (iv) Appliquer cet algorithme pour calculer le plus grand commun diviseur de 3347 et 1151 dans $\mathbb{Z}$, et l'écrire comme combinaison linéaire de ces deux entiers.
    (v) Faire de même pour calculer un plus grand commun diviseur de $X^5 - 1$ et $X^3 - 1$ dans $\mathbb{Q}[X]$, et l'écrire comme combinaison linéaire de ces deux polynômes.

36. Le but de cet exercice est de comprendre les éléments irréductibles de l'anneau $\mathbb{R}[X]$, ainsi que la décomposition en irréductibles d'un polynôme $P \in \mathbb{R}[X]$.
    (i) Vérifier que si $\lambda \in \mathbb{C}$ est une racine d'un polynôme $P \in \mathbb{R}[X]$, alors le conjugué complexe $\overline{\lambda}$ est aussi racine de P.
    (ii) En déduire que tout élément irréductible de degré 2 dans $\mathbb{R}[X]$ est associé à un unique polynôme de la forme $X^2 - 2aX + (a^2 + b^2)$ avec $a \in \mathbb{R}$ et $b \in \mathbb{R}^*$, ou de manière équivalente, de la forme

$$X^2 + a_1 X + a_0$$

    avec $a_1^2 - 4a_0 < 0$.
    (iii) Donner une classification des éléments irréductibles de $\mathbb{R}[X]$ à association près.
    (iv) Écrire la décomposition en irréductibles d'un polynôme $P \in \mathbb{R}[X]$ à partir de ses racines (dans $\mathbb{C}$).

37. Montrer que l'anneau quotient

$$\mathbb{R}[X]/(X^2 + 1)$$

est isomorphe au corps $\mathbb{C}$ des nombres complexes.

Chapitre III: Espaces vectoriels et modules

En Algèbre I automne, vous avez étudié l'algèbre linéaire sur $\mathbb{R}$ et $\mathbb{C}$. Le but de ce chapitre est d'étendre cette théorie de deux manières.

Dans un premier temps, en sections III.1 et III.2, nous allons montrer que nombre de ces résultats s'étendent aux espaces vectoriels sur un corps quelconque, en particulier le théorème de classification des espaces vectoriels de dimension finie. Comme cette généralisation ne présente pas de difficulté majeure, nous allons la traiter de manière relativement concise, tout en restant le plus complet possible.

Dans un second temps, en section III.3 et III.4, nous allons initier l'extension de cette théorie aux "espaces vectoriels sur un anneau A", appelés *A-modules*. Comme vous le verrez, l'abandon de l'axiome faisant d'un anneau un corps enrichit et complexifie considérablement la théorie. Néanmoins, nous montrerons que dans le cas où A est un anneau euclidien, un théorème de classification peut être obtenu. Ce résultat illustre à merveille le pouvoir unificateur de l'algèbre formel, puiqu'il donne en un seul énoncé et une seule preuve :

- le théorème de classification des espaces vectoriels de dimension finie sur K (pour $A = K$ un corps),
- le théorème de classification des groupes abéliens finis (pour $A = \mathbb{Z}$),
- la réduction de Jordan des endomorphismes d'un $\mathbb{C}$-espace vectoriel de dimension finie (pour $A = \mathbb{C}[X]$).

Notons d'ores et déjà que la section III.4, qui traite de ce résultat, ne fait pas partie du champ de l'examen et est proposée "pour votre culture".

III.1 Espaces vectoriels et applications linéaires

Guiseppe Peano (1858-1932)

La première définition axiomatique d'un espace vectoriel semble remonter à 1888, et est due à Guiseppe Peano. La voici.

Définition III.1

Soit K un corps, et soit E un ensemble muni d'une loi de composition interne

$$E \times E \longrightarrow E, \quad (v, w) \longmapsto v + w$$

et d'une loi de composition externe

$$K \times E \longrightarrow E, \quad (\lambda, v) \longmapsto \lambda \cdot v\,.$$

On dit que E est **espace vectoriel sur** K (ou K**-espace vectoriel**) s'il satisfait les axiomes suivants :

$(E1)$ $(E,+)$ est un groupe abélien,

$(E2)$ $\lambda \cdot (\mu \cdot v) = (\lambda\mu) \cdot v$,

$(E3)$ $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$,

$(E4)$ $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$,

$(E5)$ $1_K \cdot v = v$,

pour tous $\lambda, \mu \in K$ et $v, w \in E$.

Remarques et terminologie.

1. Les éléments de E sont appelés *vecteurs* et ceux de K *scalaires*.

2. Naturellement, la loi de composition interne est appelée *l'addition*, et toutes les remarques, notations, terminologies et règles de calcul vues pour les groupes abéliens en section I.1 se transposent verbatim. En particulier, nous adopterons les notations $0 = 0_E$ pour le neutre additif et $-v$ pour l'inverse additif, ainsi que $n \cdot v$ pour la $n^{\text{ième}}$ puissance [1] additive de $v \in E$ pour $n \in \mathbb{Z}$.

3. La loi de composition externe est appelée *multiplication par un scalaire*. Comme d'habitude, on aura tendance à la noter simplement $\lambda \cdot v =: \lambda v$ pour $\lambda \in K$ et $v \in E$.

4. Pour $K = \mathbb{R}$ ou $\mathbb{C}$, on retrouve la définition vue en automne. Mais nous travaillons à présent sur un corps K quelconque, par exemple $\mathbb{Q}, \mathbb{F}_p, \mathbb{Q}[\sqrt{-5}], \ldots$

5. On a les règles de calcul suivantes, valides pour tous $\lambda \in K$ et $v \in E$:
   (i) $\lambda \cdot 0_E = 0_E$ et $0_K \cdot v = 0_E$.
   (ii) $(-\lambda)v = \lambda(-v) = -(\lambda v)$, que l'on notera donc simplement $-\lambda v$.
   (iii) Si $\lambda \cdot v = 0_E$, alors $\lambda = 0_K$ ou $v = 0_E$.

   ⌜ La preuve des deux premiers points ressemble beaucoup à celle des règles de calcul correspondantes dans les anneaux, et est laissée comme exercice. Pour montrer le troisième, considérons $\lambda \in K$ et $v \in E$ tels que $\lambda \cdot v = 0_E$, et supposons $\lambda \neq 0_K$.

1. On pourrait penser que cette notation entre en conflit avec celle de la loi de composition externe, mais il n'en est rien. En effet, pour tout $n \in \mathbb{Z}$, l'élément $\epsilon(n) \in K$ (pour ϵ l'unique homomorphisme d'anneau $\mathbb{Z} \to K$) satisfait $\epsilon(n) \cdot v = n \cdot v$ pour tout $v \in E$. C'est une conséquence directe des axiomes pour $n > 0$, et des règles de calcul (i) et (ii) ci-dessous pour $n = 0$ et $n < 0$.

Comme K est un corps[2], il existe $\lambda^{-1} \in K$ tel que $\lambda^{-1}\lambda = 1_K$. Ainsi, on a

$$v \overset{(E5)}{=} 1_K \cdot v = (\lambda^{-1}\lambda) \cdot v \overset{(E2)}{=} \lambda^{-1} \cdot (\lambda \cdot v) = \lambda^{-1} \cdot 0_E \overset{(i)}{=} 0_E\,,$$

ce qu'il fallait démontrer. ⌟

Exemples (d'espaces vectoriels)**.**

1. Les $\mathbb{F}_2$-espaces vectoriels coïncident avec les groupes abéliens dont tous les éléments non-neutres sont d'ordre 2. C'est le sujet de l'exercice 1.

2. Soient A un anneau, et $K \subset A$ un sous-anneau qui est un corps : on parle de *sous-corps* de A. Alors, l'anneau A est un K-espace vectoriel.

   ⌜ L'axiome $(A1)$ pour l'anneau A est équivalent à l'axiome $(E1)$ pour l'espace vectoriel, tandis que l'axiome $(A2)$ implique $(E2)$, $(A4)$ implique $(E3)$ et $(E4)$, et $(A3)$ est équivalent à $(E5)$. ⌟

   En particulier, tout corps K est un K-espace vectoriel.
   Aussi, comme $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des sous-anneaux qui sont des corps, $\mathbb{R}$ et $\mathbb{C}$ sont des $\mathbb{Q}$-espaces vectoriels et $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel.
   Comme autre famille d'exemples, rappelons[3] que si A est un anneau de caractéristique p premier, alors il contient un sous-anneau isomorphe à $\mathbb{Z}/p\mathbb{Z}$, qui n'est autre que le corps $\mathbb{F}_p$. Ainsi, tout anneau de caractéristique p est un $\mathbb{F}_p$-espace vectoriel. (Par exemple : $\mathbb{F}_p, \mathbb{F}_p[X], \dots$)
   Similairement, tout anneau A de caractéristique nulle contient un sous-anneau isomorphe à $\mathbb{Z}$. Si cet anneau A est un corps, alors on vérifie qu'il contient un sous-corps isomorphe à $\mathbb{Q}$. Ainsi, tout corps de caractéristique nulle est un $\mathbb{Q}$-espace vectoriel. (Par exemple : $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[\sqrt{5}], \dots$)

3. Soit K un corps quelconque, et $n \geq 1$ un entier. Alors, on vérifie facilement que le produit cartésien $K^n = \overbrace{K \times \cdots \times K}^{n}$ est un K-espace vectoriel pour les lois données par

   $$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$
   $$\lambda \cdot (x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n)\,.$$

   Par convention, on pose $K^0 = \{0\}$.

4. Pour K un corps quelconque, l'ensemble $K[X]$ est un K-espace vectoriel pour les lois

   $$\sum_i a_i X^i + \sum_i b_i X^i = \sum_i (a_i + b_i) X^i \quad \text{et} \quad \lambda \cdot \sum_i a_i X^i = \sum_i (\lambda a_i) X^i\,.$$

2. Cette hypothèse est utilisée très rarement, mais de manière absolument cruciale, voir section III.3.
3. Voir la fin de la section II.3.

Ce fait se vérifie facilement, et peut également être vu comme une conséquence de l'exemple 2 puisque $K[X]$ est un anneau qui contient K comme sous-corps.
Similairement, pour tout $n \geq 0$ fixé, l'ensemble

$$K_n[X] = \{P \in K[X] \,|\, \deg(P) < n\}$$

est un K-espace vectoriel pour ces mêmes lois [4].

5. Pour K un corps quelconque et $n, m \geq 1$ fixés, l'ensemble $\mathscr{M}_{n,m}(K)$ des matrices $n \times m$ à coefficients dans K est un K-espace vectoriel pour les lois évidentes.

6. Si $E_1, \ldots, E_n$ sont des K-espaces vectoriels, alors l'ensemble $E_1 \times \cdots \times E_n$ est un K-espace vectoriel pour les lois

$$(v_1, \ldots, v_n) + (w_1, \ldots, w_n) = (v_1 + w_1, \ldots, v_n + w_n)$$
$$\lambda \cdot (v_1, \ldots, v_n) = (\lambda \cdot v_1, \ldots, \lambda \cdot v_n)\,.$$

Il est noté $E_1 \oplus \cdots \oplus E_n$, et appelé *la somme directe (externe)* de $E_1, \ldots, E_n$. Notons que dans le cas $E_1 = \cdots = E_n = K$, on retrouve l'exemple 3 ci-dessus.

Terminologie. Un sous-ensemble F non-vide de E est un *sous-espace vectoriel* de E s'il satisfait :

(i) pour tous $v, w \in F$, on a $v + w \in F$,
(ii) pour tous $\lambda \in K$ et $v \in F$, on a $\lambda v \in F$.

