Groupes et Applications

J. Féjoz
jacques.fejoz@dauphine.fr
Université Paris-Dauphine, Ceremade

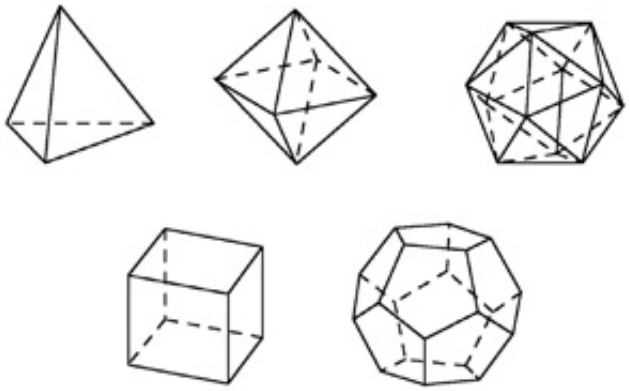
Printemps 2020

Table des matières

Introduction

La découverte des cinq polyèdres réguliers, [1] décrits à la fin des *Éléments* d'Euclide, peut être considérée comme la plus remarquable réussite mathématique de l'Antiquité.

0.1 Théorème (Solides platoniciens)**.** *Il existe cinq polyèdres réguliers dans l'espace ; on les nomme* tétraèdre*,* cube*,* octaèdre*,* dodécaèdre *et* icosaèdre*.* [2]



À chaque polyèdre régulier correspond son polyèdre dual, dont les sommets sont les centres des faces du premier. Un polyèdre et son dual sont invariants par le même "sous-groupe" fini du "groupe" des rotations ; à ce stade, on peut entendre "groupe" dans le sens où Galois l'utilisait, à savoir un simple ensemble de symétries, avec l'idée qu'on peut composer ces symétries pour en obtenir de nouvelles. Le tétraèdre est auto-dual, le cube et l'octaèdre sont duaux l'un de l'autre, ainsi que le dodécaèdre et l'icosaèdre. Les groupes correspondants, notés T, O et Y, sont d'ordre respectif

$$|T| = 12, \quad |O| = 24, \quad |Y| = 60.$$

0.a Exercice. Montrer que T contient l'identité, 8 rotations d'angle $\pi/3$ et dont l'axe passe par un sommet du tétraèdre et le milieu du côté opposé, et 3 rotations d'angle π et dont l'axe joint les milieux de deux côtés opposés.

Le théorème 0.1 découle du fait de théorie des groupes selon lequel les seuls sous-groupes finis du groupe des rotations dans l'espace à trois dimensions sont

— les groupes cycliques $C_n = \mathbb{Z}/n\mathbb{Z}$,

— les groupes dihédraux D_n (D_n étant le groupe de symétrie du polygone régulier à n sommets, dans le plan [3])

1. Soit P un polyèdre convexe borné dans $\mathbb{R}^n$. Notons G_P son groupe de symétrie G_P, soit l'ensemble des rotations qui le préservent. Un *drapeau* de P est un ensemble $D = \{P_0, P_1, ..., P_{n-1}\}$, où P_i est une face i-dimensionnelle de P et $P_i \subset P_{i+1}$. P est *régulier* si G_P agit transitivement sur l'ensemble des tous les drapeaux de P (c'est-à-dire que l'ensemble des drapeaux n'a qu'une seule orbite sous l'action de G_P).

2. Un *n-èdre* est un polyèdre à n faces. Le cube s'appelle donc aussi l'hexaèdre.

3. Un polgone régulier peut être vu comme un polyèdre dégénéré plan.

— les groupes T, O et Y.[4]

On trouvera une démonstration directe de cette classification des sous-groupes finis de SO_3 dans le livre de Sternberg [Ste94], avec en plus des explications sur le lien avec l'hypothèse atomique et la cristallogrphie.

0.b Exercice. Vérifier le théorème en utilisant la formule d'Euler-Poincaré reliant les nombres de sommets s, de faces f et d'arêtes a [Hat02, Chapitre 2] :

$$s - a + f = 2.$$

Indication : on pourra exprimer a en fonction du nombre n d'arêtes par sommet et du nombre p d'arêtes par face (la régularité du polyèdre se traduisant par le fait que n et p sont constants), pour en déduire que $s(1 - \frac{n}{2} + \frac{n}{p}) = 2$.

Les groupes ci-dessus sont les symétries les plus profondes découvertes dans l'Antiquité. La classification des "groupes de Lie simples" occupe une place analogue au 19e et 20e siècle. Un groupe de Lie est un groupe continu muni d'une structure différentielle compatible avec sa loi de groupe (sur lequel on peut donc faire du calcul infinitésimal) ; un exemple est le groupe SO_3 des rotations dans $\mathbb{R}^3$. Un groupe est simple s'il est indécomposable en plus petits sous-groupes. Ces groupes représentent les symétries les plus subtiles, qui puissent être décrites par les mathématiques modernes.

0.2 Théorème. *Les groupes de Lie classiques suivants sont simples*[5] *:*

1. *Groupes compacts : SU_n ($n > 1$), SO_n ($n \neq 1, 2, 4$), SpU_n ($n \geqslant 1$)*
2. *Groupes complexes : $SL_n(\mathbb{C})$ ($n > 1$), $SO_n(\mathbb{C})$ ($n \neq 1, 2, 4$), $Sp_{2n}(\mathbb{C})$ ($n \geqslant 1$).*

Il existe un énoncé beaucoup plus précis. Et il s'avère qu'il existe exactement, en plus des séries ci-dessus et de la série analogue des groupes algébriques, cinq groupes de Lie simples, qui n'appartiennent à aucune famille infinie. Ces derniers, qualifiés d'*exceptionnels* et notés E_6, E_7, E_8, G_2 et F_4, ont pour dimensions $78, 133, 248, 14$ et 52. Et, de même que Platon associait les polyèdres réguliers aux quatre éléments du feu, de l'air, de la Terre et de l'eau (réservant le dodécaèdre comme le symbole du cosmos), les physiciens de notre temps tentent de trouver des lois générales dictant la variété des particules élémentaires en termes de divers groupes de Lie, tels que $U(1)$ (électrons-positrons), SU_2 (nucléons), SU_3 (quarks), etc.

Ce cours est une introduction à la théorie des groupes et quelques unes de leurs applications, à la géométrie, à la physique, et aux extensions de corps, avec le parti pris d'offrir un point de vue plus panoramique qu'exhaustif, parfois au prix d'un manque de précision certain. Heureusement, le sujet est couvert par de nombreux ouvrages excellents, parmi lesquels nous recommandons les livres de M.

4. Dans la suite du cours, on notera ces groupe T^+, O^+ et Y^+, tandis que T, O et Y désigneront les groupes des isométries, directes ou indirectes, des mêmes polyèdres.

5. Ces groupes seront définis par la suite, ainsi que la propriété d'être simple, qui n'est pas exactement la même pour les groupes de Lie et pour les groupes abstraits.

Artin [Art91], de S. Sternberg [Ste94] ou de I.R. Shafarevich [Sha05]. Les articles mathématiques de *Wikipedia*, notamment ceux en anglais, sont aussi remarquablement utiles.

Les exercices font partie intégrante du cours et, si on ne les résoud pas tous, il est nécessaire au moins de lire leur énoncé.

1 Notion de groupe de transformations

Si X est un ensemble, une *transformation (bijective)* de X est une bijection $f : X \circlearrowleft$. L'ensemble $\mathrm{Trans}(X)$ des transformations de X est muni de la loi de composition, qui associe, à tout couple (f, g) de transformations, une troisième, notée $f \circ g$ et définie par

$$(f \circ g)(x) = f(g(x)).$$

1.1 Définition. Une partie G de $\mathrm{Trans}(X)$ est un *groupe de transformations* si elle vérifie ces trois axiomes :

— G est unifère : $\mathrm{id} \in G$
— G est stable par la loi de composition : $f \circ g \in G$ (si $f, g \in G$)
— G est stable par inversion : $f^{-1} \in G$ (si $f \in G$).

Rappelons que l'inverse f^{-1} est ici l'unique transformation de G telle que $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}$. [6]

Par exemple, $\mathrm{Trans}(X)$ et $\{\mathrm{id}\}$ sont trivialement des groupes de transformation.

1.2 Exemple. Si E est un espace vectoriel, les automorphismes linéaires de E forment un groupe de transformations de E, appelé le *groupe linéaire* et noté $GL(E)$. On note parfois $GL(E) = \mathrm{Aut}(E)$, car il est entendu que ce qu'on appelle automorphisme d'un espace vectoriel est en réalité un automorphisme linéaire.

Si G est un groupe de transformations de X et $x \in X$, l'*orbite* de x est $Gx = \{g(x),\ g \in G\}$, tandis que le *stabilisateur* de x est $G_x = \{g \in G,\ g(x) = x\}$.

Groupes dihédral et cyclique

Soit

$$P_n = \left\{ \exp \frac{i2\pi k}{n},\ k = 0...n-1 \right\}$$

le *polygone régulier* à n sommets. Le *groupe dihédral* et le *groupe cyclique* associés sont

$$\begin{cases} D_n = \{f \in O_2,\ f(P_n) = P_n\} \\ C_n = D_n \cap SO_2. \end{cases}$$

6. Pour lever toute ambiguité, par exemple dans le cas où $X = \mathbb{R}$ ou $\mathbb{C}$, on pourrait noter plus explicitement $f^{\circ -1}$, pour distinguer cette transformation de celle, pas toujours définie, $x \mapsto 1/f(x)$.

1.a Exercice. Montrer que D_n et C_n sont des groupes de transformations de $\mathbb{R}^2$, de cardinaux respectifs $2n$ et n.

La généralisation de ces groupes en dimension 3 (ou plus) sera abordée dans la suite, et est liée aux solides platoniciens évoquées dans l'introduction.

Groupe des déplacements d'un espace euclidien

Rappelons qu'un *espace euclidien* est un espace vectoriel réel E de dimension finie, muni d'une forme bilinéaire g non-dégénérée (la matrice de g dans une base quelconque a un détemrinant non nul) positive ($g(x,x) \geqslant 0$) définie ($g(x,x) \neq 0$ si $x \neq 0$) ; g s'appelle une *produit scalaire euclidien.*

Un *déplacement* ou une *isométrie* de E est une transformation de E telle que

$$d(f(x), f(y)) = d(x,y) \quad \text{(pour tous } x, y),$$

où la distance d est la distance induite par g :

$$d(x,y) = \sqrt{g(x-y, x-y)}.$$

On note $D(E)$ l'ensemble des déplacements de E ; c'est un groupe de transformations de E.

Rappelons par ailleurs que, si E est un espace vectoriel, une *transformation affine* de E est une application $f : E \circlearrowleft$ de la forme

$$f(x) = f(0) + \varphi(x), \tag{1}$$

où $\varphi \in GL(E)$ (autrement dit, f est la composée d'une transformation linéaire puis d'une translation) ; $f(0)$ est la partie constante de f, et φ est sa *partie linéaire.*

1.3 Complément (Groupe affine d'un espace affine)**.** Un *espace affine* dirigé par un espace vectoriel E est un ensemble $\mathcal{E} \neq \varnothing$ muni d'une application

$$\varphi : \mathcal{E}^2 \to E, \quad (A,B) \to v = \overrightarrow{AB}.$$

et vérifiant les deux axiomes suivants :

— transitivité [7] : pour tous $A \in \mathcal{E}$ et $v \in E$, il existe un unique $B \in \mathcal{E}$, noté $B = A+v$, tel que $v = \overrightarrow{AB}$

— relation de Chasles : $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$.

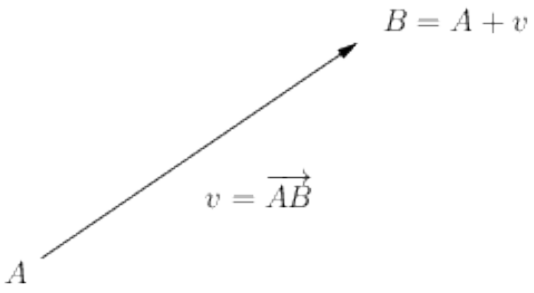
Si $\mathcal{E}$ est un espace affine dirigé par E, et si O est un point quelconque de $\mathcal{E}$, l'application $\mathcal{E} \to E$, $A \mapsto \overrightarrow{OA}$ est une bijection qui envoie le point O sur le vecteur nul 0_E (pourquoi ?), qui permet d'identifier $\mathcal{E}$ à E. Cette identification dépend du choix de O et, dans ce sens, un espace affine est un espace vectoriel dont on a oublié l'origine.

Réciproquement, tout espace vectoriel E possède un espace affine sous-jacent, défini par l'application $\varphi : (x,y) \mapsto \overrightarrow{xy} = y - x$.

Une application $f : \mathcal{E} \to \mathcal{F}$ entre deux espaces affines dirigés respectivement par les espaces vectoriels E et F est *affine* si il existe $\varphi \in L(E,F)$ telle que

$$f(B) - f(A) = \varphi(\overrightarrow{AB});$$

7. Cette terminologie sera expliquée dans le chapitre sur les actions de groupes.



on note $\mathrm{Aff}(\mathcal{E}, \mathcal{F})$ l'ensemble des telles applications affines, et $\mathcal{G}\,\mathrm{Aff}(\mathcal{E})$ le groupe des transformations affines de $\mathcal{E}$. En particulier, on peut récupérer f à partir de $\vec{f}$ et de l'image par f d'un point unique $O \in \mathcal{E}$, puisque

$$f(A) = f(O) + \varphi(\overrightarrow{OA}).$$

La définition (1) d'une transformation affine d'un espace vectoriel E est la transposition de la définition précédente d'application affine dans le cas où l'on identifie un espace vectoriel E à l'espace affine sous-jacent.

1.b Exercice. Montrer qu'un déplacement f de E est affine, i.e. de la forme

$$f(x) = c + \varphi(x)$$

avec $c \in E$ et $\varphi \in GL(E)$; on pourra montrer que φ préserve le produit scalaire et est linéaire.

On note $O(E) = D(E) \cap GL(E)$ l'ensemble des isométries vectorielles de E. Il est lui aussi un groupe de transformations de E. La dernière propriété de l'exercice suivant justifie qu'on aussi appelle les isométries vectorielles des *transformations orthogonales* ou des *opérateurs orthogonaux*.

1.c Exercice.
Soit $f \in GL(E)$. Montrer l'équivalence entre les propriétés suivantes :

1. f préserve le produit scalaire euclidien
2. f préserve la norme euclidienne
3. f préserve la distance euclidienne (i.e. est isométrique)
4. f envoie toute base orthonormée sur une base orthonormée
5. la matrice M de f dans une base orthonormée vérifie $M^T M = I$.

Autres exemples

Groupes de symétries moléculaires

Les molécules sont constituées d'atomes d'un ou plusieurs éléments chimiques. Une symétrie moléculaire est un déplacement dans l'espace qui envoie chaque atome de la molécule sur un atome du même élément. Par exemple, la molécule de méthane CH_4 est faite de 4 atomes d'hydrogène situés au somet d'un tétraèdre régulier, et d'un atome de carbonne situé en son centre. Donc son groupe de symétrie est le groupe T de symétrie du tétraèdre régulier.

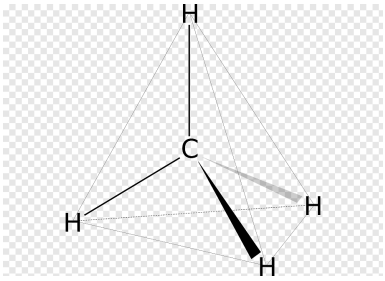


FIGURE 1 – Molécule de méthane CH_4

Groupes cristallographiques

Les cristaux sont des solides dont les molécules sont agencées de façon à ce qu'il existe en son sein un petit ensemble de molécules, appelé *motif*, qui engendre tout le cristal par déplacements.

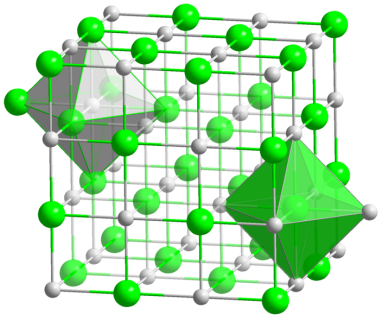


FIGURE 2 – Cristal de $NaCl$ (sel)

Une symétrie de ce cristal est un déplacement qui envoie chaque atome du cristal sur un atome du même élément. Les groupes de symétries ainsi obtenus s'appellent les *groupes cristallographiques*.

Groupes de Galilée et de Poincaré

Les symétries des lois de la Physique sont des caractéristiques importantes de ces lois. Ces "symétries" sont les transformations de l'espace-temps qui préservent les lois. Par exemple, les lois de la Mécanique sont préservées par changement de repères galiléens, c'est-à-dire par changement de coordonnées de la forme

$$x' = x - vt \;\; t' = t$$

en mécanique classique, et

$$x' = \frac{x - vt}{\sqrt{1 - (v/c)^2}}, \;\; t' = \frac{t - (v/c)^2 x}{\sqrt{1 - (v/c)^2}}$$

en relativité spéciale, où c est la célérité de la lumière dans le vide. Les groupes correspondants sont le *groupe de Galilée-Newton* et le *groupe de Lorentz* (dont

Poincaré a remarqué qu'il était le groupe de symétrie des équations de Maxwell en électromagnétisme).

1.4 Complément. Suite à ces exemple, il peut être utile de dire un mot de la notion de catégorie en mathématiques. En première approximation, une *catégorie* est une entité formée

— d'*objets* d'une part, qui sont les ensembles munis d'une certaine structure

— de *morphismes*, qui sont les applications entre objets qui conservent la structure.

Des catégories classiques sont les suivantes :

— la catégorie $\mathfrak{Ens}$ des ensembles (sans structure particulière) et des applications

— la catégorie $\mathfrak{EuclLin}$ des espaces vectoriels euclidiens et des isométries linéaires

— la catégorie $\mathfrak{E}_{\mathbb{C}}$ des espaces vectoriels complexes et des applications $\mathbb{C}$-linéaires

— la catégorie $\mathfrak{T}$ des espaces topologiques et des applications continues

— la catégorie $\mathfrak{Mes}$ des espaces mesurables et des applications mesurables.

Au sein de chaque catégorie, les *endomorphismes* sont les morphismes d'un objet dans lui-même, les *isomorphismes* sont les morphismes inversibles dont l'inverse aussi est un morphisme, les *automorphismes* sont les endomorphismes qui sont aussi des isomorphismes (ce que nous avons appelé les *transformations*), les *monomorphismes* sont les morphismes injectifs, et les *épimorphismes* sont les morphismes qui sont aussi surjectifs. Ces notions dépendent ainsi de la catégorie considérée.

La notion générale de catégorie en mathématique est une abstraction de la définition précédente, qui inclut des catégories dans lesquelles les morphismes ne sont pas des applications (un exemple est la catégorie des homotopies entre espaces topologiques pointés).

Certaines constructions permettent d'associer, à tout objet d'une catégorie, un objet d'un autre catégorie, et de même avec les morphismes. Ces constructions s'appellent des *foncteurs*. Par exemple, en topologie algébrique, on essaye d'associer à chaque espace topologique un ou des groupes, et à chaque application continue un ou des morphismes de groupes.

2 Notion de groupe

La notion de groupe (abstrait) est une abstraction de celle de groupe G de transformations d'un ensemble X, où l'on se concentre sur la loi de composition des éléments de G, en oubliant totalement l'ensemble de X. Cette notion plus pauvre a permis de comprendre ce qu'il y avait de commun dans beaucoup de groupes de transformations agissant sur des ensembles différents, et a ainsi considérablement clarifié les problèmes de classification.

2.1 Définition. Un *groupe* est un ensemble G muni d'une loi de composition interne $G \times G \to G$, $(x, y) \mapsto xy$, aussi appelée *multiplication*, vérifiant les axiomes suivants :

1. Associativité : $x(yz) = (xy)z$
2. G possède un élément neutre e ($xe = ex = x$ pour tout x)
3. Tout élément est inversible (pour tout x il existe un élément noté x^{-1} tel que $xx^{-1} = x^{-1}x = e$).

L'*ordre* de G est son cardinal, dans $\mathbb{N}_* \cup \{\infty\}$; il se note $|G|$.

On note alors x^k l'élément de G défini par récurrence par les formules

$$x^0 = e,\ x^{k+1} = xx^k.$$

G est *commutatif* si $xy = yx$ pour tous x, y. Il est alors d'usage de noter l'opération de G additivement : $x + y$ au lieu de xy ou $x \times y$, nx au lieu de x^n ($n \in \mathbb{N}$).

Des exemples de groupes commutatifs sont : $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}, \times), (E, +)$ si E est un espace vectoriel. Un groupe non commutatif (si $n \geqslant 2$) est $(GL_n(\mathbb{R}), \times)$.

2.a Exercice.
Montrer que, dans un groupe,

1. l'élément neutre est unique
2. pour tout x, l'inverse de x est unique
3. $xy = xz \Rightarrow y = z$ et $yx = zx \Rightarrow y = z$
4. $xy = e \Rightarrow y = x^{-1}$
5. $(xy)^{-1} = y^{-1}x^{-1}$.

2.2 Définition. Une partie H d'un groupe G est un *sous-groupe* si la loi induite par restriction de celle de G est une loi de groupe de H (en particulier, la restriction de la loi $G \times G \to G$ à $H \times H$ est à valeurs dans H, i.e. H est stable par produit) ; on note $H \leqslant G$.

2.3 Lemme. *Un sous-groupe de G contient l'élément neutre et est stable par produit et inversion.*

Démonstration. Soit $H \leqslant G$. Par définition, H est stable par produit. Supposons que $e' \in H$ soit neutre pour les éléments de H. En particulier, $e'e' = e'$ dans G, donc $e' = e$. Donc H est stable par inversion. □

2.b Exercice. Soit $H \subset G$. Montrer que les propriétés suivantes sont équivalentes :

1. $H \leqslant G$ i.e. H est stable par produit
2. H est non vide et stable par produit et inversion
3. H est non vide et, pour tous $x, y \in H$, $xy^{-1} \in H$

Nous allons maintenant décrire une façon très efficace de construire des sous-groupes ; cette méthode sera d'ailleurs généralisée ultérieurement pour construire des groupes (qui ne se présentent pas comme des sous-groupes).

2.4 Définition. Si X est une partie de G, le *sous-groupe engendré par X* est

$$\langle X \rangle = \bigcap_{X \subset H \leqslant G} H.$$

2.c Exercice. 1. Montrer que $\langle X \rangle$ est bien un sous-groupe (modulo quoi c'est donc le plus petit sous-groupe de G, pour l'inclusion, contenant X).

2. Montrer que $\langle X \rangle$ est l'ensemble des produits finis d'élements de la forme x ou x^{-1} avec $x \in X$:

$$\langle X \rangle = \left\{ x_1 ... x_k,\ k \in \mathbb{N},\ x_i \in X \text{ ou } x_i^{-1} \in X\ (\forall i) \right\}$$

où, quand $k = 0$, cette écriture désigne conventionnellement e.

En particulier ($n = 1$), si $x \in G$,

$$\langle x \rangle = \{x^k,\ k \in \mathbb{Z}\},$$

et l'on définit l'*ordre* de x comme $|x| = |\langle x \rangle|$.

2.d Exercice. 1. Montrer que, si $x \in G$,

$$|x| = \min\{k \in \mathbb{N}_*,\ x^k = e\}.$$

2. Quel est l'ordre des éléments de D_n ?

2.5 Définition. Une application $f : G \to G'$ entre deux groupes est un *morphisme de groupes* si

$$f(xy) = f(x)f(y) \quad (\text{pour tous } x, y \in G).$$

Notons que, dans l'égalité précédente, le produit xy est relatif à la loi de groupe de G, tandis que le produit $f(x)f(y)$ est relatif à celle de G'. (On pourrait noter plus explicitement $x \times_G y$ etc.)

Comme déjà mentionné dans le complément 1.4, si f est un morphisme, il existe des noms plus précis dans les cas particuliers suivants :

— f bijective : f *isomorphisme* (et l'on note alors $G \xrightarrow{\sim} G'$ et l'on dit que G et G' sont isomorphes)
— $G = G'$: f *endomorphisme* (et l'on note $f : G \circlearrowleft$)
— $f : G \circlearrowleft$ bijective : f *automorphisme* (on note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G)
— f injective : *monomorphisme* (et l'on note $f : G \hookrightarrow G'$)
— f surjective : *épimorphisme* (et l'on note $f : G \twoheadrightarrow G'$).

2.e Exercice.
Soit $f : G \to G'$ un morphisme de groupes. Montrer :

1. $f(e) = e'$
2. $f(x^{-1}) = f(x)^{-1}$
3. si f est un isomorphisme, f^{-1} est un morphisme
4. si de plus $g : G' \to G''$ est un morphisme de groupes, $g \circ f$ est un morphisme de groupes.

Deux groupes isomorphes sont, du strict point de vue de leur structure de groupe, indiscernables. On dit qu'ils appartiennent à la même classe d'isomorphie. La question ultime de la théorie des groupes serait de décrire toutes les classes d'isomorphie.

2.f Exercice. Soit G un groupe. Montrer que

1. si G est engendré par l'un de ses éléments (on dit que G est *monogène*), G est commutatif ;
2. si tous les éléments de G sont d'ordre $\leqslant 2$, G est commutatif.

2.g Exercice. Décrire les (classes d'isomorphie de) groupes non commutatifs d'ordre $\leqslant 8$. On pourra s'aider de leur *table de Cayley* (i.e. leur table de multiplication), utiliser le théorème de Lagrange 4.4, et admettre l'existence du groupe quaternionique (voir l'exercice 9.e).

2.6 Exemple (Premier groupe d'homotopie d'un espace métrique). Soient X un espace métrique et $\xi \in X$. Un *lacet* partant de ξ sur X est un chemin continu $c : [0,1] \to X$ tel que $c(0) = c(1) = \xi$. On s'intéresse à l'espace Γ_ξ des tels lacets, qui est un espace "de dimension infinie" (par exemple si X est un ouvert de $\mathbb{R}^n$). Si c, $\bar{c} \in \Gamma_\xi$, on note $\bar{c}c$ le chemin obtenu en parcourant d'abord c, puis $\bar{c}$; $\bar{c}c$ s'appelle la *concaténation* de c et de $\bar{c}$. Cette concaténation est définie sur l'intervalle de temps $[0,2]$ de sorte que $\bar{c}c \notin \Gamma_\xi$. On pourrait reparamétrer ce lacet de façon à le parcourir entièrement sur l'intervalle de temps $[0,1]$, donc deux fois plus vite. Mais ce reparamétrage n'a rien d'unique, et l'on va en fait procéder à une opération plus radicale, consistant à identifier les chemins obtenus par reparamétrage mais aussi par déformation continue.

Deux tels chemins c et $\bar{c}$ sont *homotopes* si il existe une application continue $C : [0,1]^2 \to X$, appelée *homotopie*, telle que
— $C(0,\cdot) = c$ et $C(1,\cdot) = \bar{c}$ (donc C interpole entre c et $\bar{c}$)
— $C(\cdot,0) = C(\cdot,1) = \xi$.
Il s'agit là d'une relation d'équivalence sur X_ξ, et l'on note $\pi_1(X,\xi)$ le quotient de X_ξ (i.e. $\pi_1(X,\xi)$ est l'ensemble des classes d'équivalences). On peut vérifier que la loi de concaténation des lacets induit une loi de groupe sur $\pi_1(X,\xi)$, pour laquelle l'élément neutre est la classe d'homotopie du lacet constant $t \mapsto \xi$ et l'inverse d'une classe d'homotopie $[c]$ est la classe d'homotopie du lacet $t \mapsto c(1-t)$ obtenu en parcourant c en sens inverse (exercice). $\pi_1(X,\xi)$ est le *premier groupe d'homotopie*, ou le *groupe de Poincaré* de (X,ξ). En fait, il dépend très peu du choix de ξ puisque, si X est connexe, $\pi_1(X,\xi)$ et $\pi_1(X,\xi')$ sont isomorphes. Donc on peut le noter $\pi_1(X)$.