Remarques.

1. Un sous-ensemble $F \subset E$ est un sous-espace vectoriel de E si et seulement s'il est un espace vectoriel pour la restriction des lois de E à F.
2. Un sous-espace vectoriel $F \subset E$ est en particulier un sous-groupe de $(E, +)$.

Exemples (de sous-espaces vectoriels)**.**

1. Tout espace vectoriel E contient les sous-espaces vectoriels $\{0\}$ et E.
2. Si $K \subset B \subset A$ est une suite de sous-anneaux avec K un corps, alors A et B sont des K-espaces vectoriels (par l'exemple 2 ci-dessus), et B est un sous-espace vectoriel de A.
3. Pour tous $n \leq m$, l'espace vectoriel $K_n[X]$ est un sous-espace vectoriel de $K_m[X]$, et de $K[X]$.
4. L'intersection de deux sous-espaces vectoriels est encore un sous-espace vectoriel.
5. Si F_1, F_2 sont deux sous-espaces vectoriels de E, alors

$$F_1 + F_2 \coloneqq \{v_1 + v_2 \,|\, v_1 \in F_1,\ v_2 \in F_2\}$$

est un sous-espace vectoriel de E.

4. Mais ce n'est pas un anneau pour $n > 1$.

Définition III.2

Soient E, E' deux espaces vectoriels sur un même corps K. Une application $f : E \to E'$ est dite **K-linéaire** (ou simplement **linéaire**) si elle satisfait

$$f(v+w) = f(v) + f(w) \quad \text{et} \quad f(\lambda v) = \lambda f(v)$$

pour tous $v, w \in E$ et $\lambda \in K$.

Remarques et terminologie.

1. Bien entendu, il faut comprendre une application linéaire comme un "homomorphisme d'espaces vectoriels".
2. La composition de deux applications linéaires est à nouveau linéaire.
3. Par définition, une application linéaire $f : E \to E'$ fournit un homomorphisme de groupes $f : (E, +) \to (E', +)$. Par conséquent, tous les résultats vus en section I.3 s'appliquent. En particulier, on peut considérer le noyau $\mathrm{Ker}(f) = \{v \in E \mid f(v) = 0\}$ et l'image $\mathsf{Im}(f) = f(E)$ de f, qui sont des sous-groupes de $(E, +)$ et $(E', +)$, respectivement ; de plus, f est injective si et seulement si $\mathrm{Ker}(f) = \{0\}$. On vérifie facilement que le noyau et l'image de f sont en fait des sous-espaces vectoriels.
4. Un *isomorphisme d'espaces vectoriels* (ou *isomorphisme linéaire*) est une application linéaire $f : E \to E'$ bijective [5]. On dit alors que E et E' sont *isomorphes*, noté $E \simeq E'$.

   Les cinq remarques faites en section I.3 sur les isomomorphismes de groupes se transposent presque mot à mot aux isomorphismes linéaires.

Exemples (d'applications linéaires)**.**

1. *L'application nulle* $f : E \to E'$ donnée par $f(v) = 0$ pour tout $v \in E$ est linéaire.
2. Si $F \subset E$ est un sous-espace vectoriel, alors l'inclusion $f : F \to E$ est linéaire.
3. Pour $\lambda \in K$ fixé, l'application $\mathrm{ev}_\lambda : K[X] \to K$ donnée par $\mathrm{ev}_\lambda(P) = \overline{P}(\lambda)$ est linéaire. Son image est K, et son noyau est $(X - \lambda) \subset K[X]$, l'idéal principal de $K[X]$ engendré par $X - \lambda$.

   ⌜ Tout $\mu \in K$ peut-être réalisé comme $\mathrm{ev}_\lambda(P)$ pour un certain $P \in K[X]$: il suffit de choisir $P = \mu$, le polynôme constant égal à μ. Quant au noyau, il est par définition constitué des polynômes $P \in K[X]$ tels que λ est une racine de P ; par la proposition II.23, ce sont les polynômes $P \in K[X]$ tels que $X - \lambda$ divise P, i.e. les éléments de l'idéal $(X - \lambda) \subset K[X]$. ⌟

Terminologie. Un espace vectoriel E est la *somme directe interne* des sous-espaces vectoriels $F_1, \ldots, F_n \subset E$ si tout vecteur $v \in E$ s'écrit de manière unique comme $v = v_1 + \cdots + v_n$ avec $v_1 \in F_1, \ldots, v_n \in F_n$.

5. On vérifie facilement que son inverse est également linéaire.

Remarque. On vérifie facilement que E est somme directe interne de F_1, F_2 si et seulement si $F_1 + F_2 = E$ et $F_1 \cap F_2 = \{0\}$.

Le lien entre somme directe interne et externe est donné par la proposition suivante (voir l'exercice 5 pour la réciproque).

Proposition III.1. *Si E est la somme directe interne des sous-espaces vectoriels $F_1, \dots, F_n \subset E$, alors E est isomorphe à la somme directe externe $F_1 \oplus \cdots \oplus F_n$ des espaces vectoriel $F_1, \dots, F_n$.*

Démonstration. Soit donc E un espace vectoriel, et soient $F_1, \dots, F_n \subset E$ des sous-espaces vectoriels tels que E est la somme directe interne des F_i. Posons

$$f : F_1 \oplus \cdots \oplus F_n \longrightarrow E, \quad f(v_1, \dots, v_n) = v_1 + \cdots + v_n \,.$$

Cette application est linéaire : en effet, pour tous $(v_1, \dots, v_n)$ et $(w_1, \dots, w_n)$ dans $F_1 \oplus \cdots \oplus F_n$ et tout $\lambda \in K$, on a

$$\begin{aligned} f((v_1, \dots, v_n) + (w_1, \dots, w_n)) &= f(v_1 + w_1, \dots, v_n + w_n) \\ &= (v_1 + w_1) + \cdots + (v_n + w_n) \\ &= (v_1 + \cdots + v_n) + (w_1 + \cdots + w_n) \\ &= f(v_1, \dots, v_n) + f(w_1, \dots, w_n) \,, \end{aligned}$$

et

$$\begin{aligned} f(\lambda(v_1, \dots, v_n)) = f(\lambda v_1, \dots, \lambda v_n) &= (\lambda v_1) + \cdots + (\lambda v_n) \\ &= \lambda(v_1 + \cdots + v_n) = \lambda f(v_1, \dots, v_n) \,. \end{aligned}$$

De plus, f est surjective puisque tout $v \in E$ s'écrit $v = v_1 + \dots v_n$ avec $v_i \in F_i$, et est injective puisque cette écriture est unique. Ainsi, l'application f est un isomorphisme, et l'on a bien $E \simeq F_1 \oplus \cdots \oplus F_n$. □

Remarque. Si F est un sous-espace vectoriel d'un espace vectoriel E sur K, alors on a en particulier que $(F, +)$ est un sous-groupe (normal) de $(E, +)$. Ainsi, on peut construire le groupe abélien quotient $(E/F, +)$ via $[v] + [w] = [v + w]$. De plus, on vérifie facilement que E/F est un espace vectoriel pour la loi externe donnée par $\lambda \cdot [v] = [\lambda \cdot v]$ pour $v \in E$ et $\lambda \in K$: c'est *l'espace vectoriel quotient.*

Tous les résultats vus aux sections I.8 et II.3 s'adaptent facilement. En particulier, la projection canonique $\pi : E \to E/F$ est une application linéaire de noyau F. Aussi, toute application linéaire $f : E \to E'$ définit un isomorphisme linéaire

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

C'est le sujet de l'exercice 6.

III.2 Classification des espaces vectoriels

Le but de cette section est de démontrer le résultat fondamental de la théorie du point de vue de l'algèbre formelle, à savoir la classification des espaces vectoriels de dimension finie (théorème III.8). Nous montrerons également le théorème du rang (théorème III.9) qui, à ce stade, tombera comme un fruit mûr.

Commençons par un peu de terminologie.

Terminologie. Soit E un K-espace vectoriel

- Pour $v_1, \dots, v_n \in E$, tout vecteur de la forme $\lambda_1 v_1 + \cdots + \lambda_n v_n$ avec $\lambda_1, \dots, \lambda_n \in K$ est appelé *combinaison linéaire* de $v_1, \dots, v_n$.
- Pour S un sous-ensemble non-vide de E, on note $\mathrm{Vect}(S)$ l'ensemble des combinaisons linéaires d'éléments de S, i.e.

$$\mathrm{Vect}(S) = \{\lambda_1 v_1 + \cdots + \lambda_n v_n \,|\, \lambda_1, \dots, \lambda_n \in K \text{ et } v_1, \dots, v_n \in S\}\,.$$

  Par convention, on pose $\mathrm{Vect}(\varnothing) = \{0\}$.

  On parle du *sous-espace de E engendré par S*.
- Si $\mathrm{Vect}(S) = E$, on dit que S est une *famille génératrice* de E.

Lemme III.2. *Le sous-ensemble $\mathrm{Vect}(S) \subset E$ est le plus petit sous-espace vectoriel de E contenant S.*

Démonstration. Pour vérifier que $\mathrm{Vect}(S)$ est un sous-espace vectoriel, notons d'abord qu'il est non-vide puisqu'il contient 0 (via $0 = 0 \cdot v$ avec $v \in S$ si S est non-vide, et par convention si S est vide). De plus, on a trivialement que la somme de deux combinaisons linéaires d'éléments de S est encore une telle combinaison, tandis que si $v \in \mathrm{Vect}(S)$ et $\lambda \in K$, alors il existe $v_1, \dots, v_n \in S$ et $\lambda_1, \dots, \lambda_n \in K$ tels que $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$, d'où

$$\lambda v = \lambda(\lambda_1 v_1 + \cdots + \lambda_n v_n) = (\lambda\lambda_1)v_1 + \cdots + (\lambda\lambda_n)v_n \in \mathrm{Vect}(S)\,.$$

Ainsi, $\mathrm{Vect}(S)$ est bien un sous-espace vectoriel de E. Ce sous-espace contient S, puisque pour tout $v \in S$, on a $v = 1 \cdot v \in \mathrm{Vect}(S)$. Finalement, si F est un sous-espace vectoriel de E avec $F \supset S$, alors par définition d'un sous-espace, F contient toutes les combinaisons linéaires d'éléments de S, d'où $F \supset \mathrm{Vect}(S)$. Ainsi, $\mathrm{Vect}(S)$ est bien le plus petit sous-espace de E contenant S. □

Terminologie. Un espace vectoriel E est dit *de-dimension-finie*[6] *(sur K)* s'il admet une famille génératrice finie, i.e. s'il existe un sous-ensemble fini $S \subset E$ tel que $E = \mathrm{Vect}(S)$.

Exemples (de familles génératrices)**.**

1. L'espace trivial est de-dimension-finie (sur tout K), puisque $\{0\} = \mathrm{Vect}(\varnothing)$.
2. L'espace vectoriel $\mathbb{C}$ est de-dimension-finie sur $\mathbb{R}$, puisque $\mathbb{C} = \mathrm{Vect}(\{1, i\})$.

6. On enlèvera les tirets lorsque la notion de dimension aura été vue ; pour l'instant, il s'agit purement d'une terminologie.

3. L'espace K^n est de-dimension-finie sur K puisque $K^n = \mathrm{Vect}(\{e_1, \ldots, e_n\})$, où $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$.
4. Comme on a $K_n[X] = \mathrm{Vect}(\{1, X, \ldots, X^{n-1}\})$, l'espace $K_n[X]$ est de-dimension-finie sur K.
5. En revanche, l'espace $K[X]$ n'est *pas* de-dimension-finie sur K.