Par exemple, on montre que $\pi_1(\mathbb{T}^n) = \mathbb{Z}^n$. Ainsi, la "dimension" n de $\mathbb{Z}^n$ (n s'appelle le *rang* du groupe $\mathbb{Z}^n$) compte le nombre de trous. En général, le groupe d'homotopie capture des propriétés qui ne se laissent pas décrire par un simple nombre. Ici, les groupes apparaissent donc comme une généralisation de la notion de nombre.

2.7 Complément (Conjecture de Poincaré)**.** On montre aussi que le premier groupe d'homotopie de la sphère $\mathbb{S}^n$ est trivial si $n \geqslant 2$. Poincaré a conjecturé que toute "variété fermée" (des espaces topologiques compacts localement euclidiens) de dimension 3 dont le groupe de Poincaré est trivial est homéomorphe à $\mathbb{S}^3$. Le résultat analogue en dimension 2 était connu au 19e siècle. En grande dimension ($\geqslant 5$), il est une conséquence du théorème du h-cobordisme, qui a valu la médaille Fields à Stephen Smale en 1966. En dimension 4, il fut démontré par Michael Freedman, qui a ainsi obtenu la médaille Field en 1986. La conjecture de Poincaré, en dimension 3, resta longtemps énigmatique – les spécialistes ne pouvant pas même exclure qu'elle fût fausse —), jusqu'aux travaux de

Thurston sur les variétés de dimension 3, et de Richard Hamilton sur le flot de Ricci des variétés riemanniennes. Grigori Perelman la démontra finalement, en surmontant une série de redoutables obstacles, qu'Hamilton n'avait pu franchir. Il refusa la médaille Fields et le Millenium Prize de un million de dollars qui lui furent offerts, estimant, dans une rare démonstration d'intégrité, que d'autres avaient participé à la démonstration du théorème.

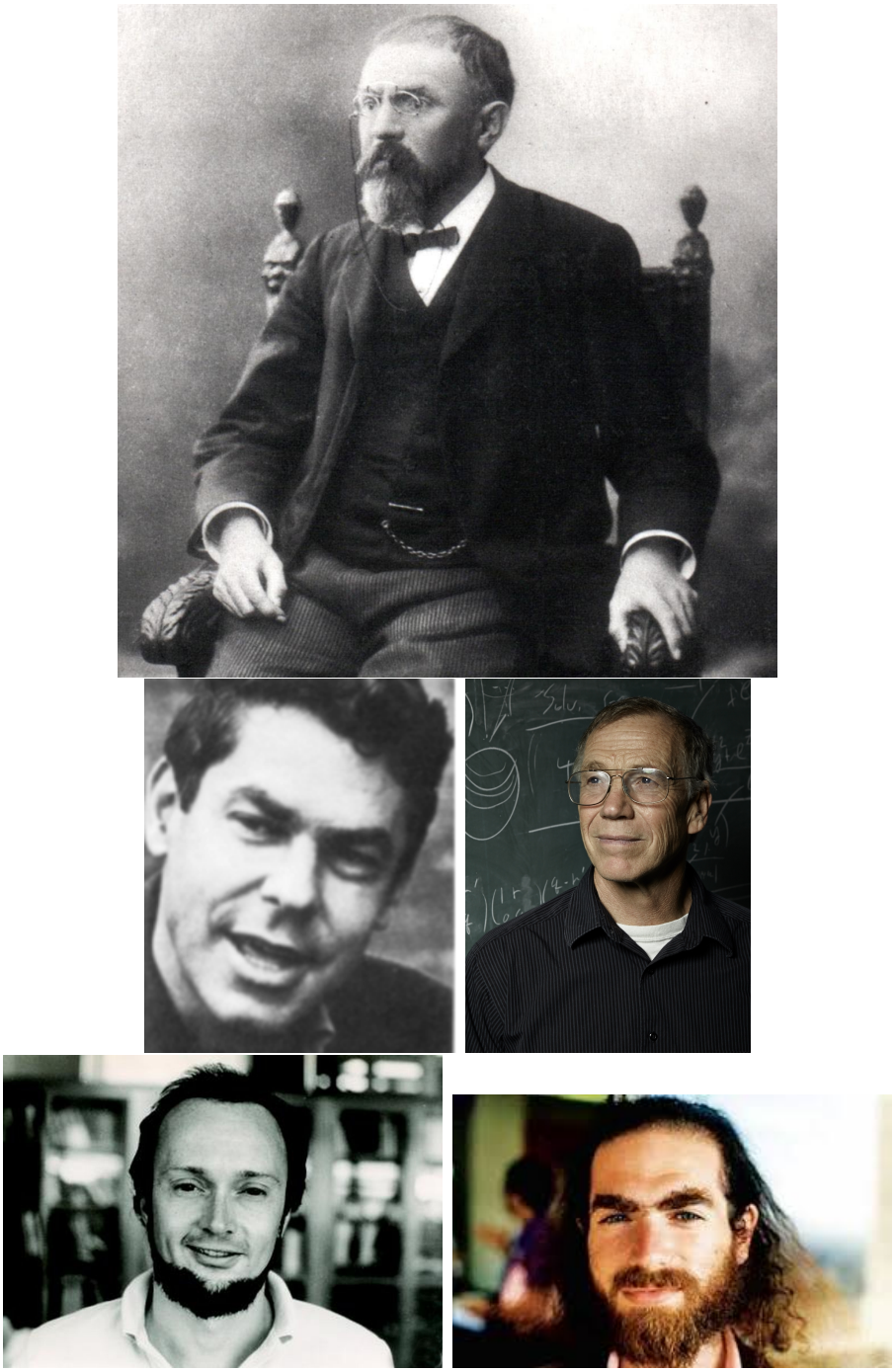


FIGURE 3 – Les mathématiciens Henri Poincaré (1854-1912), Stephen Smale (1930), Michael Freedman (1951), Richard Hamilton (1943) et Grigori Perelman (1966)

3 Théorèmes de Sylow

Les trois théorèmes de Sylow (admis) permettent de décrire les sous-groupes d'ordre premier d'un groupe fini arbitraire. Soient G un groupe d'ordre n, p un diviseur premier de n et e le plus grand entier tel que p^e divise n, de sorte que

$$n = p^e m$$

pour un certain entier m qui n'est pas multiple de p.

3.1 Théorème (Premier théorème de Sylow)**.** *Il existe un sous-groupe de G d'ordre p^e ; un tel sous-groupe s'appelle un* sous-groupe de Sylow*, ou un p-*sous-groupe de Sylow*.*

3.a Exercice. Trouver un élément de G d'ordre p.

3.b Exercice. Montrer qu'il existe exactement deux classes d'isomorphisme de groupes d'ordre 6. Quelles sont-elles ?

Le deuxième théorème de Sylow est plus technique.

3.2 Théorème (Deuxième théorème de Sylow)**.** *Soient K un sous-groupe de G dont l'ordre est un multiple de p, et H un p-sous-groupe de Sylow de G. Il existe un sous-groupe H' conjugué à H (i.e. il existe $g \in G$ tel que $H' = gHg^{-1}$), tel que $K \cap H'$ est un sous-groupe de Sylow de K.*

3.c Exercice. En déduire que :
- Si K est un sous-groupe de G dont tous les éléments ont un ordre qui est une puissance de p (on dit que K est un *p-groupe*), K est contenu dans un p-sous-groupe de Sylow de G.
- Les p-sous-groupes de Sylow de G sont tous conjugués.

3.3 Théorème (Troisième théorème de Sylow)**.** *Soit s le nombre de p-sous-groupes de Sylow de G. Alors s divise m et est congru à 1 modulo p :*

$$s|m \quad et \quad s = ap + 1, \quad a \in \mathbb{N}.$$

3.d Exercice. Trouver les 2-sous-groupes de Sylow de D_{10}.

4 Action d'un groupe sur un ensemble

La notion de groupe est une remarquable abstraction de celle de groupe de transformation, destinée à étudier la structure intrinsèque d'une loi de groupe, indépendamment des transformations d'ensemble particulières que les éléments du groupe représentent. Les actions de groupes sont l'ingrédient manquant à un groupe, pour réaliser (*représenter*, dit-on) ses éléments comme des transformations.

4.1 Définition. Une *action* d'un groupe G sur un ensemble X, ou encore une *représentation* de G sur X, est un morphisme de groupes

$$f : G \to \mathrm{Trans}(X), \quad g \mapsto f(g) : x \mapsto f(g)(x) =: g \cdot x.$$

FIGURE 4 – Ludwig SYLOW (1832-1918), mathématicien norvégien

L'*orbite* de $x \in X$ est

$$G \cdot x = \{g \cdot x,\ g \in G\} \subset X.$$

Le fait que f soit un morphisme dit que

$$g_1 \cdot (g_2 \cdot x) = (g_1 g2) \cdot x.$$

4.a Exercice. Montrer que les orbites de f forment une partition de X.

4.2 Définition. L'*ensemble des orbites* de X sous l'action de G se note $G\backslash X$.[8] L'action est *transitive* si X ne possède qu'une orbite.

Si G est donné comme un groupe de transformations de X, il "agit" tautologiquement sur X, via

$$g \cdot x = g(x).$$

Si X possède une structure supplémentaire, il est souvent intéressant de considérer les actions à valeurs dans le groupe $\mathrm{Aut}(X)$ des automorphismes de X. Par exemple,

- si X est un espace vectoriel, une *représentation linéaire* de G sur X est une action de G à valeurs dans $GL(X)$;
- si X est un espace de Hilbert, une *représentation unitaire* de G sur X est une action de G à valeurs dans le groupe $U(X)$ des transformations unitaires de X, etc.

Les représentations linéaires et unitaires sont particulièrement importantes dans l'étude des groupes. D'ailleurs, toute action $f : G \to \mathrm{Trans}(X)$ induit une représentation linéaire $\tilde{f} : G \to GL(\mathcal{F}(\tilde{X}, \mathbb{R}))$, où $\tilde{X}$ est l'espace vectoriel réel engendré

8. On définit aussi une action *à droite* de G sur X comme une application $(x, g) \mapsto x \cdot g$ telle que $(x \cdot g) \cdot g' = x \cdot (gg')$ (à comparer à $g' \cdot (g \cdot x) = (g'g) \cdot x$ pour une action telle qu'on l'a définie, à gauche). L'ensemble des orbites d'une action à droite se note alors X/G.

par X [9] et $\mathcal{F}(\tilde{X}, \mathbb{R})$ est l'espace vectoriel réel des fonctions sur $\tilde{X}$, définie par

$$g \cdot \varphi = \varphi \circ g^{-1} \quad (\forall \varphi \in \mathcal{F}(X, \mathbb{R}),\ g \in G).$$

On verra qu'il en est de même avec les représentations unitaires.

4.b Exercice. Soit Y est une partie d'un ensemble X sur lequel un groupe G agit. Montrer que le *fixateur* et le *stabilisateur* de Y, soient

$$\begin{cases} Fix(Y) = \{g \in G,\ g \cdot y = y\ (\forall y \in Y)\} \\ Stab(Y) = \{g \in G,\ g \cdot y \in Y\ (\forall y \in Y)\}, \end{cases}$$

sont des sous-groupes de G.

Dans la suite de cette section nous décrivons plusieurs exemples.

Actions de $\mathbb{R}$ et $\mathbb{Z}$ vues comme des systèmes dynamiques

Considérons une action f de $\mathbb{Z}$ sur un ensemble X. La bijection $f(1) : M \circlearrowleft$ définit une transformation de f. Réciproquement, si φ est une transformation de X, l'application

$$f : \mathbb{Z} \to \mathrm{Trans}(X), \quad k \mapsto \varphi^{\circ k}$$

est une action de $\mathbb{Z}$ sur X. Donc la donnée d'une action de $\mathbb{Z}$ sur X est équivalente à celle d'un système dynamique à temps discret (inversible) sur X.

Soit maintenant une action f de $\mathbb{R}$ sur une variété différentielle M. Supposons que l'application $(t, x) \mapsto f(t)(x)$ soit dérivable. Définissons le champ de vecteurs v sur M par

$$v(x) = \left.\frac{d}{dt}\right|_{t=0} f(t)(x).$$

4.c Exercice. Montrer que, pour tous t, x,

$$\begin{cases} \frac{d}{dt} f(t)(x) = v(f(t)(x)) \\ f(0)(x) = x, \end{cases} \tag{2}$$

i.e. f est le flot de v.

Réciproquement, soit v est un champ de vecteurs sur variété différentielle M (complet signifie ici que toutes ses courbes intégrales sont définies pour tout temps).

4.d Exercice. Montrer que le flot f de v, défini par le problème de Cauchy (2), est une action de $\mathbb{R}$ sur M :

$$f(s) \circ f(t) = f(s + t).$$

Indication : utiliser l'unicité des solutions maximales du problème de Cauchy.

Donc la donnée d'une action de $\mathbb{R}$ sur X est équivalente, sous hypothèse de dérivabilité, à celle d'un système dynamique à continu (inversible) sur X.

9. Autrement dit, $\tilde{X}$ est l'espace vectoriel réel des combinaisons linéaires formelles d'éléments de X.

Action par conjugaison

Soient X est un ensemble et $\mathrm{End}(X)$ l'ensemble des endomorphismes de X (applications $X \circlearrowleft$, pas forcément inversibles). Le groupe $\mathrm{Aut}(X)$ des automorphismes de X agit sur $\mathrm{End}(X)$ par la formule

$$g \cdot f = g \circ f \circ g^{-1}.$$

Les endormorphismes f et $g \cdot f$ sont dit *conjugués* et un orbite sous cette action s'appelle une *classe de conjugaison*.