   ⌜ Pour tout $S \subset K[X]$ fini, on a $\mathrm{Vect}(S) \subset K_{n+1}[X]$ avec $n = \max\{\deg(P) \mid P \in S\}$, d'où $\mathrm{Vect}(S) \subsetneq K[X]$. ⌟

   L'espace $K[X]$ admet la famille génératrice infinie $S = \{1, X, X^2, \ldots\}$.

Terminologie. Soit E un K-espace vectoriel. On dit que $S \subset E$ est constitué de vecteurs *linéairement indépendants (sur K)* si pour tous $v_1, \ldots, v_n \in S$, on a

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0 \text{ avec } \lambda_1, \ldots, \lambda_n \in K \;\Rightarrow\; \lambda_1 = \cdots = \lambda_n = 0\,.$$

On dit aussi que S est une *famille libre*. Dans le cas contraire, les vecteurs sont dits *linéairement dépendants*, et on parle de *famille liée*.

Exemples (de familles libres et liées)**.**

1. La famille vide $S = \varnothing$ est trivialement libre.
2. Les vecteurs $1, i \in \mathbb{C}$ sont linéairement indépendants sur $\mathbb{R}$ (puisque $a+bi = 0$ avec $a, b \in \mathbb{R}$ implique $a = b = 0$), mais ils sont linéairement dépendants sur $\mathbb{C}$ (puisque $i \cdot 1 + (-1) \cdot i = 0$).
3. Les vecteurs $e_1, \ldots, e_n \in K^n$ sont linéairement indépendants.
4. Les vecteurs $1, X, \ldots, X^n \in K[X]$ sont linéairement indépendants.

Remarques.

1. Par définition, tout sous-ensemble d'une famille libre est libre.
2. Si $S \subset E$ est une famille libre, alors tout élément de $\mathrm{Vect}(S)$ s'écrit de manière unique comme combinaison linéaire d'éléments de S.

   ⌜ Par définition, tout $v \in \mathrm{Vect}(S)$ s'écrit comme combinaison linéaire d'éléments de S. Si on a deux telles combinaisons linéaires pour v, quitte à rajouter des termes de la forme $0 \cdot w$ avec $w \in S$, on peut supposer que ces deux combinaisons linéaires font intervenir les mêmes éléments de S. Supposons donc qu'on ait $v = \lambda_1 v_1 + \cdots + \lambda_n v_n = \lambda'_1 v_1 + \cdots + \lambda'_n v_n$ avec $v_1, \ldots, v_n \in S$. Cela implique

   $$0 = v - v = (\lambda_1 v_1 + \cdots + \lambda_n v_n) - (\lambda'_1 v_1 + \cdots + \lambda'_n v_n) = (\lambda_1 - \lambda'_1) v_1 + \cdots + (\lambda_n - \lambda'_n) v_n\,.$$

   Comme S est libre, cela implique $(\lambda_1 - \lambda'_1) = \cdots = (\lambda_n - \lambda'_n) = 0$, i.e. $\lambda_i = \lambda'_i$ pour tout i. ⌟

Le lemme suivant est tout à fait élémentaire, mais constitue néanmoins la clé de voûte de la théorie.

Lemme III.3. *Si $v_1, \dots, v_n \in E$ sont linéairement dépendants, alors il existe $j \in \{1, \dots, n\}$ tel que v_j est combinaison linéaire de $v_1, \dots, v_{j-1}$.*

Démonstration. Supposons donc $v_1, \dots, v_n \in E$ linéairement dépendants. Par définition, il existe $\lambda_1, \dots, \lambda_n \in K$ non-tous nuls avec $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$. Posons $j = \max\{i \in \{1, \dots, n\} \mid \lambda_i \neq 0\}$. Comme $\lambda_i = 0$ pour tout $i > j$, on a donc

$$0 = \lambda_1 v_1 + \cdots + \lambda_n v_n = \lambda_1 v_1 + \cdots + \lambda_j v_j \,,$$

d'où $\lambda_j v_j = -\lambda_1 v_1 - \cdots - \lambda_{j-1} v_{j-1}$. Comme K est un corps [7], on a $\lambda_j \in K \setminus \{0\} = K^*$ et il existe $\lambda_j^{-1} \in K$ tel que $\lambda_j^{-1} \lambda_j = 1$. Cela mène aisément à l'égalité

$$v_j = (-\lambda_j^{-1} \lambda_1) v_1 + \cdots + (-\lambda_j^{-1} \lambda_{j-1}) v_{j-1} \,,$$

et v_j est bien combinaison linéaire de $v_1, \dots, v_{j-1}$. □

Définition III.3

Un sous-ensemble S d'un espace vectoriel E est appelé une **base** de E (sur K) si

(i) S est une famille génératrice de E, i.e. $\mathrm{Vect}(S) = E$,

(ii) S est une famille libre.

Remarque. Un sous-ensemble S est une base de E si et seulement si tout élément de E s'écrit de manière unique comme combinaison linéaire d'éléments de S.

⌜ Si S est une base de E, alors tout élément de E s'écrit comme combinaison linéaire d'éléments de S puisque $\mathrm{Vect}(S) = E$, et de manière unique puisque S est libre (voir la remarque 2 ci-dessus). Réciproquement, si tout élément de E s'écrit de manière unique comme combinaison linéaire d'éléments de S, alors $\mathrm{Vect}(S) = E$ par définition, et S est libre puisque la seule manière d'écrire 0_E comme combinaison linéaire d'éléments de S est la manière triviale. ⌟

Exemples (de bases)**.**

1. La famille vide $S = \varnothing$ forme une base de l'espace vectoriel trivial $\{0\}$.
2. La famille $\{1, i\}$ forme une base de $\mathbb{C}$ sur $\mathbb{R}$.
3. Les vecteurs $\{e_1, \dots, e_n\}$ forment une base de K^n sur K.
4. Les vecteurs $\{1, X, \dots, X^n\}$ forment une base de $K_n[X]$ sur K.
5. Les vecteurs $\{1, X, X^2 \dots\}$ forment une base de $K[X]$ sur K.

Le théorème suivant est le plus technique de cette section.

7. Notons qu'il s'agit du seul endroit où cette hypothèse cruciale est utilisée.

Théorème III.4: Théorème de la base incomplète

Soient S une famille génératrice finie d'un espace vectoriel E, et $L \subset S$ une famille libre. Alors, il existe une base T de E avec $L \subset T \subset S$.

Démonstration. Soit donc $S = \{v_1, \dots, v_n\}$ une famille génératrice de E, avec $L = \{v_1, \dots, v_k\}$ libre pour un certain $k \in \{0, \dots, n\}$. L'idée de la preuve est d'enlever un à un des éléments de $v_{k+1} \dots, v_n$ sans modifier l'espace engendré, jusqu'à obtenir une base. La démonstration formelle se fait par récurrence sur $n \geq k$.

Le départ de récurrence $n = k$ est trivial puisque dans ce cas, le choix $T = S$ convient. Soit donc $S = \{v_1, \dots, v_n\}$ avec $L = \{v_1, \dots, v_k\}$ libre, et supposons la proposition démontrée pour toute famille génératrice $S' \subset E$ contenant L avec $|S'| < n$. Étant donné S, de deux choses l'une :

- Si pour tout $j \in \{1, \dots, n\}$, v_j n'est pas combinaison linéaire de $v_1, \dots, v_{j-1}$, alors par la contraposée du lemme III.3, on sait que S est libre. On pose alors simplement $T = S$, qui satisfait trivialement les propriétés voulues.
- Dans le cas contraire, il existe $j \in \{1, \dots, n\}$ tel que v_j est combinaison linéaire de $v_1, \dots, v_{j-1}$: considérons un tel v_j et posons $S' \coloneqq S \setminus \{v_j\}$. Notons que comme $L = \{v_1, \dots, v_k\}$ est libre, aucun v_i n'est combinaison linéaire de $v_1, \dots, v_{i-1}$ pour $i \leq k$. Ainsi, on a $j > k$, d'où $L \subset S' \subset S$.

  Notons également que S' est toujours génératrice car v_j est combinaison linéaire de $v_1, \dots, v_{j-1}$: plus formellement, comme il existe $\mu_1 \dots, \mu_{j-1} \in K$ tels que $v_j = \mu_1 v_1 + \dots + \mu_{j-1} v_{j-1}$, tout élément de $E = \mathrm{Vect}(S)$ peut s'écrire

$$\begin{aligned} \lambda_1 v_1 + \dots + \lambda_n v_n &= \lambda_1 v_1 + \dots + \lambda_{j-1} v_{j-1} + \lambda_j (\mu_1 v_1 + \dots + \mu_{j-1} v_{j-1}) + \dots + \lambda_n v_n \\ &= (\lambda_1 + \lambda_j \mu_1) v_1 + \dots + (\lambda_{j-1} + \lambda_j \mu_{j-1}) v_{j-1} + \lambda_{j+1} v_{j+1} + \dots + \lambda_n v_n \,, \end{aligned}$$

  qui est un élément de $\mathrm{Vect}(S')$. On a donc bien $\mathrm{Vect}(S') = E$.

Par hypothèse de récurrence, il existe une base T de E avec $L \subset T \subset S'$. Comme on a $S' \subset S$, la conclusion suit. □

Ce résultat implique en particulier le résultat fondamental que voici.

Corollaire III.5. *Tout espace vectoriel de-dimension-finie admet une base finie.*

Démonstration. Soit donc E un espace vectoriel de-dimension-finie. Par définition, il existe une famille génératrice finie $S \subset E$. Par le théorème III.4 appliqué à $L = \varnothing$, il existe une base T de E avec $T \subset S$, qui est donc une base finie de E. □

Remarques.

1. Dans un espace vectoriel de-dimension-finie, toute famille génératrice de taille minimale est une base.

   ⌜ Soit S une famille génératrice qui n'est pas une base de E. Ainsi, S est liée : il existe $\{v_1, \dots, v_n\} \subset S$ linéairement dépendants. Par le lemme III.3, il existe v_j

combinaison linéaire de $v_1, \dots, v_{j-1}$. Alors, l'ensemble $S' = S \setminus \{v_j\}$ engendre toujours E (voir la preuve du théorème III.4), et S n'est donc pas une famille génératrice minimale.

⌟

2. En fait tout espace vectoriel (pas forcément de-dimension-finie) admet une base. Mais contrairement à la preuve du théorème III.4, la preuve générale n'est pas constructive : elle repose sur *l'axiome du choix* (sous la forme du *lemme de Zorn*). En d'autres termes, nous savons qu'il existe toujours une base mais dans certains cas, il nous est impossible d'en exhiber une explicitement.

L'existence d'une base va nous permettre de montrer que tout K-espace vectoriel de-dimension-finie est isomorphe à K^n pour un certain entier $n \geq 0$ (voir théorème III.8 ci-dessous). Pour montrer que cet entier n est unique, il nous faut la notion de *dimension*, dont la définition repose sur un dernier résultat technique.