4.e Exercice. Montrer que, si $x \in X$ est un point périodique de f, $g(x)$ est un point périodique de $g \cdot f$.

Plus généralement, les propriétés dynamiques de f et de $g \cdot f$ sont qualitativement les mêmes, puisque g peut être vu comme un changement de coordonnées par lequel f est transformé en $g \cdot f$:

$$\begin{array}{ccc} X & \xrightarrow{f} & X \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} \\ X & \xrightarrow{g \cdot f} & X \end{array}$$

La théorie qualitative des systèmes dynamiques a donc pour objet l'étude des classes de conjugaison des endomorphismes f.

Un premier exemple est l'action naturelle du groupe $\mathfrak{S}_n = \mathrm{Trans}(\{1, ..., n\})$ sur $\{1, ..., n\}$. Une orbite s'appelle aussi un *cycle*. Si $\sigma \in \mathfrak{S}_n$ possédant k cycles, la *signature* de σ est

$$\epsilon(\sigma) = (-1)^{n-k},$$

où k est le nombre de cycle $(= \sharp\{1, ..., n\}/\langle\sigma\rangle)$.

Un autre cas particulier important est celui des matrices carrées. $GL_n(\mathbb{R})$ agit sur $X = M_n(\mathbb{R})$ par la même formule

$$g \cdot x = gxg^{-1},$$

où, dans le membre de droite, on a maintenant le produit de trois matrices ; les matrices x et $g \cdot x$ sont dites *conjuguées* ou (en France) *semblables*. Une orbite de cette action s'appelle conséquemment une *classe de similitude*. Pour tout $n \geqslant 1$, il existe une infinité de classes de similitudes (puisque deux matrices semblables ont mêmes valeurs propres), classifiées par leur *forme normale de Jordan*.

4.f Exercice. Montrer que, si deux matrices réelles sont semblables sur $\mathbb{C}$, elles le sont sur $\mathbb{R}$. (La théorie de Galois permettra de répondre facilement, par exemple, à la question analogue pour des matrices à coefficients dans $\mathbb{Q}$.)

De même, le groupe des difféomorphismes g sur une variété différentielle M agit sur les applications $f : M \circlearrowleft$ par la formule

$$g \cdot f = g \circ f \circ g^{-1}.$$

Équivalence gauche-droite des applications

Soient X et Y deux ensembles. Le groupe $\mathrm{Aut}(X) \times \mathrm{Aut}(Y)$ agit sur l'ensemble des applications $X \to Y$ par la formule

$$(g, h) \cdot f = g \circ f \circ h^{-1}.$$

Les endormorphismes f et $g \circ f \circ h^{-1}$ sont dit *équivalents*.

Le cas des matrices est classique : $GL_m(\mathbb{R}) \times GL_n(\mathbb{R})$ agit sur l'espace $X = M_{mn}(\mathbb{R}) = L(\mathbb{R}^n, \mathbb{R}^m)$ des matrices (rectangulaires) par la formule

$$(g, h) \cdot x = gxh^{-1}$$

Une orbite de cette action est une *classe d'équivalence*. Les classes s'équivalences sont classifiées par le rang $r \in \{0, 1, ..., \min(m, n)\}$ des matrices, et sont donc au nombre fini de $1 + \min(m, n)$.

4.g Exercice. Montrer que deux matrices de mêmes dimensions sont équivalentes si et seulement si leurs rangs sont égaux.

Action d'un groupe sur lui-même

4.3 Définition.

1. *Action à gauche* : $L_g x = g \cdot x = gx$
2. *Action à droite* : $R_g x = g \cdot x = xg^{-1}$
3. *Action adjointe* ou *action par conjugaison* : $Ad_g x = gxg^{-1}$.

4.h Exercice. Les actions L et R sont à valeurs dans $\mathrm{Trans}(G)$ (bijections de G dans lui-même), tandis que Ad est à valeurs dans $\mathrm{Aut}(G)$ (automorphismes de G).

Soit H un sous-groupe de G. Une action quelconque de G sur lui-même induit, par restriction à H, une action de H sur G. Prenons les exemples de l'action à gauche et de l'action adjointe :

— L'orbite d'un élément $g \in G$ sous l'action à gauche de H est

$$Hg = \{hg,\ h \in H\};$$

une telle orbite s'appelle la *classe à gauche de g modulo H*. Comme on l'a déjà remarqué (exercice 4.a), les orbites forment une partition de G, i.e. $G = \cup_{g \in G} Hg$ se décompose en l'union disjointe de ses classes à gauche.
Dans un groupe fini, l'*indice* de H dans G est le nombre, noté $(G : H)$, des classes à gauche de H. Comme toutes les classes ont même cardinal, à savoir celui de H (l'application $H \to Hg$, $h \mapsto hg$ est une bijection), on voit que

$$|G| = (G : H)\,|H|. \tag{3}$$

— L'orbite d'un élément $g \in G$ sous l'action adjointe de H est

$$\{hgh^{-1},\ h \in H\};$$

une telle orbite s'appelle la *classe de conjugaison de* g sous l'action de H. Deux éléments h et h' de la même classe de conjugaison sont dits *conjugués*.

La formule (3) implique le théorème suivant, capital pour décrire les sous-groupes de G.

4.4 Théorème. *Si H est un sous-groupe d'un groupe fini G, l'ordre de H divise celui de G.*

4.5 Définition. Deux sous-groupes H et H' de G sont *conjugués* s'il existe $g \in G$ tel que $H' = gHg^{-1}$.

4.i Exercice.
1. Montrer que deux sous-groupes conjugués sont isomorphes.
2. Si G agit sur un ensemble X et si x et y ont même orbite, montrer que les stabilisateurs de x et de y sont conjugués.
3. Quels sont les sous-groupes conjugués de D_3 ?

4.j Exercice. Soit G un groupe agissant sur un ensemble X. Montrer que le cardinal de X vaut

$$|X| = \sum_{\alpha \in G\backslash X} (G : G_{x_\alpha}),$$

où, pour toute orbite α, $x_\alpha \in \alpha$. On pourra commencer par traiter le cas où l'action est transitive.

4.k Exercice. Soient T le groupe des symétries du tétraèdre régulier, et T^+ le sous-groupe des rotations de T (voir figure 5). Quels éléments de T^+ sont conjugués ?

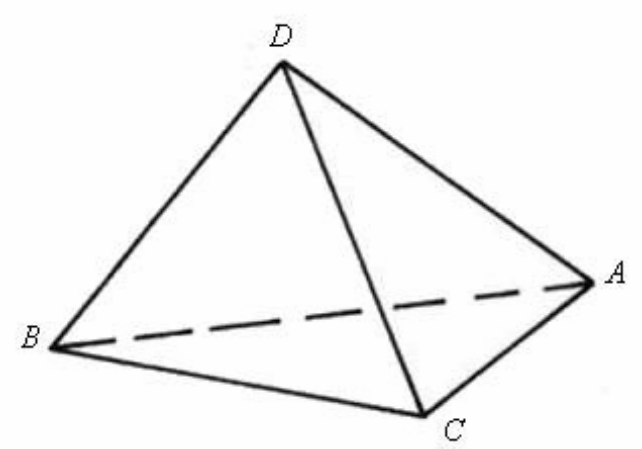


FIGURE 5 – Tétraèdre régulier

5 Notion de quotient, arithmétique modulaire

Rappelons l'idée générale des quotients d'ensemble ; il s'agit d'un procédé fondamental pour construire de nouveaux ensembles à partir d'anciens, en regroupant

des éléments par paquets. Soient X un ensemble et $\mathcal{Q}$ une partition de X, c'est-à-dire un ensemble de parties non vides (appelées les *classes*) de X tel que

— $\mathcal{Q}$ recouvre X :

$$X = \cup_{A\in\mathcal{Q}} A$$

— Les classes distinctes de $\mathcal{Q}$ ne se chevauchent pas :

$$A, B \in \mathcal{Q} \Rightarrow A = B \text{ ou } A \cap B = \varnothing.$$

Pour tout $x \in X$, il existe donc une classe $\bar{x} \in \mathcal{Q}$ contenant x (propriété de recouvrement), et cette classe est unique (seconde propriété). On peut ainsi définir la *surjection canonique*

$$p : X \to \mathcal{Q}, \quad x \mapsto \bar{x}$$

qui, à un élément, associe l'unique classe dont il est un représentant. Le fait de représenter une même classe $A \in \mathcal{Q}$, pour deux éléments de X, définit une relation d'équivalence :

$$x \sim y \Leftrightarrow \bar{x} = \bar{y},$$

et réciproquement la relation d'équivalence détermine $\mathcal{Q}$. La partition $\mathcal{Q}$ s'appelle le *quotient* de X par $\sim$ et l'on note $\mathcal{Q} = X/\sim$.

Enfin, un *domaine fondamental* ou un *système fondamental de représentants* est une partie de X possédant un unique représentant dans chaque classe.

5.1 Exemple (Un angle comme une classe de nombres). Considérons la partition de $\mathbb{R}$ suivante :

$$\mathbb{T} = \big\{x + 2\pi\mathbb{Z},\ x \in \mathbb{R}\big\}. \tag{4}$$

Elle est associée à la relation d'équivalence

$$x \sim y \Leftrightarrow x - y \in 2\pi\mathbb{Z}$$

(si $x \in \mathbb{R}$, sa classe d'équivalence est $\bar{x} = x + 2\pi\mathbb{Z}$). Les éléments de $\mathbb{T}$ sont appelés des *angles*.

Dans cette définition de $\mathbb{T}$, les parties $x + 2\pi\mathbb{Z}$ ne sont bien sûr pas distinctes deux à deux (pour deux x, y, soit $x + 2\pi\mathbb{Z} = y + 2\pi\mathbb{Z}$, soit $x + 2\pi\mathbb{Z} \cap y + 2\pi\mathbb{Z} = \varnothing$). Pour décrire $\mathbb{T}$ de façon non redondante, remarquons que, pour tout $y \in \mathbb{R}$, il existe un unique $x \in [0, 2\pi[$ tel que $\bar{x} = \bar{y}$ (exercice) ; x s'appelle la *détermination principale* de y. [10] L'intervalle $[0, 2\pi[$ est donc un système fondamental de représentants, et l'on obtient toutes les classes en se limitant aux classes des $x \in [0, 2\pi[$ [11] :

$$\mathbb{T} = \big\{x + 2\pi\mathbb{Z},\ x \in [0, 2\pi[\big\}.$$

L'addition de $\mathbb{R}$ "passe au quotient", au sens où la formule

$$\bar{x} + \bar{y} = \overline{x + y}$$

10. Parfois on choisit plutôt $x \in]-\pi, \pi[$.

11. I est en bijection avec $\mathbb{T}$, mais n'en est pas une parfaite "image", du point de vue de la topologie, parce que par exemple la suite $2\pi - \frac{1}{n}$ tend vers le nombre 2π, dont la classe n'est pas représentée par 2π mais par 0.

définit bien une addition sur $\mathbb{T}$. Ce n'est pas parfaitement évident parce que le membre de gauche ne doit dépendre que des classes $\bar{x}$ et $\bar{y}$, tandis que le membre de droite est calculé à partir de deux représentants particuliers x et y de ces classes. Heureusement, si $x' = x + 2k\pi$ et $y' = y + 2l\pi$ sont deux autres représentants des classes de x et de y,

$$x' + y' = x + y + 2(k + l)\pi$$

donc

$$\overline{x' + y'} = \overline{x + y},$$

de sorte que l'addition des classes est bien définie.

5.a Exercice. 1. La moitié d'un angle est-elle un angle ?

2. Le produit de deux angles est-il un angle ?

5.2 Exemple (Espace vectoriel quotient). Si E est un espace vectoriel et F un sous-espace vectoriel de E, le *quotient* de E par F est la partition notée E/F formée des classes $\bar{x} = x + F$ de vecteurs $x, y \in E$ tels que $x - y \in F$. On montre comme précédemment que l'addition de E et la multiplication externe par un scalaire passent au quotient, et induisent donc une structure d'espace vectoriel sur E/F, pour laquelle l'application de passage au quotient, $x \mapsto \bar{x}$, est linéaire.

Par exemple, si $(E, \mathcal{E}, \mu)$ est un espace mesuré, l'espace de Lebesgue $L^p(E, \mathcal{E}, \mu)$ est le quotient de

$$\mathcal{L}^p(E, \mathcal{E}, \mu) = \left\{ f : E \to \mathbb{R} \text{ mesurable}, \int |f|^p \, d\mu < \infty \right\}$$

par le sous-espace des fonctions nulles presque partout.

5.3 Exemple (Arithmétique modulaire). L'exemple principal de ce chapitre est l'*arithmétique modulaire*. Fixons $n \in \mathbb{Z}$. On note

$$\bar{x} = x + n\mathbb{Z} \quad (x \in \mathbb{Z})$$

et

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{x}, \quad x \in \mathbb{Z}\}.$$

5.b Exercice. 1. Quelle est la relation d'équivalence associée à cette partition de $\mathbb{Z}$?

2. Trouver un système fondamental de représentants, et en déduire le cardinal de $\mathbb{Z}/n\mathbb{Z}$; on pourra utiliser la *division euclidienne* sur $\mathbb{Z}$: pour tout $k \in \mathbb{Z}$, il existe un unique $(q, r) \in \mathbb{Z}$ tel que

$$k = nq + r, \quad 0 \leqslant r \leqslant n - 1.$$

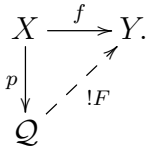
3. Montrer que l'addition et la multiplication de $\mathbb{Z}$ passent au quotient ; ces opérations font de $\mathbb{Z}/n\mathbb{Z}$ un *anneau* et définissent l'*arithmétique modulaire*.