Lemme III.6. *Si $v_1, \dots, v_n \in E$ engendrent E et $w_1, \dots, w_m \in E$ sont linéairement indépendants, alors on a $m \leq n$.*

Démonstration. Comme $\{v_1, \dots, v_n\}$ engendre E qui contient w_1, cet élément est combinaison linéaire de $v_1, \dots, v_n$. Ainsi, la famille $S_1 \coloneqq \{w_1, v_1, \dots, v_n\}$ est liée. Comme $L_1 \coloneqq \{w_1\}$ est libre (puisque $\{w_1, \dots, w_m\}$ l'est) et S_1 est génératrice (puisque $\{v_1, \dots, v_n\}$ l'est), on peut appliquer le théorème III.4 : il existe une base T_1 de E avec $L_1 \subset T_1 \subset S_1$. Comme S_1 est liée et T_1 libre, on a $T_1 \subsetneq S$, d'où $|T_1| < |S_1| = n + 1$, donc $|T_1| \leq n$.

On recommence maintenant la même procédure, avec w_2 et T_1 : comme T_1 engendre E qui contient w_2, la famille $S_2 \coloneqq \{w_2\} \cup T_1$ est liée. Comme $L_2 \coloneqq \{w_1, w_2\}$ est libre (puisque $\{w_1, \dots, w_m\}$ l'est) et S_2 est génératrice (puisque T_1 l'est), le théorème III.4 assure l'existence d'une base T_2 de E avec $L_2 \subset T_2 \subset S_2$. Comme S_2 est liée et T_1 libre, on a $T_1 \subsetneq S_2$, d'où $|T_2| < |S_2| = |T_1| + 1$, donc $|T_2| \leq |T_1| \leq n$.

Après m itérations de cette procédure, on aboutit à une base T_m de E avec $\{w_1, \dots, w_m\} \subset T_m$ et $|T_m| \leq \dots \leq |T_1| \leq n$. On a donc bien $m \leq n$. □

Théorème III.7

Deux bases d'un espace vectoriel de-dimension-finie ont même cardinal fini.

Démonstration. Notons tout d'abord qu'un espace vectoriel E de-dimension-finie n'admet pas de base infinie : en effet, cela fournirait des familles libres de taille arbitrairement grande alors que E est engendrée par une famille finie, et contredirait donc le lemme III.6. Soient à présent $\{v_1, \dots, v_n\}$ et $\{w_1, \dots, w_m\}$ deux bases (finies) de E. Comme $\{v_1, \dots, v_n\}$ est génératrice et $\{w_1, \dots, w_m\}$ libre, on a $m \leq n$ par le lemme III.6. Réciproquement, comme $\{w_1, \dots, w_n\}$ est génératrice et $\{v_1, \dots, v_n\}$ libre, on a $n \leq m$. Ainsi, on a bien l'égalité $m = n$. □

Définition III.4

Si E est un espace vectoriel de-dimension-finie, alors le cardinal d'une base de E est appelé la **dimension** de E, notée $\dim(E)$.

Remarques.

1. Ce théorème est vrai en toute généralité, et l'on peut définir $\dim(E)$ comme le cardinal (pas forcément fini) d'une base quelconque de E[8]. Mais à nouveau, la preuve repose sur l'axiome du choix.
2. Un espace vectoriel E est de-dimension-finie si et seulement si $\dim(E) < \infty$, et l'on peut donc finalement abandonner les tirets disgracieux.

   ⌜ Si E est de-dimension-finie, alors il admet une base finie S par le corollaire III.5, d'où $\dim(E) = |S| < \infty$. Réciproquement, si $\dim(E) < \infty$, alors E admet une base finie, et donc une famille génératrice finie ; il est donc bien de-dimension-finie. ⌟

Tout est maintenant en place pour le résultat fondamental de la théorie : le *théorème de classification des espaces vectoriels de dimension finie.*

Théorème III.8: Classification des espaces vectoriels

Deux espaces vectoriels de dimension finie sur un même corps sont isomorphes si et seulement s'ils ont même dimension.

Démonstration. Soit E un K-espace vectoriel de dimension finie $n \geq 0$. On va vérifier que E est isomorphe à K^n, ce qui montre une implication : en effet, si E et E' sont deux K-espaces vectoriels de même dimension n, on aura $E \simeq K^n \simeq E'$, d'où $E \simeq E'$.

Démontrons cette affirmation. Comme E est de dimension finie, le corollaire III.5 nous garantit l'existence d'une base $v_1, \ldots, v_n$ de E. Soit $f : K^n \to E$ l'application définie par $f(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i v_i$. On vérifie immédiatement qu'il s'agit bien d'une application linéaire. De plus, cette application est surjective puisque $v_1, \ldots, v_n$ engendre E, et son noyau est trivial puisque $v_1, \ldots, v_n$ est libre. Ainsi, c'est une application linéaire bijective, et donc un isomorphisme linéaire.[9]

Pour l'autre implication, nous allons montrer que si $f : E \to E'$ est un isomorphisme linéaire et S une base de E, alors $f(S)$ est une base de E'. Comme la restriction de f à S fournit une bijection entre S et $f(S)$, on aura donc bien $\dim(E) = |S| = |f(S)| = \dim(E')$.

8. Rappelons à ce sujet qu'il existe des cardinaux infinis différents. Par exemple, l'espace vectoriel $K[X]$ est de dimension infinie dénombrable, tandis que $K^{[0,1]}$ est de dimension non-dénombrable.

9. Alternativement, on aurait pu utiliser la remarque 2 pour dire que E est somme directe interne des sous-espaces $F_1, \ldots, F_n$ engendrés par $v_1, \ldots, v_n$, respectivement, puis conclure que $E \simeq K^n$ à l'aide de la proposition III.1.

Pour vérifier cette affirmation, soient donc $f: E \to E'$ un isomorphisme linéaire et S une base de E. Il s'agit de montrer que $f(S)$ est une base de E', i.e. que $f(S)$ est une famille génératrice libre.

Pour voir que $f(S)$ est génératrice, prenons un vecteur $v' \in E'$ arbitraire. Comme f est surjective, il existe $v \in E$ tel que $f(v) = v'$. Comme S est une famille génératrice de E, il existe $v_1, \dots, v_n \in E$ et $\lambda_1, \dots, \lambda_n \in K$ tels que $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$. En utilisant la linéarité de f, on obtient

$$v' = f(v) = f(\lambda_1 v_1 + \cdots + \lambda_n v_n) = \lambda_1 f(v_1) + \cdots + \lambda_n f(v_n) \in \mathrm{Vect}(f(S)),$$

et l'on a bien $v' \in \mathrm{Vect}(f(S))$, i.e. $f(S)$ génératrice.

Pour voir que $f(S)$ est également libre, considérons $v'_1, \dots, v'_n \in f(S)$ et des scalaires $\lambda_1, \dots, \lambda \in K$ tels que $\lambda_1 v'_1 + \cdots + \lambda_n v'_n = 0$. Par définition, il existe $v_1, \dots, v_n \in S$ tels que $v'_i = f(v_i)$ pour tout i. Ainsi, on a

$$0 = \lambda_1 v'_1 + \cdots + \lambda_n v'_n = \lambda_1 f(v_1) + \cdots + \lambda_n f(v_n) = f(\lambda_1 v_1 + \cdots + \lambda_n v_n).$$

Comme f est injective, cela implique $0 = \lambda_1 v_1 + \cdots + \lambda_n v_n$. Comme S est libre, nous avons bien $\lambda_1 = \cdots = \lambda_n = 0$, et la famille $f(S)$ est libre. □

Exemples.

1. Les K-espaces vectoriels $K_n[X]$ et K^n sont isomorphes [10] pour tout $n \geq 0$.
2. Les $\mathbb{R}$-espaces vectoriels $\mathbb{C}$ et $\mathbb{R}^2$ sont isomorphes.
3. Les $\mathbb{R}$-espaces vectoriels $\mathbb{R}$ et $\mathbb{R}^2$ ne sont pas isomorphes [11].

Remarque. Ce théorème est valide en toute généralité, sans hypothèse de dimension finie, avec exactement la même preuve. Mais cette preuve repose bien évidemment sur les versions générales des théorèmes III.4 et III.7, que nous n'avons pas démontrées, et donc sur l'axiome du choix.

Nous allons conclure cette section avec un résultat fondamental, appelé le *théorème du rang*, que voici.

Théorème III.9: Théorème du rang

Si $f: E \to E'$ est une application linéaire avec E de dimension finie, alors

$$\dim(E) = \dim(\mathrm{Ker}(f)) + \dim(\mathsf{Im}(f)).$$

La preuve que nous allons en donner repose sur le lemme suivant.

Lemme III.10. *Si F est un sous-espace vectoriel d'un espace vectoriel E de dimension finie, alors F et E/F sont également de dimension finie, et satisfont* $\dim(E/F) = \dim(E) - \dim(F)$.

10. C'est la raison du choix de cet indice pour $K_n[X]$: on obtient ainsi un espace vectoriel de dimension n.

11. Alors que ces deux ensembles ont même cardinal.

Démonstration du théorème III.9. Soit donc $f : E \to E'$ est une application linéaire avec E de dimension finie. Par le lemme III.10, on sait que les espaces vectoriels $\mathrm{Ker}(f)$ et $E/\mathrm{Ker}(f)$ sont de dimension finie et satisfont $\dim(E/\mathrm{Ker}(f)) = \dim(E) - \dim(\mathrm{Ker}(f))$. Par le théorème d'isomorphisme, l'application linéaire f induit un isomorphisme linéaire $E/\mathrm{Ker}(f) \simeq \mathsf{Im}(f)$. Par le théorème III.8, ces espaces ont même dimension

$$\dim(\mathsf{Im}(f)) = \dim(E/\mathrm{Ker}(f)) = \dim(E) - \dim(\mathrm{Ker}(f))\,,$$

ce qui conclut la preuve. □

Démonstration du lemme III.10. Soit donc E un espace vectoriel de dimension finie, disons $\dim(E) = n$. Notons tout d'abord qu'il est impossible d'avoir une base de F avec plus de n éléments. En effet, on aurait alors une famille libre de taille plus grande que n alors qu'une base de E, forcément de taille $\dim(E) = n$, est une famille génératrice : cela contredirait le lemme III.6. On a donc bien que F est de dimension finie avec $\dim(F) \leq \dim(E)$.

Par le théorème III.7, il existe des bases $w_1, \ldots, w_m$ de F et $v_1, \ldots, v_n$ de E avec $m = \dim(F) \leq \dim(E) = n$. Ainsi, la famille $\{w_1, \ldots, w_m, v_1, \ldots, v_n\}$ engendre E avec $\{w_1, \ldots, w_m\}$ libre. Par le théorème III.4, il existe une base T de E avec $\{w_1, \ldots, w_m\} \subset T \subset \{w_1, \ldots, w_m, v_1, \ldots, v_n\}$. On a donc une base

$$T = \{w_1, \ldots, w_m, v_{i_1}, \ldots, v_{i_r}\}$$

de E pour un certain sous-ensemble d'indices $\{i_1, \ldots, i_r\} \subset \{1, \ldots, n\}$.

Montrons maintenant que $S = \{[v_{i_1}], \ldots, [v_{i_r}]\}$ est une base de E/F. Cela terminera la preuve du lemme, puisqu'on aura alors que E/F est de dimension finie égale à

$$\dim(E/F) = |S| = r = |T| - m = \dim(E) - \dim(F)\,.$$

Pour montrer que S engendre E/F, prenons un vecteur quelconque E/F. Il est de la forme $[v]$ avec $v \in E = \mathrm{Vect}(T)$: il existe donc $\lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_r \in K$ tels que

$$v = \lambda_1 w_1 + \cdots + \lambda_m w_m + \mu_1 v_{i_1} + \cdots + \mu_r v_{i_r} \in E\,.$$

En appliquant à cette égalité la projection $\pi : E \to E/F, x \mapsto [x]$, qui est une application linéaire de noyau F, on obtient

$$[v] = [\lambda_1 w_1 + \cdots + \lambda_m w_m] + [\mu_1 v_{i_1} + \cdots + \mu_r v_{i_r}] = \mu_1 [v_{i_1}] + \cdots + \mu_r [v_{i_r}] \in \mathrm{Vect}(S)\,,$$

ce qui montre que S est bien une famille génératrice de E/F.