5.4 Théorème (Propriété universelle du quotient). *Soient X un ensemble et $\sim$ une relation d'équivalence X. Il existe un ensemble $\mathcal{Q}$ et une application $p : X \to \mathcal{Q}$ vérifiant la propriété suivante :*

Quels que soient un ensemble Y et une application $f : X \to Y$ telle que $x \sim x' \Rightarrow f(x) = f(x')$,[12] *il existe une unique application $F : \mathcal{Q} \to Y$ telle que*

$$F(p(x)) = f(x);$$

on écrit alors que le diagramme d'applications suivant commute :



De plus, Q est unique à bijection près, i.e. si $p' : X \to \mathcal{Q}'$ est une application vérifiant la même propriété, il existe une bijection $\mathcal{Q} \to \mathcal{Q}'$; un tel ensemble $\mathcal{Q}$ (défini à bijection près) s'appelle un quotient *de X par la relation d'équivalence, et p s'appelle une* application de passage au quotient.

Les flèches ne vont pas dans le bon sens pour qu'on puisse définir F à partir de f par une simple composition d'application parce que, comme on le verra, l'application p n'est généralement pas inversible ; on dit que f *se factorise par p.*

La propriété vérifiée par $p : X \to \mathcal{Q}$ est qualifiée d'*universelle* parce qu'elle résoud un problème de factorisation *pour toute application f partant de X* telle que $x \sim x' \Rightarrow f(x) = f(x')$ (par opposition à si la propriété était vérifiée seulement pour *une* application f donnée).

Attention, la propriété universelle affirme l'existence d'une unique application F vérifiant certaines propriétés, tandis que la seconde affirmation concerne l'unicité de $\mathcal{Q}$ et de p.

Démonstration. Existence du quotient. Soient $\mathcal{Q} = X/\sim$ et $p : X \to Q$, $x \mapsto \bar{x}$.

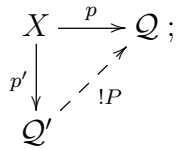
Si l'application F existe, elle est unique (c'est-à-dire déterminée par f) puisque, pour tout $\alpha \in \mathcal{Q}$, si l'on choisit un représentant $x \in \alpha$, on a $F(\alpha) = f(x)$.

Réciproquement, F existe. En effet la formule $F(\alpha) = f(x)$ avec $x \in \alpha$ définit bien F puisque, si x' est un autre représentant de α, par hypothèse sur f on a $f(x) = f(x')$.

Donc notre construction de $\mathcal{Q}$ et de p résoud le problème posé.

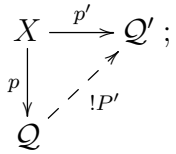
Unicité du quotient. Supposons qu'un autre ensemble Q' et une autre application $p' : X \to \mathcal{Q}'$ satisfont la même propriété universelle que (Q, p). Nous allons montrer que Q et Q' sont en bijection. On va pour cela appliquer la propriété universelle du quotient à quatre reprises :

1. propriété de p' appliquée à $f = p$:

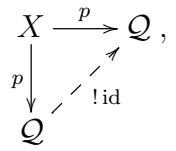


12. Cette hypothèse sur f dit que la partition des niveaux de f subordonne celle des classes d'équivalence de la relation $\sim$.

2. propriété de p appliquée à $f = p'$:

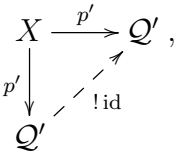


3. propriété de p appliquée à $f = p$:



mais d'après ce qui précède on a aussi $p = P \circ p' = P \circ P' \circ p$, donc $P \circ P' = \mathrm{id}$;

4. propriété de p' appliquée à $f = p'$:



mais d'après ce qui précède on a aussi $p' = P' \circ p = P' \circ P \circ p'$, donc $P' \circ P = \mathrm{id}$.

Donc P et P' sont les bijections réciproques l'une de l'autre, et $\mathcal{Q} \simeq \mathcal{Q}'$.[13] □

De prime abord, ce type de "propriété universelle" peut sembler inutilement abstraite. Mais, comme elle caractérise l'objet construit à isomorphisme (ici, bijection) près, elle permet souvent de d'oublier totalement la construction particulière faite de cet objet pour n'en retenir que la substantifique moelle.

5.5 Exemple. Si $f : \mathbb{R} \to \mathbb{R}$ est une fonction paire, il existe une unique fonction $F : [0, +\infty[\to \mathbb{R}$ telle que $f(x) = F(|x|)$ parce que $[0, +\infty[$ est un système fondamental de représentants de la relation d'équivalence $x \sim y \Leftrightarrow |x| = |y|$ et donc s'identifie à $\mathbb{R}/\sim$. On peut montrer de plus que F possède la même régularité que f : si f est de classe C^k (avec $k \in \mathbb{N} \cup \{+\infty, \omega\}$), F aussi.

5.6 Exemple. Une fonction 2π-périodique $f : \mathbb{R} \to \mathbb{R}$ définit une unique fonction $F : \mathbb{T} = \mathbb{R}/2\pi\mathbb{Z} \to \mathbb{R}$. On peut montrer de plus que F possède la même régularité que f.

5.7 Complément. Le théorème de division de Weiersrass-Malgrange permet de montrer des factorisations (appelées aussi divisions) dans le contexte plus général d'actions de groupes. Par exemple, si une fonction réelle f de n variables réelles est symétriques (au sens où elle est invariante par l'action de $\mathfrak{S}_n$ sur ses variables), elle se factorise par l'*application de Viète* (voir 13) via une application F. Si f est analytique, F est unique et analytique. Si f est C^∞, F est aussi C^∞, mais généralement pas unique ! En classe différentiable, c'est un tour de force, dû à René Thom, d'avoir eu l'intuition de ce théorème, et à Bernard Malgrange de l'avoir démontré.

13. Ce schéma de démonstration se retrouve dans quantité de constructions, et peut-être formalisé grâce à la notion de *foncteur représentable*.

6 Groupes abéliens finis

Dans un groupe abélien, tous les sous-groupes sont distingués. On décrit ci-dessous la classification des groupes abéliens finis.

On note $\mathbb{Z}_n : \mathbb{Z}/n\mathbb{Z}$.

6.a Exercice (Lemme chinois)**.** Montrer que si a et b sont deux entiers naturels premiers entre eux, $\mathbb{Z}_{ab} \simeq \mathbb{Z}_a \times \mathbb{Z}_b$.

Par récurrence on en déduit que, si un entier naturel n a pour décomposition en facteurs premiers

$$n = p_1^{a_1} \cdots p_k^{a_k},$$

alors

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}.$$

6.1 Théorème. *Si G est un groupe abélien fini, il existe des nombres premiers $p_1, ..., p_k$ et des entiers $a_1, ..., a_k \geqslant 1$ tels que G soit isomorphe à*

$$\mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}.$$

De plus, les p_i et les a_i sont uniques à l'ordre près.

Démonstration. D'après le lemme chinois, il suffit de montrer que G est isomorphe à un produit de plusieurs groupes de la forme $\mathbb{Z}_n$, $n \in \mathbb{N}\backslash\{0, 1\}$. À rédiger... □

6.b Exercice (Petits groupes abéliens finis)**.** Quels sont les groupes abéliens finis d'ordre $\leqslant 8$, à isomorphisme près ?

7 Groupes quotients

Dans le chapitre 4, nous avons défini le quotient $G\backslash X$ d'un ensemble X par l'action d'un groupe G. [14] Il s'agit de la partition induite par la relation d'équivalence

$$x \sim y \Leftrightarrow \text{il existe } g \in G \text{ tel que } y = g \cdot x.$$

Nous allons ici nous concentrer sur le cas de l'action à gauche (ou à droite) sur un groupe G de l'un de ses sous-groupes H. La structure de groupe de G passe-t-elle au quotient ? La réponse est... pas toujours !

La réponse est positive uniquement dans le cas où H est "super-symétrique" (dans un sens qu'on va définir).

Pour voir que certains sous-groupes sont plus symétriques que d'autres, introduisons la définition suivante, qui rappelle son analogue pour les applications linéaires.

14. On écrit G à gauche de X parce que les actions telles qu'on les a définies sont en fait des actions à gauche, alors qu'on peut aussi définir des actions à droite, habituellement notées $x \cdot g$ au lieu de $g \cdot x$.

7.1 Définition. Soit $f : G \to G'$ un morphisme de groupes.

— Le *noyau* de f est

$$\ker f = \{g \in G,\ f(g) = e'\} \subset G.$$

— L'*image* de f est

$$\operatorname{im} f = \{f(g),\ g \in G\} \subset G'.$$

7.a Exercice.

1. Montrer que le noyau et l'image de f sont des sous-groupes.
2. Vérifier que f est injectif si et seulement si $\ker f = \{e\}$. (La caractérisation analogue de la surjectivité est tautologique : f est surjectif si et seulement si $\operatorname{im} f = G'$.)
3. Montrer que, pour tous $g \in G$ et $h \in \ker f$, $ghg^{-1} \in \ker f$, i.e. $\ker f$ est stable par l'action adjointe de G.
4. Montrer que cette propriété n'est pas toujours vérifiée par les sous-groupes ; on pourra trouver un sous-groupe K de D_3, par exemple, tel qu'il existe $g \in D_3$ tel que $gKg^{-1} \notin K$. Construire un morphisme de groupes dont K soit l'image (tandis que ce qui précède montre que K n'est le noyau d'aucun morphisme de groupes).

7.2 Définition. $H \leqslant G$ est *distingué* ou *normal* si, pour tous $g \in G$ et $h \in H$,

$$ghg^{-1} \in H;$$

on note alors $H \lhd G$.

7.3 Exemple. Le groupe dihédral D_3 est engendré par une rotation r et une réflexion s. On a vu que $\langle r \rangle \lhd D_3$ mais que $\langle s \rangle$ n'est pas distingué dans D_3.

7.b Exercice. Montrer que les propriétés suivantes sont équivalentes :

1. $H \lhd G$
2. Pour tout $g \in G$, $gHg^{-1} = H$ (i.e. H est un point fixe de l'action de G par conjugaison sur l'ensemble des sous-groupes de G)
3. Pour tout $g \in G$, $gH = Hg$ (la classe à gauche modulo H d'un $g \in G$ quelconque, et sa classe à droite modulo H, coïncident) [15]
4. La décomposition de G en classes modulo N est compatible avec la multiplication de G i.e. la loi de G induit une loi sur l'ensemble des classes à droite de G modulo H.

7.c Exercice. Montrer que si G est un groupe fini d'ordre n et H un sous-groupe d'ordre $n/2$, H est distingué.

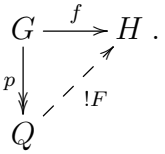
7.d Exercice. Le *centre* d'un groupe G est l'ensemble des éléments x de G qui commutent avec tous les éléments de G ($xg = gx$ pour tout $g \in G$). Montrer que le centre est un sous-groupe distingué de G.

7.e Exercice. Soient $f : G \to F$ un morphisme de groupes et H un sous-groupe distingué de F. Montrer que $f^{-1}(H)$ est distingué dans G.

15. Les actions à gauche et à droite de H ne sont pas les mêmes en général, mais ont alors mêmes orbites.

7.4 Théorème (Propriété universelle du groupe quotient)**.** *Soit $N \lhd G$. Il existe un groupe Q et un morphisme $p : G \twoheadrightarrow Q$ vérifiant la propriété suivante :*

> *Pour tout groupe H et tout morphisme $f : G \to H$ tel que $N \leqslant \ker f$, il existe un unique morphisme $F : Q \to H$ tel que le diagramme suivant commute :*



De plus, Q est unique à isomorphisme près

Le "problème universel" va être résolu par la construction suivante.

7.5 Définition. Le *quotient* de G par un sous-groupe distingué H est l'ensemble

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

des classes à droite modulo H (d'après l'exercice 7.b, G/H est aussi l'ensemble $H\backslash G$ des classes à gauche), muni de la loi induite par celle de G par passage au quotient :

$$(g_1H)(g_2H) = (g_1g_2)H.$$

En particulier, l'élément neutre de G/H est la classe $eH = H$ de l'élément neutre, et, pour tout $g \in G$, l'inverse de gH est $g^{-1}H$. Les calculs dans G/H se font de façon très semblable aux calculs dans G (en remplaçant les $x \in G$ par leur classe $\bar{x} \in G/H$), avec la règle supplémentaire que $\bar{h} = H = \bar{e}$ pour tout $h \in H$. Le fait que H soit un sous-groupe distingué de G assure que l'ajout de cette règle supplémentaire ne détruit aucunement la cohérence qu'on avait pour la loi de groupe de G.

Démonstration du théorème. Existence. Soient $Q = G/N$ et $p : G \to G/N$ l'application de passage au quotient, $x \mapsto xN$. Soit $f : G \to H$ avec $N \subset \ker f$. Si $F : Q \to H$ existe comme voulue, elle est unique puisque

$$F(xN) = f(x) \quad (\forall x \in G);$$

cette formule définie bien une application sur Q parce que si $x' = xn$ ($x \in G, n \in N$) on a $f(x') = f(x)f(n) = f(x)$. De plus, l'application F est bien un morphisme de groupes :

$$F(xN\,yN) = F(xyN) = f(xy) = f(x)f(y) = F(xN)F(yN).$$

Unicité. La démonstration est analogue à celle de la propriété d'unicité dans le théorème 5.4. □

7.f Exercice. Soit $f : G \to H$ un morphisme de groupes. Montrer que f induit un isomorphisme

$$\operatorname{im} f \xrightarrow{\sim} G/\ker f.$$

7.g Exercice. Soit H le sous-groupe distingué de D_4 engendré par la symétrie centrale. D_4/H est-il isomorphe au groupe D_4^+ des rotations du carré ou au groupe des symétries du losange ?

7.h Exercice. Soient $K \leqslant H \leqslant G$, tels que K et H soient distingués dans G. Montrer qu'alors H/K est un sous-groupe distingué de G/K et que

$$(G/K)/(H/K) \simeq G/H.$$

7.i Exercice. Soient E un espace vectoriel euclidien. Le sous-groupe $O(E)$ des isométries vectorielles et le sous-groupe $T(E) \simeq E$ des translations sont-ils des sous-groupes distingués du groupe $D(E)$ des déplacements ?