Pour montrer que S est une famille libre, prenons des scalaires $\alpha_1, \ldots, \alpha_r$ tels que $\alpha_1 [v_{i_1}] + \cdots + \alpha_r [v_{i_r}] = 0 \in E/F$. Cela signifie que le vecteur $\alpha_1 v_{i_1} + \cdots + \alpha_r v_{i_r}$ appartient à $\mathrm{Ker}(\pi) = F = \mathrm{Vect}(\{w_1, \ldots, w_m\})$, d'où l'existence de $\beta_1, \ldots, \beta_m \in K$ tels que

$$\alpha_1 v_{i_1} + \cdots + \alpha_r v_{i_r} = \beta_1 w_1 + \cdots + \beta_m w_m \in E\,,$$

que l'on peut écrire

$$(-\beta_1) w_1 + \cdots + (-\beta_m) w_m + \alpha_1 v_{i_1} + \cdots + \alpha_r v_{i_r} = 0\,.$$

Comme $\{w_1, \ldots, w_m, v_{i_1}, \ldots, v_{i_r}\}$ est libre, on a $\alpha_1 = \cdots = \alpha_r = \beta_1 = \cdots = \beta_m = 0$. En particulier, tous les α_i sont nuls, ce qui conclut la preuve. □

III.3 Modules : axiomes et exemples

Il est difficile de créditer l'invention de la notion de module à un mathématicien en particulier, mais il est incontestable que la mathématicienne EMMY NOETHER a joué un rôle prépondérant dans leur étude.

EMMY NOETHER (1882-1935)

En voici la définition.

Définition III.5

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 (de 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 [12] avec les groupes abéliens.

   ⌜ 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 (voir section I.1). De plus, on a vu que 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 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 $1 \cdot g = g$ par définition. ⌟

12. Le sens précis de ce mot est à trouver dans sa preuve ci-dessous.

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. Un anneau A est un A-module, pour la loi interne donnée par l'addition et la loi "externe" donnée par la multiplication.

   ⌜ L'axiome $(A1)$ implique $(M1)$, $(A2)$ implique $(M2)$, $(A3)$ implique $(M5)$, tandis que $(A4)$ implique $(M3)$ et $(M4)$. ⌟

4. Soit E un K-espace vectoriel muni d'un *endomorphisme* $f \in \mathrm{End}(E)$, i.e. d'une application linéaire $f\colon E \to E$. 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

$$\Big(\sum_{i\geq 0} \lambda_i X^i\Big) \cdot v = \sum_{i\geq 0} \lambda_i f^i(v)\,, \quad \text{où } f^0 = \mathrm{id} \text{ et } f^i = \overbrace{f \circ \cdots \circ f}^{i} \in \mathrm{End}(E)\,.$$

   ⌜ L'axiome $(E1)$ pour l'espace vectoriel E implique l'axiome $(M1)$.

   Pour vérifier $(M2)$, fixons $P = \sum_i a_i X^i$ et $Q = \sum_j b_j X^j$ dans $K[X]$, et v dans E. En utilisant la linéarité de f et la définition de la multiplication dans $K[X]$, on trouve

$$\begin{aligned} P \cdot (Q \cdot v) &= P \cdot \Big(\sum_j b_j f^j(v)\Big) = \sum_i a_i f^i\Big(\sum_j b_j f^j(v)\Big) \\ &= \sum_i \sum_j a_i b_j f^{i+j}(v) = \sum_k \sum_{i+j=k} a_i b_j f^k(v) = (PQ) \cdot v\,. \end{aligned}$$

   Pour vérifier $(M3)$, fixons $P, Q \in K[X]$ comme ci-dessus, et v dans E. On calcule :

$$\begin{aligned} (P+Q) \cdot v &= \Big(\sum_i a_i X^i + \sum_i b_i X^i\Big) \cdot v = \Big(\sum_i (a_i + b_i) X^i\Big) \cdot v \\ &= \sum_i (a_i + b_i) f^i(v) = \sum_i a_i f^i(v) + \sum_i b_i f^i(v) = P \cdot v + Q \cdot v\,. \end{aligned}$$

   L'axiome $(M4)$, i.e. l'égalité $P \cdot (v+w) = P \cdot v + P \cdot w$ pour tout $P \in K[X]$ et $v, w \in E$, découle de la linéarité de f. Finalement, l'axiome $(M5)$ est satisfait par définition, puisque $1_{K[X]} \cdot v = f^0(v) = v$ pour tout $v \in E$. ⌟

   Comme cette structure dépend de f, on notera E_f le $K[X]$-module correspondant.

   Réciproquement, un $K[X]$-module M est un K-espace vectoriel, et l'application $f\colon M \to M$ donnée par $f(x) = X \cdot x$ est un endomorphisme linéaire de M.

   ⌜ En effet, la restriction de la loi externe $K[X] \times M \to M$ à $K \times M \to M$ fait de M un module sur K, et donc un K-espace vectoriel. Pour vérifier que $f\colon M \to M$ est linéaire, on calcule directement

$$f(x+y) = X \cdot (x+y) \overset{(M4)}{=} X \cdot x + X \cdot y = f(x) + f(y)$$

et

$$f(\lambda \cdot x) = X \cdot (\lambda \cdot x) \overset{(M2)}{=} (X\lambda) \cdot x = (\lambda X) \cdot x \overset{(M2)}{=} \lambda \cdot (X \cdot x) = \lambda \cdot f(x)$$

pour tous $x, y \in M$ et $\lambda \in K$. ⌟

En conclusion : les $K[X]$-modules coïncident avec les K-espaces vectoriels munis d'un endomorphisme, dans le sens précis explicité ci-dessus.

5. Si $M_1, \ldots, M_n$ sont des A-modules, alors $M \times \cdots \times M_n$ est un A-module pour les lois

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$
$$a \cdot (x_1, \ldots, x_n) = (a \cdot x_1, \ldots, a \cdot v_n)\,.$$

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.

Remarque. Exactement comme pour les espaces vectoriels, on montre les règles de calcul suivantes dans un A-module M, valides pour tous $a \in A$ et $x \in M$:

(i) $a \cdot 0_M = 0_M$ et $0_A \cdot x = 0_M$,

(ii) $(-a) \cdot x = a \cdot (-x) = -(a \cdot x)$.

En revanche, la troisième règle de calcul vue en section III.1 n'est pas valide pour un A-module M quelconque : si $a \in A$ et $x \in M$ satisfont $a \cdot x = 0_M$, cela n'implique *pas* $a = 0_A$ ou $x = 0_M$.

Par exemple, considérons l'anneau $A = \mathbb{Z}$ et le $\mathbb{Z}$-module (i.e. groupe abélien) $M = \mathbb{Z}/2\mathbb{Z}$. Les éléments $a = 2 \in \mathbb{Z}$ et $x = [1] \in \mathbb{Z}/2\mathbb{Z}$ sont tous les deux non-nuls, mais satisfont néanmoins $a \cdot x = 2 \cdot [1] = [1] + [1] = [0] = 0_M$.

Terminologie. Un sous-ensemble N non-vide d'un A-module M est un *sous-module* de M s'il satisfait :

(i) pour tous $x, y \in N$, on a $x + y \in N$,

(ii) pour tous $a \in A$ et $x \in N$ on a $a \cdot x \in N$.

Remarques.

1. Un sous-ensemble $N \subset M$ est un sous-module de M si et seulement s'il est un module pour la restriction des lois de M à N.
2. Un sous-module $N \subset M$ est en particulier un sous-groupe de $(M, +)$.

Exemples (de sous-modules)**.**

1. Si $A = K$ est un corps, alors par définition, les sous-modules coïncident avec les sous-espaces vectoriels.
2. Si $A = \mathbb{Z}$, alors les sous-modules d'un $\mathbb{Z}$-module M coïncident avec les sous-groupes du groupe abélien correspondant.
3. Si A est un anneau commutatif, alors les sous-modules du A-module $M = A$ coïncident avec les idéaux de A.

4. Si E est un K-espace vectoriel muni d'un endomorphisme $f \in \mathrm{End}(E)$, alors les sous-modules du $K[X]$-module E_f coïncident avec les sous-espaces vectoriel F de E qui sont *stables* par f, i.e. tels que $f(F) \subset F$.

   ⌜ La seconde condition implique en particulier que pour tout $v \in F$, on a $X \cdot v = f(v) \in F$, ce qui signifie exactement que $f(F) \subset F$. Comme F est un sous-espace vectoriel, c'est en fait équivalent à $P \cdot v \in F$ pour tout $P \in K[X]$. ⌟

5. Si N_1, N_2 sont des sous-modules d'un A-module M, alors

$$N_1 + N_2 \coloneqq \{x_1 + x_2 \,|\, x_1 \in N_1,\ x_2 \in N_2\}$$

   est un sous-module de M.

Définition III.6

Soient M, M' deux modules sur un anneau A. Une application $\varphi : M \to M'$ est un **homomorphisme de A-modules** (ou **application 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 $a \in A$.

Si φ est bijective, c'est un *isomorphisme de A-modules*. On dit alors que M, M' sont *isomorphes*, ce qui est noté $M \simeq M'$.

Exemples (d'applications A-linéaires)**.**

1. Si $A = K$ est un corps, alors on retombe bien entendu sur la notion d'application 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 a vu que tout homomorphisme de groupes $\varphi : G \to G'$ satisfait $\varphi(n \cdot g) = n \cdot \varphi(g)$ pour tous $n \in \mathbb{Z}$ et $g \in G$: cela découle par exemple de la preuve de la proposition II.2. ⌟

3. Venons-en au cas de $A = K[X]$. Soient donc E, E' deux K-espaces vectoriels munis d'endomorphismes $f \in \mathrm{End}(E), f' \in \mathrm{End}(E')$. 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 $\varphi \circ f = f' \circ \varphi$.

   ⌜ Par définition, une application $\varphi : E_f \to E_{f'}$ est $K[X]$-linéaire si et seulement si elle satisfait $\varphi(v+w) = \varphi(v) + \varphi(w)$ pour tous $v, w \in E$ et $\varphi(P \cdot v) = P \cdot v$ pour tout $P \in K[X]$ et $v \in E$. Vu que tout $P \in K[X]$ est la somme de produits de scalaires $\lambda \in K$ et du polynôme $X \in K[X]$, ces deux conditions sont équivalentes aux trois conditions suivantes :

(i) $\varphi(v+w) = \varphi(v) + \varphi(w)$ pour tous $v, w \in E$,

(ii) $\varphi(\lambda \cdot v) = \lambda \cdot \varphi(v)$ pour tout $\lambda \in K$ et $v \in E$,

(iii) $\varphi(X \cdot v) = X \cdot \varphi(v)$ pour tout $v \in E$.

Notons que les deux premières conditions signifient que $\varphi : E \to E'$ est K-linéaire. Quant à la troisième, comme

$$\varphi(X \cdot v) = \varphi(f(v)) = (\varphi \circ f)(v) \quad \text{et} \quad X \cdot \varphi(v) = f'(\varphi(v)) = (f' \circ \varphi)(v)$$

pour tout $v \in E$, elle se traduit par $\varphi \circ f = f' \circ \varphi$. ⌟

En particulier, deux $\mathbb{C}[X]$-modules E_f et $E_{f'}$ sont isomorphes si et seulement s'il existe un isomorphisme $\mathbb{C}$-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.