7.j Exercice. Quels sont les sous-groupes distingués du groupe T^+ des rotations du tétraèdre (voir l'exercice 4.k) ? Identifier les groupes quotients correspondants.

7.k Exercice. Est-il possible que deux sous-groupes distingués d'un même groupe G soient non-isomorphes tandis que les quotients correspondants soient isomorphes ?

7.6 Définition. Un groupe est *simple* s'il ne possède pas d'autre sous-groupe distingué que $\{e\}$ et lui-même.

Les groupes simples jouent un rôle primordial dans la classification des groupes, puisque les groupes qui ne sont pas simples peuvent se "dévisser" en un sous-groupe et une extension de ce sous-groupe par un sous-groupe distingué. La classification des extensions elles-mêmes n'est pas pour autant facile.

7.7 Complément (Classification des groupes finis simples)**.** La classification des groupes finis simples a été plus ou moins achevée dans les années 1980, bien que des doutes persistent sur certaines parties de la démonstration, notamment concernant les groupes quasi-minces (cette partie en elle-même est longue d'environ 2 000 pages).

On connaît plusieurs familles infinies de groupes finis simples :
— les groupes cycliques C_p d'ordre premier
— les groupes alternés A_n de degré $n \geqslant 5$
— les groupes de type Lie finis $G(k)$ (dont les groupes classiques sur les corps finis).
Dans les années 1860, Émile Mathieu découvrit cinq groupes finis simples qui ne font partie d'aucune de ces familles infinies ; ce sont des groupes de permutations, maintenant appelés les *groupes de Mathieu* M_{11}, M_{12}, M_{22}, M_{23} et M_{24}, que Mathieu étudia dans sa thèse. Par exemple, M_{24} est d'ordre 244 823 040. Entre 1965 et 1975, on découvrit 21 autres groupes finis simples supplémentaires, et l'on dût se convaincre qu'il n'en existait pas d'autres que ces 26 groupes, qualifiés de *sporadiques*. Le plus grand de ces groupe, le groupe Monstre ou groupe de Fischer-Griess F_1, est d'ordre environ 8.10^{53}. Son existence a d'abord été conjecturée en 1973, puis il a été construit en 1980 par Robert Fischer, comme le groupe d'automorphismes de "l'algèbre de Griess", une algèbre non associative, mais commutative, à 196 884 dimensions. La démonstration de son existence n'a en fait jamais été publiée en détail.

Citons encore un exemple de théorème célèbre, sur le sujet des groupes finis simples. Celui-ci a été démontré en 1953 après avoir été conjecturé 50 ans plus tôt.

7.8 Théorème (Feit-Thompson)**.** *Un groupe fini simple non abélien est d'ordre pair.*

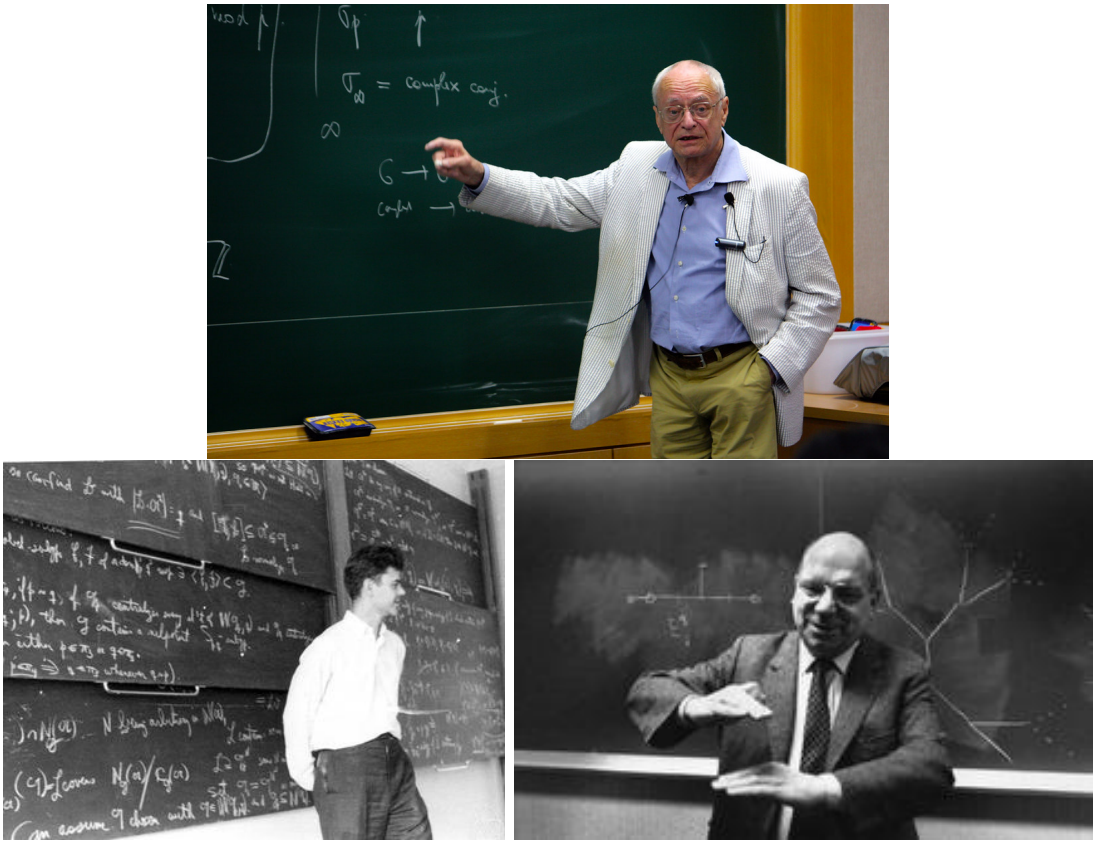


FIGURE 6 – Les mathématiciens Jean-Pierre Serre (1926), Jacques Tits (1930) et John G. Thomson (1932), parmi beaucoup d'autres, ont contribué à la classification de groupes finis simples

8 Produit semi-direct

L'archétype le plus trivial de groupe qui ne soit pas simple est le produit direct $G \times G'$ de deux groupes (muni de la loi produit $(g_1, g_1')(g_2, g_2') = (g_1 g_2, g_1' g_2')$). Dans un tel groupe, les sous-groupes $G \times \{e'\}$ et $\{e\} \times G'$ sont distingués et l'on peut légitimement considérer que l'étude de la structure de groupe de $G \times G'$ se ramène à l'étude des briques plus élémentaires que sont G et G'.

Dans ce chapitre, nous étudions une situation un peu plus générale, appelée un produit semi-direct.

8.1 Point de vue interne

Soient G un groupe et N et H deux sous-groupes vérifiant
— $N \cup H$ engendre G et $H \cap N = \{e\}$.
— N est distingué
La première hypothèse ressemble à la situation où un espace vectoriel est la somme directe de deux de ses sous-espaces (et alors l'un de ces sous-espace est isomorphe au quotient du gros espace par l'autre sous-espace). La seconde est

spécifique aux groupes, pour pouvoir passer au quotient par N.

8.1 Définition. G est un *produit semi-direct* de N et H, et l'on note $G = N \rtimes H$.

8.2 Lemme. *L'application*

$$N \times H \to G, \quad (n, h) \mapsto nh$$

est une bijection.

Démonstration. Surjectivité : Le groupe engendré par N et H est l'ensemble des éléments de G de la forme $x = n_1 h_1 ... n_k h_k$, avec $n_i \in N$ et $h_i \in H$. Par hypothèse, tout élément de G est de cette forme, et il s'agit de montrer qu'il est dans l'image de l'application $N \times H \to G$ de l'énoncé. Comme N est distingué, pour tout $h \in H$, $hN = Nh$, i.e. pour tout $n \in N$, il existe n' tel que $hn = n'h$. Donc, par récurrence, on voit qu'il existe $n'_2, ..., n'_k$ tels que $x = n_1 n'_2 ... n'_k h_1 ... h_k$.

Injectivité : Supposons que $nh = n'h'$ avec $n, n' \in N$ et $h, h' \in H$. On a $n'^{-1}n = h'h^{-1} \in H \cap N = \{e\}$, donc $n = n' = h = h' = e$. □

Attention, cette bijection n'est généralement pas un isomorphisme.

8.3 Proposition. *Le loi de groupe sur $N \times H$ induite de celle de G par l'identification du lemme est*

$$(n, h)(n', h') = (nhn'h^{-1}, hh'). \tag{5}$$

Démonstration. Notons p la bijection précédente $N \times H \to G$. La loi induite sur $N \times H$ par cette identification vérifie

$$\begin{aligned} p((n, h)(n', h')) &= p(n, h)p(n', h') \\ &= nhn'h' \\ &= (nhn'h^{-1})(hh'), \end{aligned}$$

d'où l'affirmation. □

8.a Exercice. Montrer que le groupe dihédral D_n est un produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

8.2 Point de vue externe

Dans la loi de groupe décrite dans (5), le produit de deux éléments de N est "tordu" par l'action adjointe de H. Nous allons généraliser ceci.

Soient N et H deux groupes. Supposons qu'il existe une action

$$\rho : H \to \mathrm{Aut}(N)$$

de H sur N, à valeurs dans les automorphismes de groupe. Définissons sur $N \times H$ la loi

$$(n, h)(n', h') = (n(h \cdot n'), hh').$$

8.4 Lemme. *Cette loi fait de $N \times H$ un groupe isomorphe à*

$$(N \times \{e_H\}) \rtimes (\{e_N\} \times H)$$

(au sens de la définition 8.1).

8.b Exercice. Démontrer le lemme.

8.3 Extensions

8.5 Définition. Une *suite exacte* est une suite de groupes G_i et de morphismes $\phi_i : G_i \to G_{i+1}$,

$$\cdots G_{i-1} \xrightarrow{\phi_{i-1}} G_i \xrightarrow{\phi_i} G_{i+1} \xrightarrow{\phi_{i+1}} G_{i+2} \cdots$$

telle que, pour tout i, $\operatorname{im} \phi_i = \ker \phi_{i+1}$.

Une *suite exacte courte* est une suite exacte de la forme

$$\{e\} \to N \xrightarrow{\phi} G \xrightarrow{\psi} H \to \{e\}$$

(ϕ est injectif, ψ est surjectif et $\operatorname{im} \phi = \ker \psi$). On dit que G est une *extension de H par N* ; il est équivalent de dire que H est isomorphe à G/N.

Le fait que ψ soit surjectif dit qu'il existe toujours un inverse à droite s de ψ ($\psi \circ s = \mathrm{id}$). Mais, parmi les inverses à droite, généralement aucun n'est un morphisme de groupe. L'extension est *scindée* si elle en possède un, et un tel morphisme $s : H \to G$ qui soit un inverse à droite de ψ s'appelle une *section* de ψ, et $s(H)$ un *complément* de $\phi(N)$ dans G.

8.6 Proposition. *Si l'extension est scindée et si s est une section,*

$$G = \phi(N) \rtimes s(H).$$

Démonstration. $\phi(N)$ et $s(H)$ sont des sous-groupes de G parce que ϕ et s sont des morphismes. De plus, $\phi(N) = \ker \psi$ est distingué.

Par ailleurs, si $g \in G$, soient $h = s(\psi(g)) \in s(H)$ et $n = gh^{-1}$; on a $\psi(n) = e$, donc $n \in \ker \psi = \phi(N)$. Donc $\phi(N)s(H) = G$. Enfin, si $g = s(h) \in \phi(N) \cap s(H)$, $\psi(g) = e = h$ donc $g = s(e) = e$. Donc $\phi(N) \cap s(H) = \{e\}$. □

Si $G = N \rtimes H$, on voit que H s'identifie au groupe quotient G/N. Plus généralement, si un groupe G possède un sous-groupe distingué N, le quotient $G' = G/N$ est une sorte de version simplifiée de G, obtenue en considérant G modulo N. Jusqu'à quel point un groupe G peut-il être simplifié ainsi, en considérant des quotients successifs $G' = G/N$, $G'' = G'/N'$, etc. ? Pour un groupe fini, une telle suite est forcément de longueur finie, inférieure à l'ordre de G. (Comme on l'a déjà vu, un groupe G sans aucun sous-groupe distingué autre que $\{e\}$ et G lui-même est

qualifié de *simple.*) [16] En répétant la procédure, on obtient ainsi (au moins dans le cas fini) une suite

$$G = N_0 \rhd N1 \rhd \cdots \rhd N_k \rhd N_{k+1}\{e\}$$

dans laquelle les quotients successifs N_i/N_{i+1} sont simples. Une telle suite s'appelle une *série de composition.* Bien sûr, un groupe donné peut avoir des séries de composition différentes. Donc le résultat suivant, ici admis (et dont la démonstration utilise très peu les propriétés des groupes, paradoxalement), est très important.

8.7 Théorème (Jordan-Hölder)**.** *Deux séries de composition d'un groupe G ont la même longueur et les quotients N_i/N_{i+1} sont isomorphes deux à deux (à l'ordre près).*

Dans quelle mesure peut-on reconstruire une extension G à partir de N et de $H = G/N$? Regardons le cas particulier où N est abélien. H agit sur N, qui devient un H-module (mais avec l'opération de groupe de N écrite multiplicativement, plutôt qu'additivement). Soit s une section de la projection canonique $\psi : G \to H = G/N$; autrement dit, pour tout $h \in H$, $s(h)$ est un représentant de la classe h modulo N. Comme on l'a déjà remarqué, s n'est généralement pas un morphisme : $s(h)s(h') \neq s(hh')$, mais ces deux éléments appartiennent à la même classe modulo N. Donc il existe des éléments $f(h, h') \in N$ tels que

$$s(h)s(h') = f(h, h')s(hh').$$

Les éléments $f(h, h')$ ne peuvent pas être choisis arbitrairement, puisque l'associativité de la loi de G $((s(h)s(h'))s(h'') = s(h)(s(h')s(h'')))$ impose la condition suivante :

$$f(h, h'h'')hf(h', h'') = f(hh', h'')f(h, h').$$

De plus, notre construction dépend du choix de la section s. N'importe quel autre choix est de la forme $s'(h) = s(h)a(h)$ avec $a(h) \in N$, et la fonction f' associée à s' est reliée à la première par l'identité

$$f'(h, h') = f(h, h')a(h)ha(h')a(hh')^{-1}.$$

Ceci conduit à définir le *deuxième groupe de cohomologie* $\mathcal{H}^2(H, N)$ de H comme l'ensemble des fonctions $f : G \times G \to G$ satisfaisant la relation précédente, modulo le groupe des fonctions de la forme

$$f(h, h') = a(h)ha(h')a(hh')^{-1}$$

(souvent la notation additive est plutôt adoptée). Alors une extension de H par N est uniquement déterminée par la structure de H-module de N et par un élément de $\mathcal{H}^2(H, N)$ [Sha05, § 21].