Terminons cette section en notant que plusieurs résultats obtenus dans le cadre des espaces vectoriels s'étendent *verbatim* aux modules.

Remarques.

1. Si $\varphi : M \to M'$ est A-linéaire, alors $\mathrm{Ker}(\varphi)$ est un sous-module de M et $\mathsf{Im}(\varphi)$ un sous-module de M'.
2. Si N est un sous-module d'un A-module M, alors le groupe abélien quotient M/N est un A-module via $a \cdot [x] = [a \cdot x]$ pour $a \in A$ et $x \in M$.
3. Toute application A-linéaire $\varphi : M \to M'$ induit un isomorphisme de A-modules $\overline{\varphi} : M/\mathrm{Ker}(\varphi) \to \mathsf{Im}(\varphi)$.

III.4 Modules sur un anneau euclidien

Le but de cette section est d'énoncer, puis de démontrer partiellement, un théorème de classification des modules de génération finie sur un anneau euclidien. Comme mentionné précédemment, ce résultat illustre magnifiquement la puissance unificatrice de l'algèbre formel, mais ne fait pas partie du champ de l'examen.

Commençons par introduire les notions nécessaires à l'énoncé de ce théorème, à savoir celles de *somme directe interne*, de *module cyclique*, et de *module de génération finie*.

Terminologie. Un A-module M est la *somme directe interne* de sous-modules $M_1, \ldots, M_n \subset M$ si tout $x \in M$ s'écrit de manière unique comme $x = x_1 + \cdots + x_n$ avec $x_1 \in M_1, \ldots, x_n \in M_n$.

Toute la discussion correspondante de la section III.1, en particulier la proposition III.1, s'étend *verbatim* :

Remarques.

1. Si M est la somme directe interne de sous-modules $M_1, \ldots, M_n \subset M$, alors M est isomorphe à la somme directe externe $M_1 \oplus \cdots \oplus M_n$ des modules $M_1, \ldots, M_n$.

2. Un module M est somme directe interne de $M_1, M_2 \subset M$ si et seulement si $M_1 + M_2 = M$ et $M_1 \cap M_2 = \{0\}$.

Exemples (de sommes directes)**.**

1. Si $A = K$ est un corps, la notion de somme directe interne de sous-modules coïncide bien évidemment avec celle de somme directe interne de sous-espaces vectoriels.
2. Si $A = \mathbb{Z}$, la somme directe externe $G_1 \oplus G_2$ de deux $\mathbb{Z}$-modules G_1, G_2 coïncide avec le produit direct des groupes (abéliens) correspondants vu en section I.1, et noté $G_1 \times G_2$.
3. Venons-en à l'exemple de l'anneau $A = K[X]$. Soit E un K-espace vectoriel muni d'un endomorphisme f, et soit E_f le $K[X]$-module correspondant. Rappelons que les sous-modules de E_f sont les sous-espaces vectoriel de E stables par f. Il en résulte que E_f est somme directe interne de sous-modules $F_1, \dots, F_n \subset E_f$ si et seulement si :
   (i) le K-espace vectoriel E est somme directe interne des sous-espaces vectoriels $F_1, \dots, F_n \subset E$, et
   (ii) on a $f(F_i) \subset F_i$ pour tout $i = 1, \dots, n$.

   Ainsi, par le premier point, si S_i est une base de F_i sur K pour $i = 1, \dots, n$, alors $S = S_1 \cup \cdots \cup S_n$ est une base de E sur K. De plus, par le second point, la matrice de $f \in \mathrm{End}(E)$ dans cette base S est donnée par la somme directe des matrices de $f|_{F_i} \in \mathrm{End}(F_i)$ dans la base S_i.

Terminologie. Un A-module M est dit *cyclique* s'il existe $x_0 \in M$ tel que pour tout $x \in M$, il existe $a \in A$ tel que $x = a \cdot x_0$. On dit alors que M est *engendré* par x_0, et que x_0 est un *générateur* de M.

Exemples (de modules cycliques)**.**

1. Pour $A = K$ un corps, les seuls modules cycliques sont les K-espaces vectoriels $E = \{0\}$ et $E \simeq K$.

   ⌜ Soit E un espace vectoriel cyclique engendré par $v_0 \in E$: on a donc $E = \mathrm{Vect}(\{v_0\})$. Si $v_0 = 0$, alors $E = \{0\}$. Si $v_0 \neq 0$, alors $\{v_0\}$ forme une base de E, qui est donc de dimension 1, d'où $E \simeq K$. ⌟
2. Pour $A = \mathbb{Z}$, les $\mathbb{Z}$-modules cycliques coïncident par définition avec les groupes (abéliens) cycliques, et sont donc de la forme $\mathbb{Z}/n\mathbb{Z}$ avec $n \geq 0$.
3. Si I est un idéal d'un anneau A, alors cet idéal est un sous-module du A-module $M = A$ et l'on peut considérer le A-module quotient A/I. Il s'agit d'un A-module cyclique.

   ⌜ Posons $x_0 = [1_A] \in A/I$. Tout élément $x \in A/I$ est de la forme $x = [a]$ avec $a \in A$, que l'on peut écrire $x = [a] = [a \cdot 1_A] = a \cdot [1_A] = a \cdot x_0$. Ainsi, A/I est un A-module cyclique engendré par x_0. ⌟

En particulier, le A-module $M = A$ lui-même est un A-module cyclique.

Notons que pour $A = K$, les seuls idéaux de K sont $I = \{0\}$ et $I = K$, d'où les K-modules cycliques $K/\{0\} \simeq K$ et $K/K = \{0\}$, et l'on retrouve l'exemple 1 ci-dessus.

Pour $A = \mathbb{Z}$, les seuls idéaux de $\mathbb{Z}$ sont $I = n\mathbb{Z}$ avec $n \geq 0$, d'où les $\mathbb{Z}$-modules cycliques $\mathbb{Z}/n\mathbb{Z}$, et l'on retrouve l'exemple 2.

En fait, tous les modules cycliques sont de cette forme !

Proposition III.11. *Soit A un anneau commutatif. Si M est un A-module cyclique, alors il existe un idéal $I \subset A$ tel que $M \simeq A/I$.*

Démonstration. Soit donc M un A-module cyclique, engendré par $x_0 \in M$. Considérons l'application $\varphi\colon A \to M$ définie par $\varphi(a) = a \cdot x_0$. Comme x_0 est un générateur de M, cette application est surjective. De plus, c'est un homomorphisme de A-modules, puisque pour tous $a, b \in A$, on a

$$\varphi(a+b) = (a+b)\cdot x_0 = a\cdot x_0 + b\cdot x_0 = \varphi(a) + \varphi(b)$$

et

$$\varphi(a\cdot b) = (a\cdot b)\cdot x_0 = a\cdot(b\cdot x_0) = a\cdot\varphi(b)\,.$$

Ainsi le noyau de φ est un sous-module de A. Comme A est commutatif, ce sous-module est un idéal I de A. Finalement, par le théorème d'isomorphisme, cette application induit un isomorphisme de A-modules $\overline{\varphi}\colon A/\mathrm{Ker}(\varphi) \to \mathsf{Im}(\varphi)$, i.e. un isomorphisme $A/I \simeq M$. □

Par la proposition II.11, on obtient directement le corollaire suivant.

Corollaire III.12. *Soit M un A-module cyclique avec A euclidien. Alors, il existe $x \in A$ tel que $M \simeq A/(x)$.* □

Remarque. Dans le cas $A = \mathbb{Z}$, on retrouve la classification des groupes cycliques (le théorème I.10), avec essentiellement la même preuve. Mais pour $A = K[X]$, c'est un résultat nouveau.

Venons-en finalement à la dernière notion.

Terminologie. 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 $x = a_1x_1 + \cdots + a_nx_n$ avec $a_1, \ldots, a_n \in A$.

Exemples (de 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.
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.

4. Un module cyclique est de génération finie, puisqu'il est engendré par un élément. Plus généralement, tout module qui est la somme directe d'un nombre fini de modules cycliques est de génération finie.

Nous sommes finalement en mesure d'énoncer le résultat le plus technique de ce cours, qui est la réciproque du dernier exemple ci-dessus pour les modules sur un anneau euclidien.

Théorème III.13

Si A est un anneau euclidien, alors tout A-module de génération finie est somme directe (interne) d'un nombre fini de sous-modules cycliques.

La preuve de ce théorème ne sera donnée que plus tard. En voici une conséquence, qui est la raison d'être de cette section, et dont la preuve fait intervenir un très grand nombre de résultats vus tout au long de ce cours.

Théorème III.14

Soit M un module de génération finie sur A un anneau euclidien. Alors, il existe des entiers $r, n \geq 0$, une suite de premiers $p_1, \dots, p_n \in A$ (pas forcément distincts) et des entiers $\nu_1, \dots, \nu_n \geq 1$, tels que

$$M \simeq A^r \oplus A/(p_1^{\nu_1}) \oplus \cdots \oplus A/(p_n^{\nu_n})\,. \qquad (*)$$

Démonstration. Soit donc M un A-module de génération finie avec A euclidien. Par le théorème III.13, il existe des sous-modules cycliques $M_1, \dots, M_n$ de M dont M est la somme directe interne. Par la proposition III.1 (qui s'étend aux modules, voir remarque 1 en début de cette section), on a donc un isomorphisme de A-modules $M \simeq M \oplus \cdots \oplus M_n$. Comme A est euclidien, on peut appliquer le corollaire III.12 : il existe des éléments $x_1, \dots, x_m \in A$ tels que $M_i \simeq A/(x_i)$ pour tout $i = 1, \dots, m$. En résumé, on a un isomorphisme de A-modules

$$M \simeq A/(x_1) \oplus \cdots \oplus A/(x_n)\,.$$

Analysons à présent ces différents facteurs, tous de la forme $A/(x)$ pour $x \in A$.

- Si $x = 0$, alors $A/(x) = A/(0) \simeq A$: le facteur correspondant contribue donc à A^r dans la somme directe $(*)$.
- Si $x \in A^*$, alors $A/(x) = A/A = \{0\}$: le facteur correspondant ne contribue pas à la somme directe.
- Si x n'est ni zéro ni une unité, alors par le théorème II.16, il existe des premiers $p_1, \dots, p_\ell$ de A et des entiers $\mu_1, \dots, \mu_\ell$ tels que $x = p_1^{\mu_1} \cdots p_\ell^{\mu_\ell} \in A$. Comme les premiers $p_1, \dots, p_\ell$ sont distincts, les éléments $p_1^{\mu_1}, \dots, p_\ell^{\mu_\ell}$ de A sont deux à deux premiers entre eux. Par théorème des restes chinois (et une récurrence sur $\ell \geq 1$), on a un isomorphisme d'anneaux

$$A/(x) = A/(p_1^{\mu_1} \cdots p_\ell^{\mu_\ell}) \simeq A/(p_1^{\mu_1}) \oplus \cdots \oplus A/(p_\ell^{\mu_\ell})\,.$$

Finalement, on vérifie facilement que cet isomorphisme d'anneaux est un isomorphisme de A-modules.

En mettant ensemble les facteurs $A/(x_i)$ pour $x_i = 0$ (qui contribuent à A^r dans $(*)$), pour $x_i \in A^*$ (qui ne contribuent pas), et pour $x_i \notin A^* \cup \{0\}$ (qui contribuent aux $A/(p^\nu)$ dans $(*)$), on obtient l'isomorphisme annoncé. □

Remarques.

1. Cet énoncé est un *théorème de décomposition* des modules de génération finie sur un anneau euclidien. Le *théorème de classification* dit que, de plus, l'entier $r \geq 0$ est unique, et les éléments $p_1^{\nu_1}, \ldots, p_n^{\nu_n}$ sont uniques à l'ordre et à multiplication par des unités près. Nous ne verrons pas la preuve de ce théorème, qui nécessite des outils que nous n'avons pas à notre disposition [13].
2. On parle de *théorème de classification* car un tel énoncé permet de classifier ces modules à isomorphisme près. En effet, il implique que deux modules $M \simeq A^r \oplus A/(p_1^{\nu_1}) \oplus \cdots \oplus A/(p_n^{\nu_n})$ et $N \simeq A^s \oplus A/(q_1^{\mu_1}) \oplus \cdots \oplus A/(q_m^{\mu_m})$ sont isomorphes si et seulement $r = s$, $n = m$ et les éléments $p_1^{\nu_1}, \ldots, p_n^{\nu_n}$ et $q_1^{\mu_1}, \ldots, q_m^{\mu_m}$ coïncident à l'ordre et à multiplication par des unités près.
3. Ce théorème de classification est valide dans le cadre légèrement plus général des modules de génération finie sur un anneau principal. En revanche, il n'est pas valide si l'une des hypothèses n'est pas satisfaite, à savoir : si M n'est pas de génération finie (puisque tout module de la forme $(*)$ est de génération finie), ou si A n'est pas principal (puisqu'un idéal $I \subset A$ avec I pas principal est un A-module qui n'est pas de la forme $(*)$).

Avant de donner la preuve du théorème III.13, tentons de voir ce que le théorème de classification nous dit dans trois exemples d'anneaux euclidiens : les corps, l'anneau des entiers $\mathbb{Z}$, et l'anneau $\mathbb{C}[X]$.

Exemple A : Les corps

Commençons avec le cas de $A = K$ un corps. Comme on le sait, il n'y a pas d'éléments premiers dans un corps. On obtient donc l'énoncé bien connu suivant :

Soit E un espace vectoriel de dimension finie sur un corps K. Alors, il existe un entier $r \geq 0$ tel que $E \simeq K^r$.

Comme on l'a vu dans la preuve du théorème III.8, cet énoncé est essentiellement équivalent à l'existence d'une base. Le théorème de classification des K-modules de génération finie dit que, de plus, cet entier r est unique. Comme on le sait, cet énoncé-là est équivalent à l'existence de la dimension.

Ainsi, il faut voir l'entier $r \geq 0$ uniquement associé à M dans $(*)$ comme une généralisation de la notion de dimension aux modules de génération finie sur un anneau euclidien [14].

13. Ces outils sont les *facteurs invariants*, voir par exemple le chapitre 15 du livre *Invitation à l'algèbre*, de Jeanneret-Lines.

14. Cet entier peut en fait être défini pour tout module de génération finie sur un anneau intègre.

Exemple B : L'anneau des entiers $\mathbb{Z}$

Dans le cas $A = \mathbb{Z}$, on obtient comme cas particulier le théorème de décomposition des groupes abéliens finis, démontré par Leopold Kronecker en 1870.

Théorème III.15: Décomposition des groupes abéliens finis

Soit G un groupe abélien fini. Alors, il existe une suite de premiers $p_1, \dots, p_n$ (pas forcément distincts) et des entiers $\nu_1, \dots, \nu_n \geq 1$ tels que

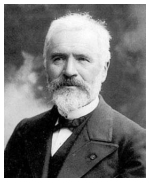
$$G \simeq \mathbb{Z}/p_1^{\nu_1} \times \cdots \times \mathbb{Z}/p_1^{\nu_1}\,.$$

Leopold Kronecker (1823-1891)

Démonstration. Soit donc G un groupe abélien fini. C'est un $\mathbb{Z}$-module de génération finie, et l'on peut appliquer le théorème III.14. Comme G est fini, on a forcément $r = 0$. Finalement, comme observé en exemple 2 en début de cette section, la somme directe des $\mathbb{Z}$-modules correspond au produit direct des groupes abéliens. □

C'est exactement le théorème de classification des groupes abéliens finis, déjà annoncé en section I.9, sans l'unicité des $p_1^{\nu_1}, \dots, p_n^{\nu_n}$ à l'ordre près. Bien entendu, le résultat complet découle du théorème de classification des $\mathbb{Z}$-modules de génération finie. Ainsi, on comprend que la preuve d'un tel résultat de classification requière des considérations "d'ordre", par exemple pour montrer que $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes.

Exemple C : L'anneau des polynômes $\mathbb{C}[X]$



Camille Jordan (1838-1922)

Dans ce dernier exemple, nous allons voir comment le théorème III.14 permet de "redécouvrir" très naturellement la décomposition de Jordan d'un endomorphisme complexe. Soit donc E un $\mathbb{C}$-espace vectoriel de dimension finie, et soit $f : E \to E$ un endomorphisme de E.

Comme on l'a vu, cela définit un $\mathbb{C}[X]$-module E_f via $X \cdot v = f(v)$ pour tout $v \in E$. Notons qu'une base finie de E sur $\mathbb{C}$ est une famille génératrice finie de E sur $\mathbb{C}$, et donc également une famille génératrice finie de E sur $\mathbb{C}[X]$. Ainsi, on est bien en présence d'un module E_f de génération finie sur l'anneau euclidien $\mathbb{C}[X]$, et l'on peut appliquer le théorème III.14 : il existe des entiers $r, n \geq 0$, des premiers $p_1, \dots, p_n \in \mathbb{C}[X]$ pas forcément distincts, et des entiers $\nu_1, \dots, \nu_n \geq 1$, tels qu'on a un isomorphisme de $\mathbb{C}[X]$-modules

$$E_f \simeq \mathbb{C}[X]^r \oplus \mathbb{C}[X]/(p_1^{\nu_1}) \oplus \cdots \oplus \mathbb{C}[X]/(p_n^{\nu_n})\,.$$

Notons à présent que comme on suppose E de dimension finie sur $\mathbb{C}$, et que $\mathbb{C}[X]$ est de dimension infinie sur $\mathbb{C}$, on a forcément $r = 0$. Rappelons également que, comme on l'a vu en fin de section II.6, tout premier [15] de $\mathbb{C}[X]$ est associé à un unique élément de la forme $X - \lambda$ avec $\lambda \in \mathbb{C}$. On a donc une

15. C'est ici le seul endroit où l'on utilise le fait qu'on travaille sur $\mathbb{C}$; le reste de l'argument est valide dans l'anneau $K[X]$ pour tout corps K.

suite $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ de nombres complexes pas forcément distincts et des entiers $\nu_1, \dots, \nu_n \geq 1$ tels que

$$E_f \simeq \mathbb{C}[X]/((X-\lambda_1)^{\nu_1}) \oplus \cdots \oplus \mathbb{C}[X]/((X-\lambda_n)^{\nu_n}) .$$

Par l'exemple 3 de somme directe, une matrice pour $f \in \mathrm{End}(E)$ est donnée par la somme directe des matrices des restrictions de f aux sous-espaces vectoriels $\mathbb{C}[X]/((X-\lambda_i)^{\nu_i}), i = 1, \dots, n$, avec f donné par la multiplication par X.

Tentons donc de comprendre cet endomorphisme.

Lemme III.16. *Soit $\lambda \in \mathbb{C}$ et $\nu \geq 1$ fixés. Alors, l'endomorphisme du $\mathbb{C}$-espace vectoriel $\mathbb{C}[X]/((X-\lambda)^{\nu})$ donné par la multiplication par X admet la matrice carrée de taille ν suivante :*

$$J_\nu(\lambda) = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \lambda & 1 \\ & & & \lambda \end{pmatrix} .$$

Démonstration. Notons que le $\mathbb{C}$-espace vectoriel $\mathbb{C}[X]/((X-\lambda)^{\nu})$ admet la base

$$e_1 = [(X-\lambda)^{\nu-1}],\ e_2 = [(X-\lambda)^{\nu-2}],\ \dots, e_{\nu-1} = [X-\lambda],\ e_\nu = [1] .$$

Ce fait est clair dans le cas $\lambda = 0$, puisque tout élément de $\mathbb{C}[X]/(X^{\nu})$ s'écrit de manière unique comme combinaison linéaire des classes de $1, X, \dots, X^{\nu-1}$. Le cas général en découle via l'isomorphisme de $\mathbb{C}$-espaces vectoriels $\mathbb{C}[X]/(X^{\nu}) \simeq \mathbb{C}[X]/((X-\lambda)^{\nu})$ induit par $X \mapsto X - \lambda$.

Exprimons donc la multiplication par X dans cette base. Dans l'espace vectoriel $\mathbb{C}[X]/((X-\lambda)^{\nu})$, on a

$$0 = [(X-\lambda)^{\nu}] = (X-\lambda)\cdot[(X-\lambda)^{\nu-1}] = (X-\lambda)\cdot e_1 = X\cdot e_1 - \lambda\cdot e_1 ,$$

d'où une première égalité $X \cdot e_1 = \lambda \cdot e_1$. Similairement, on trouve pour $i \geq 2$

$$e_{i-1} = [(X-\lambda)^{\nu-i+1}] = (X-\lambda)\cdot[(X-\lambda)^{\nu-i}] = (X-\lambda)\cdot e_i = X\cdot e_i - \lambda\cdot e_i ,$$

d'où $X \cdot e_i = \lambda \cdot e_i + e_{i-1}$. Cela donne donc bien la matrice $J_\nu(\lambda)$. □

On a donc le résultat suivant.

Théorème III.17: Théorème de réduction 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 $\lambda_1, \dots, \lambda_n$ pas forcément distincts, et certains entiers $\nu_1, \dots, \nu_n \geq 1$. □

Remarques.

1. Le théorème de classification des modules de génération finie nous dit que de plus, les paires $(\lambda_1, \nu_1), \ldots, (\lambda_n, \nu_n)$ sont uniques à l'ordre près. Par l'exemple 3 d'application A-linéaire, on obtient une classification des endomorphismes d'un espace vectoriel complexe de dimension finie à conjuguaison près.
2. Pour les endomorphismes d'espaces vectoriels réels, on peut obtenir une classification légèrement plus compliquée en utilisant la caractérisation des éléments premiers de $\mathbb{R}[X]$ vue en exercice 36 du chapitre II.

Comme promis, nous terminons cette section, et ce cours, avec la preuve du théorème de décomposition dont nous avons maintenant exploré bien des conséquences. Cette démonstration étant très technique, il est recommandé de penser à $A = \mathbb{Z}$ avec f donné par la valeur absolue. (Le cas de $A = K$ un corps n'est pas très instructif : ce n'est rien d'autre que la preuve qu'une famille génératrice minimale dans un K-espace vectoriel est une base, voir remarque 1 en section III.2.)

Démonstration du théorème III.13. Soit A un anneau euclidien avec $f : A \setminus \{0\} \to \{1, 2, \ldots\}$ une application associée. Définissons le *rang* d'un A-module de génération finie comme le cardinal (fini) d'un ensemble de générateurs de taille minimale [16]. On va démontrer le théorème par récurrence sur le rang de M.

Par convention, un module de rang 0 est trivial, tandis que par définition, un module de rang 1 est cyclique. Dans ces deux cas, il n'y a rien à démontrer et le départ de récurrence est vérifié.