16. Dans le cas des groupes de matrices (ou de Lie), il est naturel de ne considérer, parmi les sous-groupes, que ceux qui sont des sous-groupes de matrices (ou de Lie) distingués *connexes.* Ainsi, un groupe de matrice qui est simple au regard de cette définition peut ne pas être simple en tant que groupe abstrait. (Par exemple, $\mathbb{R}$ est simple comme groupe de Lie, bien qu'il contient le sous-groupe discret $\mathbb{Z}$.) Par un argument analogue à celui des groupes finis (où la notion de dimension remplace celle de l'ordre), les groupes de matrice aussi sont de "longueur finie".

8.c Exercice.
Montrer que, si le second groupe de cohomologie de H est trivial, l'unique extension de H par N est le produit semi-direct $N \rtimes H$.

8.d Exercice ★ (Extensions de groupes)**.**
Soient A, E, G trois groupes tels que A soit abélien, et i et p deux morphismes de groupes

$$A \xrightarrow{i} E \xrightarrow{p} G$$

une suite exacte courte de groupes, telle que A soit abélien ; E s'appelle une *extension* de G par A. Soit de plus ρ, $\rho(g)(a) = g \cdot a$, une action de G sur le groupe A.

1. Donner un exemple d'extension qui ne soit pas un produit direct $A \times G$.

Revenons au cas général. Pour tout $g \in G$, on choisit un antécédent $\hat{g} \in E$ de g par p.

3. Montrer que, pour tout $x \in E$, il existe $a \in A$ et $g \in G$ uniques tels que $x = a\hat{g}$.
4. Le sous-groupe $i(A)$ est-il distingué dans E ? En déduire, lorsque l'application $g \mapsto \hat{g}$ est un morphisme de groupes, la loi de groupe induite sur $A \times G$.

Dans la suite, on cherche à décrire toutes les extensions E possibles de G par A (à isomorphisme près), compatibles avec l'action donnée de G sur A (c'est-à-dire dont la multiplication à gauche prolonge cette action). On identifie dorénavant A à son image par i.

5. Montrer que l'action de G sur A induit une action de G sur l'ensemble $\mathrm{App}(G^n, A)$ des applications $x : G^n \to A$, $(g_1, ..., g_n) \mapsto x_{g_1,...,g_n}$ $(n \in \mathbb{N})$, par la formule
$$(g \cdot x)_{g_1,...,g_n} = g \cdot x_{g^{-1}g_1,...,g^{-1}g_n)}.$$

Soient $\partial^i : \mathrm{App}(G^{i-1}, A) \to \mathrm{App}(G^i, A)$, $i = 2, 3$, les deux applications définies par

$$\begin{cases} (\partial^2 x)_{g,h} = (g \cdot x_h)\, x_{gh}^{-1}\, x_g \\ (\partial^3 x)_{g,h,k} = (g \cdot x_{h,k})\, x_{gh,k}{}^{-1}\, x_{g,hk}\, x_{g,h}{}^{-1}. \end{cases}$$

6. Montrer que $\operatorname{im} \partial^2 \subset \ker \partial^3$.

On note $\mathcal{H}^2 = \mathcal{H}^2(G, A)$ et l'on appelle 2e *groupe de cohomologie* le groupe quotient $\mathcal{H}^2 = \ker \partial^3 / \operatorname{im} \partial^2$.

7. Montrer que, pour tous $g, h \in G$, il existe un unique $x_{g,h} \in A$ tel que $\hat{g}\hat{h} = x_{g,h}\widehat{gh}$, et que l'application x ainsi définie vérifie $\partial^3 x = e$.
8. Montrer que la classe de x dans $\mathcal{H}^2$ ne dépend pas du choix qu'on a fait de de l'inverse à droite de p, $g \mapsto \hat{g}$.
9. Quelle est la relation entre $\mathcal{H}^2$ et les extensions cherchées ?

9 Présentation par générateurs et relations

La "présentation" d'un groupe par générateurs et relations est une définition souvent très concise d'un groupe.

Soient S un ensemble (appelé l'*alphabet*) et

$$S' = S \cup \{a^{-1},\ a \in S\},$$

où a^{-1} désigne un élément de S' associé à a mais distinct de a, sans référence à une quelconque loi de groupe à ce stade. Si S est fini, $|S'| = 2|S|$.

Notons L_S^o l'ensemble des *mots* sur S', c'est-à-dire des suites finies de symboles tirés de S'. Par exemple, si $a, b, c \in S$,

$$aaba^{-1}abcc^{-1}$$

est un mot $\in L_S^o$ de longueur 8. Le mot vide sera désigné par le symbole $\varnothing$.

9.a Exercice. Montrer que la loi de concaténation des mots définit sur L_S^o une loi associative possédant le mot vide comme élément neutre [17], mais qu'elle n'est pas une loi de groupe.

Le *groupe libre* sur S est l'ensemble L_S des *mots réduits* sur S', c'est-à-dire des mots qui ne contiennent aucune occurence de séquences xx^{-1} ou $x^{-1}x$ avec $x \in S$. L_S possède une structure de groupe, dont le produit est la concaténation (à valeurs dans L_S^o) suivie de la réductions $L_S^o \to L_S$, consistant à supprimer tous les xx^{-1} ou $x^{-1}x$. Par exemple,

$$(abc, c^{-1}d) \longmapsto abcc^{-1}d \longmapsto abc \cdot c^{-1}d = abd.$$

Pour que le résultat de cette opération soit bien un mot réduit, il faut procéder à toutes les réductions successives nécessaires, comme sur cet exemple :

$$(ab, b^{-1}a^{-1}) \longmapsto abb^{-1}a^{-1} \longmapsto \varnothing$$

(la seule réduction de bb^{-1} ne suffit donc pas).

Le *rang* de L_S est le cardinal de l'alphabet S.

9.b Exercice. Montrer que la concaténation-réduction (à valeurs dans L_S) ne définit pas une loi de groupe sur L_S^o.

9.1 Théorème (Propriété universelle du groupe libre)**.** *Pour toute application $f : S \to G$ à valeurs dans un groupe, il existe un unique morphisme $F : L_S \to G$ qui prolonge f.*

9.c Exercice. Démontrer le théorème.

Soit maintenant $R \subset L_S$ une partie dont les éléments seront appelés les *relations*. L'idée est de construire un quotient de L_S dans lequel $\bar{r} = e$ pour tout $r \in R$.

17. On dit pour cela que L_S^o est un monoïde.

9.2 Théorème (Propriété universelle de la présentation)**.** *Soient S un alphabet et R une partie du groupe libre L_S. Il existe un groupe G et une application $\sigma : S \to G$ vérifiant la propriété suivante :*

> *Pour tout groupe H et toute application $f : S \to H$ telle que $R \subset \ker f$ (où f désigne l'unique prolongement de f en un morphisme de groupes $L_s \to H$ [18]), il existe un unique morphisme $\varphi : G \to H$ tel que le diagramme suivant commute :*

$$\begin{array}{ccc} L_S & \xrightarrow{f} & H\ . \\ {\scriptstyle\sigma}\downarrow & \nearrow_{!\varphi} & \\ G & & \end{array}$$

De plus, G est unique à isomorphisme près.

La construction suivante va résoudre le problème universel du théorème.

Soit N le *sous-groupe distingué engendré par R* (on dit aussi *la clôture distinguée de R*), c'est-à-dire le plus petit sous-groupe distingué de L_S contenant R. (N existe bien, parce que l'intersection de sous-groupes distingués est un sous-groupe distingué.)

9.d Exercice. Montrer que, si R est une partie d'un groupe L et N est le plus petit sous-groupe distingué de L contenant R,

$$N = \langle R^L \rangle, \quad R^L = \{grg^{-1},\ g \in L,\ r \in R\}.$$

9.3 Définition. Le *groupe défini par les générateurs de S et les relations de R* est le groupe quotient

$$\langle S \,|\, R \rangle = L_S/N.$$

Remarquons que, pour toute relation $r \in R$, $\bar{r} = e$ dans le quotient L_S/N. Une relation r est donc parfois écrite "$r = e$", afin d'insister sur la règle de calcul induite dans le quotient.

Il pourrait sembler plus systématique de définir les relations de $\langle S|R \rangle$ comme R^H (qui engendre N), plutôt que R. Mais cela reviendrait à allonger inutilement la liste des relations.

Démonstration du théorème. D'après la propriété universelle de L_S, il existe en effet un unique prolongement de f en un morphisme de groupes $L_S \to H$, que l'on continue maintenant de noter f :

$$\begin{array}{ccc} S & \xrightarrow{f} & H. \\ \downarrow & \nearrow_{f} & \\ L_S & & \end{array}$$

18. Voir le théorème 9.1.

Existence de $\sigma : L_S \to G$. Soient $G\langle S \,|\, R\rangle$ et $\sigma : \langle S \,|\, R\rangle \to G$ la composition de l'injection $S \hookrightarrow L_S$ et de la surjection canonique $L_S \twoheadrightarrow \langle S \,|\, R\rangle$. Comme $\ker f$ est un sous-groupe distingué de L_S, $R \subset \ker f$ si et seulement si $\langle R^{L_S}\rangle \subset \ker f$, c'est-à-dire si seulement si f passe au quotient par $\langle R^{L_S}\rangle$, si et seulement si (d'après la propriété universelle du quotient d'un groupe, cf. le théorème 7.4) f induit un morphisme $\varphi : \langle S \,|\, R\rangle \to G$.

Unicité de σ. La démonstration est la même, *mutatis mutandis*, que pour le théorème 5.4. □

Dans la démonstration précédente, on peut remarquer que, si f est surjective, [19] il en va de même de φ.

Les groupes déjà rencontrés admettent souvent des présentations par générateurs et relations qui sont très simples :

— Tout groupe G vérifie
$$G \simeq \langle G \,|\, xy(xy)^{-1}\rangle;$$
(on voit dès ici qu'un groupe admet généralement beaucoup de présentations différentes ; par exemple on peut augmenter ou réduire le nombre de générateurs).
— $L_S \simeq \langle S \,|\, \varnothing\rangle$
— $\mathbb{Z}/n\mathbb{Z} \simeq \langle a \,|\, a^n\rangle$
— $D_n \simeq \langle r, s \,|\, r^n, s^2, rs = sr^{n-1}\rangle = \langle r, s \,|\, r^n, s^2, srsr\rangle$ (une égalité $x = y$ dans les relations est à prendre dans le sens où l'on ajoute l'élément xy^{-1} aux relations)
— Le groupe dihédral d'ordre infini $D_\infty = \langle r, s \,|\, s^2, srsr\rangle$.

C'est un bon exercice de construire ces isomorphismes.

9.e Exercice (Groupe quaternionique)**.** Le *groupe quaternionnique* est
$$Q_8 = \langle x, y \,|\, x^4 = e,\ x^2 = y^2,\ yxy^{-1} = x^{-1}\rangle.$$
On note souvent $1 = e$, $i = x$, $j = y$, $k = xy$ et $-1 = x^2$. [20] Montrer que

1. le groupe quaternionique est d'ordre 8
2. i, j et k sont d'ordre 4
3. Q_8 possède cinq classes de conjugaison.

9.f Exercice.
Soient G un groupe de type fini (c'est-à-dire admettant une partie génératrice finie) et $H \leqslant G$. H est-il automatiquement de type fini ?

La présentation d'un groupe par générateurs et relations pose cependant plusieurs problèmes. Terminons ce chapitre par quelques théorèmes admis qui montrent que l'on tombe rapidement sur des questions difficiles.

Déterminer l'ordre d'un groupe, ou même déterminer si l'ordre de ce groupe vaut 1, s'avère parfois difficile.

19. Autrement dit, S est une partie génératrice de G et les mots $r \in R \subset L_S$ sont triviaux dans G.

20. Ces notations deviennent naturelles quand on considère Q_8 comme une partie finie du corps $\mathbb{H}$ des quaternions (voir plus loin).

9.4 Théorème (admis)**.** *La question de déterminer si l'ordre d'un groupe présenté par générateurs et relations vaut* 1*, est indécidable (dans un sens précis de la Logique, où il n'existe aucun algorithme permettant de conclure).*

Ce théorème est lié à la question suivante. Un élément d'un groupe n'a pas une écriture unique ; on l'a vu à de nombreuses reprises dans D_3, où par exemple $rs = sr^2$. Cette non-unicité est délicate :

9.5 Théorème (Novikov-Boone-Britton, admis)**.** *La question de déterminer si deux mots donnés sur S sont égaux dans $\langle S \,|\, R\rangle$ est indécidable.*

Les problèmes de classification (détermination des classes d'isomorphismes) sont eux aussi compliqués, comme le montre déjà le cas de deux générateurs :

9.6 Théorème (admis)**.** *Les classes d'isomorphisme de groupes à deux générateurs forment un ensemble infini non dénombrable.*

10 Groupes résolubles

Certaines équations (par exemple polynomiales) peuvent être "résolues" si un certain groupe qui leur est attaché vérifie la propriété d'être *résoluble* ; celle-ci généralise la commutativité.