Soit donc M un A-module de rang $m \geq 2$, et supposons le théorème démontré pour tout A-module de rang au plus $m - 1$. Commençons par reformuler ce que l'on souhaite démontrer. On cherche à trouver des éléments $x_1, \ldots, x_m \in M$ tels que tout $x \in M$ s'écrive $x = b_1 x_1 + \cdots + b_m x_m$ avec $b_1, \ldots, b_m \in A$, et ce de manière unique dans le sens suivant : si on a $b_1 x_1 + \cdots + b_m x_m = b'_1 x_1 + \cdots + b'_m x_m$ avec $b_i, b'_i \in A$ pour tout i, on veut avoir $b_i x_i = b_i x'_i$ pour tout $i = 1, \ldots, m$ [17]. En effet, cela signifie précisément que M est la somme directe interne des sous-modules cycliques engendrés par $x_1, \ldots, x_m$.

Considérons un ensemble $x_1, \ldots, x_m$ de générateurs de M de taille minimale. Supposons qu'on ait la condition suivante :

$$\text{Si } a_1 x_1 + \cdots + a_m x_m = 0 \text{ avec } a_1, \ldots, a_m \in A, \text{ alors } a_1 x_1 = \cdots = a_m x_m = 0\,. \quad (*)$$

Cela impliquerait le théorème, puisque l'égalité $b_1 x_1 + \cdots + b_m x_m = b'_1 x_1 + \cdots + b'_m x_m$ peut s'écrire $(b_1 - b'_1)x_1 + \cdots + (b_m - b'_m)x_m = 0$, ce qui par la condition $(*)$ impliquerait $(b_i - b'_i)x_i = 0$ pour tout i, et donc $b_i x_i = b'_i x_i$ comme voulu. En revanche, si la condition $(*)$ n'est pas satisfaite [18], il existe des éléments $a_1, \ldots, a_m \in A$

16. Pour $A = K$ un corps, c'est la dimension de l'espace vectoriel.

17. Attention : contrairement au cas des espaces vectoriels, on ne demande pas d'avoir $b_i = b'_i$ pour tout i. Par exemple, dans le $\mathbb{Z}$-module cyclique $M = \mathbb{Z}/2\mathbb{Z}$ engendré par $x = [1]$, on a $1 \cdot [1] = 3 \cdot [1]$ malgré le fait que $1 \neq 3 \in \mathbb{Z}$.

18. Pour $A = K$ un corps, cela n'arrive jamais puisqu'une famille génératrice minimale est toujours libre, voir remarque 1 en section III.2.

non-tous nuls tels que $a_1x_1 + \cdots + a_mx_m = 0$. On a donc une "relation" pour les générateurs $x_1, \ldots, x_m \in M$ avec "coefficients" non-tous nuls $a_1, \ldots, a_m \in A$.

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 minimisant f. 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

$$b_1y_1 + \cdots + b_my_m = 0\,. \qquad (**)$$

La stratégie est maintenant de modifier y_1 en y_1^* de telle manière que M soit la somme directe interne du module cyclique engendré par y_1^* et du module engendré par $y_2, \ldots, y_m$. Les détails de l'argument reposent sur trois affirmations, dont voici la première.

Affirmation 1. Si $a_1y_1 + \cdots + a_my_m = 0$ avec $a_i \in A$, alors $b_1 \mid a_1$ dans A.

⌜ Comme A est euclidien et b_1 non-nul, il existe $q, r \in A$ tels que $a_1 = qb_1 + r$ avec $r = 0$ ou $f(r) < f(b_1)$. Or, les deux relations pour $y_1, \ldots y_m$ impliquent

$$0 = 0 - q \cdot 0 = (a_1y_1 + \cdots + a_my_m) - q(b_1y_1 + \cdots + b_my_m) = ry_1 + \cdots + (a_m - qb_m)y_m\,.$$

Par minimalité de b_1, on ne peut pas avoir $f(r) < f(b_1)$. 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 A.

⌜ Comme A est euclidien et b_1 non-nul, il existe $q, r \in A$ tels que $b_2 = qb_1 + r$ avec $r = 0$ ou $f(r) < f(b_1)$. Comme l'ensemble $y_1, \ldots, y_m$ engendre M, il en va de même pour la famille $y_1' \coloneqq y_1 + qy_2, y_2, \ldots, y_m$, et l'on a

$$b_1y_1' + ry_2 + b_3y_3 + \cdots + b_my_m = b_1y_1 + b_2y_2 + \cdots + b_my_m \overset{(**)}{=} 0\,.$$

Par minimalité de b_1, on ne peut pas avoir $f(r) < f(b_1)$, d'où $b_1 \mid b_2$. On procède de même pour $b_3, \ldots, b_m$. ⌟

Par cette affirmation, on peut écrire $b_i = q_ib_1$ avec $q_i \in A$ pour tout $i = 2, \ldots, m$. Considérons le sous-module $M_1 \subset M$ engendré par

$$y_1^* \coloneqq y_1 + q_2y_2 + \cdots + q_my_m\,,$$

et le sous-module $M_2 \coloneqq \{a_2y_2 + \cdots + a_my_m \,|\, a_2, \ldots, a_m \in A\}$ de M engendré par $y_2, \ldots, y_m$.

Affirmation 3. On a $M_1 + M_2 = M$ et $M_1 \cap M_2 = \{0\}$.

⌜ Comme $y_1, \ldots, y_m$ engendrent M, la définition de y_1^* implique qu'il en va de même pour $y_1^*, y_2, \ldots, y_m$. Cela montre que $M_1 + M_2 = M$.

Soit maintenant $x \in M_1 \cap M_2$. Il existe donc $a_1, \ldots, a_m \in A$ tels que $x = a_1y_1^* = a_2y_2 + \cdots + a_my_m$. Cela implique

$$0 = x - x = a_1y_1^* - a_2y_2 - \cdots - a_my_m = a_1y_1 + (a_1q_2 - a_2)y_2 + \cdots + (a_1q_m - a_m)\,.$$

Par l'affirmation 1, on a $a_1 = qb_1$ pour un certain $q \in A$, d'où

$$x = a_1 y_1^* = qb_1 y_1^* = q(b_1 y_1 + b_1 q_2 y_2 + \cdots + b_1 q_m y_m) = q(b_1 y_1 + \cdots + b_m y_m) \overset{(**)}{=} q \cdot 0 = 0\,.$$

Cela conclut la preuve de l'affirmation. ⌟

Comme on l'a déjà vu (voir remarque 2 en début de section III.4), cette affirmation est équivalente au fait que M est somme directe interne de M_1 et de M_2. Par définition, le sous-module M_1 est cyclique ; le rang de M_2 étant au plus $m - 1$, nous savons par hypothèse de récurrence que M_2 est somme directe interne d'un nombre fini de sous-modules cycliques. Il en va donc de même pour M, ce qui conclut la preuve. □

Exercices

1. (i) Montrer que les $\mathbb{F}_2$-espaces vectoriels coïncident avec les groupes abéliens dont chaque élément non-trivial est d'ordre 2.
   (ii) Vérifier que tout homomorphisme de groupes $f\colon E \to E'$ entre deux tels groupes abéliens est une application $\mathbb{F}_2$-linéaire.

2. Montrer que l'ensemble $\mathscr{P}(X)$ des parties d'un ensemble X muni de la différence symétrique est un espace vectoriel sur $\mathbb{F}_2$ (voir exercice 5 du chapitre I).
   Pour X fini, calculer sa dimension.

3. Soient X un ensemble et E un K-espace vectoriel. Montrer que l'ensemble des applications $E^X = \{f\colon X \to E\}$ est un K-espace vectoriel via les lois

$$(f + g)(x) = f(x) + g(x) \quad \text{et} \quad (\lambda \cdot f)(x) = \lambda \cdot f(x)$$

   pour $f, g \in E^X$, $x \in X$ et $\lambda \in K$.

4. (i) Montrer que pour tout $\lambda \in K^*$, l'application

$$\varphi_\lambda\colon E \longrightarrow E\,, \quad v \longmapsto \lambda \cdot v$$

   est un automorphisme du groupe abélien E.
   (ii) Vérifier de plus que l'application

$$\varphi\colon K^* \longrightarrow \mathrm{Aut}(E)\,, \quad \lambda \longmapsto \varphi_\lambda$$

   est un homomorphisme de groupes injectif.

5. Si un espace vectoriel E est somme directe externe $E = E_1 \oplus \cdots \oplus E_n$, montrer qu'il existe des sous-espaces vectoriels $F_1, \ldots, F_n \subset E$ tels que $F_i \simeq E_i$ pour $i = 1, \ldots, n$ et tels que E est somme directe interne de $F_1, \ldots, F_n$.

6. (i) Vérifier que si F est un sous-espace vectoriel d'un espace vectoriel E sur K, alors le groupe abélien quotient E/F est un espace vectoriel via la loi

$$\lambda \cdot [v] = [\lambda \cdot v]\,,$$

   pour $v \in E$ et $\lambda \in K$.

(ii) Montrer que la projection canonique $\pi : E \to E/F$ est une application linéaire de noyau F.

(iii) En déduire que toute application linéaire $f : E \to E'$ définit un isomorphisme linéaire

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

7. On sait que $\mathbb{R}$ est un espace vectoriel sur $\mathbb{Q}$. Montrer que les éléments $1, \sqrt{2} \in \mathbb{R}$ sont linéairement indépendants sur $\mathbb{Q}$.

8. Soit K un corps et I l'idéal de $K[X]$ engendré par X^2. Montrer que $K[X]/I$ est un espace vectoriel sur K. Quelle est sa dimension ?

9. Quel est le cardinal d'un $\mathbb{F}_p$-espace vectoriel de dimension n ?

10. (i) Montrer qu'un espace vectoriel de dimension finie sur $\mathbb{Q}$ est dénombrable.

(ii) Vérifier que $\mathbb{R}$ n'est pas de dimension finie sur $\mathbb{Q}$.

11. Soient F_1, F_2 deux sous-espaces d'un espace E, et $f : F_1 \to (F_1 + F_2)/F_2$ l'application linéaire donnée par la composition de l'inclusion de F_1 dans $F_1 + F_2$ avec la projection canonique $F_1 + F_2 \to (F_1 + F_2)/F_2$.

(i) Montrer que f est surjective, de noyau $F_1 \cap F_2$.

(ii) En conclure que si E est de dimension finie, on a l'égalité

$$\dim(F_1 + F_2) = \dim(F_1) + \dim(F_2) - \dim(F_1 \cap F_2)\,.$$

(iii) Qu'obtient-on dans le cas où $F_1 \cap F_2 = \{0\}$?

12. (i) Montrer que si $f : E \to E$ est une application linéaire injective ou surjective avec E de dimension finie, alors f est un isomorphisme.

(ii) Donner un contre-exemple à cet énoncé dans le cas d'un espace vectoriel quelconque.

13. Montrer que tout groupe abélien $(M, +)$ est un module sur l'anneau $A = \mathrm{End}(M)$, défini à l'exercice 3 du chapitre I, via la loi $\varphi \cdot x = \varphi(x)$ pour $\varphi \in \mathrm{End}(M)$ et $x \in M$.

14. Montrer que si B est un sous-anneau d'un anneau A, alors A est un module sur B. En conclure que tout anneau de caractéristique n est un module sur $\mathbb{Z}/n\mathbb{Z}$.

15. Soient $\varphi : M \to M'$ un homomorphisme de A-modules, et N' un sous-module de M'. Montrer que $\varphi^{-1}(N')$ est un sous-module de M.