10.1 Définition. Un groupe G est *résoluble* si il existe une suite

$$G_n = \{e\} \lhd \cdots \lhd G_0 = G$$

dont les quotients successifs G_i/G_{i+1} soient commutatifs.

Si G est commutatif, il est résoluble, avec $G_1 = \{e\}$. Si G est résoluble non commutatif, G possède un sous-groupe distingué non trivial, à savoir G_1. Si G/G_1 et G_1 sont commutatifs, G est résoluble, avec $G_2 = \{e\}$. Sinon...

Nous allons caractériser les groupes résolubles en termes d'une suite de sous-groupes particulière.

10.2 Définition. Le *sous-groupe dérivé* ou *commutant* de G est le sous-groupe

$$DG = \langle [a,b],\, a,b \in G\rangle, \quad [a,b] = aba^{-1}b^{-1}.$$

DG est donc l'ensemble des produits finis d'éléments de la forme

$$[a,b] \quad \text{ou} \quad [a,b]^{-1}.$$

10.a Exercice. Montrer que DG est un sous-groupe distingué de G tel que G/DG soit commutatif, et que, parmi les tels sous-groupes, DG est le plus petit ; G/DG est l'*abélianisé* de G.

Si il existe $n \in \mathbb{N}_*$ tel que $D^nG = \{e\}$, G est résoluble, puisque

$$\{e\} = D^nG \lhd D^{n-1}G \lhd \cdots \lhd DG \lhd D^0G = G.$$

Il se trouve que la réciproque est vraie ; autrement dit, pour voir si un groupe est résoluble, il suffit de regarder la *suite dérivée* (D^iG).

10.3 Proposition. *G est résoluble $\Leftrightarrow$ il existe $n \geqslant 1$ tel que $D^nG = \{e\}$.*

Démonstration. Supposons que G soit résoluble. Soient les G_i comme dans la définition. Comme G_0/G_1 est abélien, G_1 contient DG. Puis, comme G_1/G_2 est abélien, G_2 contient $DG_1 \supset DG_0 = DG$. Par récurrence, on voit que $D^iG \subset G_i$ donc $D^nG = \{e\}$. □

10.4 Exemple. Si G est commutatif, $DG = \{e\}$ et G est résoluble. Si DG est commutatif, $D^2G = \{e\}$ donc G est résoluble, etc.

10.5 Remarque. Soit $\varphi : G \to H$ un morphisme de groupes. La restriction de φ à DG est à valeurs dans DH, puisque

$$\varphi([a,b]) = [\varphi(a), \varphi(b)].$$

On note

$$D\varphi : DG \to DH$$

le morphisme induit par φ. De plus,

$$D(\varphi \circ \psi) = D\varphi \circ D\psi.$$

On dit que D est un *foncteur* de la catégorie des groupes dans elle-même.

10.b Exercice. Montrer que tout sous-groupe d'un groupe résoluble est résoluble.

10.6 Proposition. *Soit*

$$N \hookrightarrow G \twoheadrightarrow H$$

une suite exacte.[21] *Alors G est résoluble et si seulement si N et H sont résolubles.*

Démonstration. Remarquons que, par restriction, on a des morphismes

$$D^ni : D^nN \hookrightarrow D^nG \quad \text{et} \quad D^ns : D^nG \twoheadrightarrow D^nH.$$

Si $D^nG = \{e\}$, $D^nN = D^nH = \{e\}$.

Réciproquement, si $D^nN = D^nH = \{e\}$, $\ker D^ns = \operatorname{im} D^ni = \{e\}$, donc D^ns est un isomorphisme, donc D^nG est trivial. □

10.c Exercice. Parmi les groupes suivants, lesquels sont résolubles : le groupe cyclique $\mathbb{Z}_n$, le groupe dihédral D_3, le groupe dihédral D_4, le groupe des quaternions (exemple 9.e) ; le groupe T de symétrie du tétraèdre régulier. *Indication :* Ces groupes sont tous résolubles. Mais pourquoi ? Pour T, on pourra utiliser l'exercice 4.k.

21. Les flèches modifiées signifient que le morphisme de N dans G est injectif et que celui de G dans H est surjectif. Le fait que la suite soit exacte signifie que l'image du premier morphisme est égale au noyau du second.

En revanche, le groupe de symétrie O du dodécaèdre régulier (ou, de façon équivalente comme on le verra, le groupe alterné A_5 de degré 5), n'est pas résoluble.

10.d Exercice (Groupe O^+)**.**
On note ici O^+ le groupe des rotations du dodécaèdre (figure 10).

1. Quel est l'ordre du groupe de O^+ ? *Indication.* Les rotations du dodécaèdre se rangent en quatre classes : (1) l'identité, (2) les rotations autour d'un axe passant par le centre de faces opposées, (3) les rotations autour d'un axe passant par des sommets opposés et (4) les rotations autour d'un axe passant par les centres d'arêtes opposées. On pourra déterminer le nombre d'éléments de chaque classe (sans compter l'identité dans les classes (2), (3) et (4)).
2. Soit N un sous-groupe distingué de O^+. Montrer que si N contient une rotations r, N contient toute la classe de r.
3. Montrer que O^+ est simple, et conclure que O^+ et O ne sont pas résolubles.

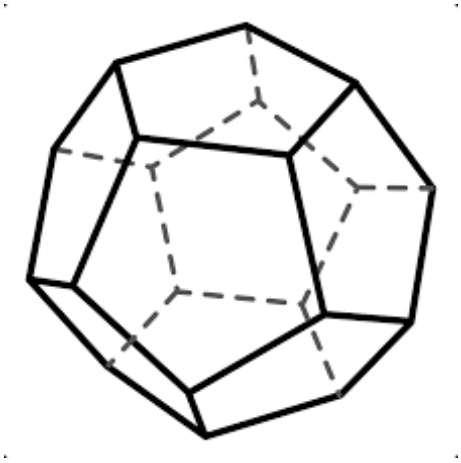


FIGURE 7 – Dodécaèdre régulier

11 Le groupe symétrique

Rappelons que le *groupe symétrique* de degré n est le groupe $\mathfrak{S}_n = \mathrm{Trans}(\{1, ..., n\})$ des bijections de $\{1, ..., n\}$ dans lui-même, muni de la loi de composition. Il est d'ordre $n!$. Pour simplifier, on note $\tau\sigma$ au lieu de $\tau \circ \sigma$, et σ^k au lieu de $\sigma^{\circ k}$.

Par exemple, $\mathfrak{S}_2$ contient deux éléments : l'identité et la permutation non triviale, qui échange 1 et 2. La structure de $\mathfrak{S}_n$ se complique rapidement quand n augmente.

11.a Exercice. Montrer que, si $n \geqslant 3$, $\mathfrak{S}_n$ n'est pas commutatif.

L'orbite de $x \in \{1, ..., n\}$ sous "l'action" de σ [22] est

$$\{\sigma^k(x),\ k \in \mathbb{Z}\}.$$

Les orbites forment une partition de $\{1, ..., n\}$.

Une permutation peut fixer certains éléments ($\sigma(i) = i$) et pas d'autres ($\sigma(j) \neq j$). Le *support* de σ est l'ensemble des x qui ne sont pas fixés par σ :

$$\operatorname{supp} \sigma = \{i,\ \sigma(i) \neq i\} \in \{0, ..., n\}.$$

Une *permutation circulaire*, ou *cycle*, est une permutation dont le support est soit vide soit une unique orbite ; autrement dit, si on enlève les points fixes, il reste zéro ou une orbite.

11.b Exercice. Montrer qu'une permutation quelconque se décompose en produit de permutations circulaires de supports disjoints.

11.1 Notation. Soient $i_1, ..., i_k$ des éléments distincts deux à deux de $\{1, ..., n\}$. On note $(i_1\, i_2 \ldots i_k)$ le cycle qui envoie i_1 sur i_2, i_2 sur i_3, ..., i_{k-1} sur i_k, et i_k sur i_1, et qui fixe tous les $j \notin \{i_1, ..., i_k\}$.

11.2 Définition. Le *type* d'une permutation est la suite des longueurs de ses orbites, ordonnée de façon croissante.

Par exemple,

$$\text{type}\,(123)(4567)(8)(9) = (1, 1, 3, 4).$$

11.c Exercice. Soient $\sigma, \tau \in \mathfrak{S}_n$. On note M_σ et M_τ leurs matrices de permutation respectives ; on rappelle que par exemple M_σ est la matrice

$$M_\sigma = (\delta_{i,\sigma(j)})_{i,j},$$

où δ_{ij} est le symbole de Kronecker. Montrer que les propriétés suivantes sont équivalentes :

1. σ et τ ont même type
2. σ et τ sont conjuguées : il existe $\alpha \in \mathfrak{S}_n$ telle que $\tau = \alpha\sigma\alpha^{-1}$
3. M_σ et M_τ sont conjuguées : il existe $G \in GL_n(\mathbb{R})$ telle que $M_\tau = PM_\sigma P^{-1}$.

Une *transposition* est un cycle dont le support est de la forme $(i\ j)$, i.e. qui ne fait qu'échanger deux éléments. Une *bitransposition* est une permutation dont le cycle est de la forme $(i\ j)(k\ l)$ où les deux transpositions $(i\ j)$ et $(k\ l)$ sont à supports disjoints (i.e. i, j, k, l sont 3 éléments distincts deux à deux).

Notons $\sigma_i = (i\ i+1)$ (si $i = n$, on identifie $i+1$ à 1). Remarquons que

$$\begin{cases} \sigma_i^2 = e \\ \sigma_i\sigma_j = \sigma_j\sigma_i \text{ si } |i-j| > 1 \\ \sigma_i\sigma_{i+1} = (i\ i+1)(i+1\ i+2) = (i\ i+1\ i+2). \end{cases} \tag{6}$$

22. Une permutation $\sigma \in \mathfrak{S}_n$ détermine une action de $\mathbb{Z}$ sur $X = \{1, ..., n\}$, par la formule $k \cdot x \mapsto \sigma^k(x)$.

11.3 Proposition (admise)**.** $\mathfrak{S}_n$ *est le groupe engendré par* σ_1, ..., σ_n, *modulo les relations* (6)*.*

11.d Exercice. Montrer que σ_1, ..., σ_{n-1} engendrent $\mathfrak{S}_n$.

(Pour montrer la proposition, étant donné que les relations voulues sont vérifiées dans $\mathfrak{S}_n$, il s'agit de montrer que toutes les relations dans $\mathfrak{S}_n$ s'en déduisent.)

11.4 Définition. Une *inversion* d'une permutation σ est une couple $(i, j) \in \{1, ..., n\}^2$ telle que $i < j$ mais $\sigma(i) > \sigma(j)$.

Le nombre d'inversions de σ caractérise le désordre de σ par rapport à l'identité.

11.e Exercice. Quel est le nombre d'inversions de la permutation (32541) ?

11.f Exercice. Montrer que la parité du nombre d'inversion change quand on compose une permutation par une transposition.

Comme les σ_i engendrent $\mathfrak{S}_n$, toute permutation s'exprime comme le produit d'un nombre fini de σ_i, et, a fortiori, comme le produit d'un nombre fini de transpositions. Bien sûr, cette écriture n'est pas unique, puisque l'on peut toujours composer un tel produit par id = (12)(12), par exemple. En particulier, le nombre de transpositions nécessaires n'est pas unique. En revanche, l'exercice montre que la parité du nombre de transpositions, dans la décomposition d'une permutation donnée, est bien définie : c'est la parité du nombre d'inversions de la permutation.

11.5 Définition. Une permutation σ est *paire* ou *impaire* en fonction de la parité de son nombre d'inversions. La *signature* de σ, notée $\epsilon(\sigma)$, vaut 1 si σ est paire et -1 si σ est impaire.

Par exemple, une transposition est impaire.

11.g Exercice. Quelle est la signature de (1 2 5 3 4) ?

11.h Exercice. Montrer que la signature est un morphisme de groupes $(\mathfrak{S}_n, \circ) \to (\{\pm 1\}, \times)$.

11.i Exercice. Quelle est la signature d'un cycle de longueur 3 ? 4 ? k ?

11.6 Définition. Le *groupe alterné* de degré n est le sous-groupe $\mathfrak{A}_n$ de $\mathfrak{S}_n$ des permutations paires.

11.j Exercice. Montrer que $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$ et que, si $n \geqslant 4$, $\mathfrak{A}_n$ n'est pas commutatif. Quel est l'ordre de A_n ?

11.7 Théorème. *Pour* $n \neq 4$*, le groupe* $\mathfrak{S}_n$ *n'a pas de sous-groupe distingué autre que* $\{e\}$*,* $\mathfrak{A}_n$ *et* $\mathfrak{S}_n$*. Le groupe* $\mathfrak{S}_4$ *possède le sous-groupe distingué supplémentaire des permutations de type* $(2, 2)$ *(appelées* bitranspositions*).*

Schéma de démonstration. Le groupe $\mathfrak{A}_5$ est d'ordre 60. Ses éléments se répartissent ainsi : l'identité, 15 bitranspositions (d'ordre 2), 20 3-cycles (d'ordre 3) et 24 5-cycles (d'ordre 5).

On vérifie que les bitranspositions sont conjuguées deux à deux, et de même pour les 3-cycles.

De plus, les 3-cycles engendrent $\mathfrak{A}_5$ (il suffit de vérifier que le produit de deux transpositions se décompose en un produit de 3-cycles).

Soit H un sous-groupe distingué de $\mathfrak{A}_5$, différent de $\{\mathrm{id}\}$. Si H contient un élément d'ordre 2 (resp. 3, resp. 5), il les contient tous ; c'est évident pour les éléments d'ordre 2 ou 3 (comme H est distingué, il est une union de classes de conjugaisons), tandis qu'il y a un travail supplémentaire à faire pour les éléments d'ordre 5. Mais H ne peut contenir un seul des trois types d'éléments précédents, en plus du neutre, parce que ni 25, ni 21 ni 16 ne divisent 60. Donc H contient 2 des trois types d'éléments non triviaux de $\mathfrak{A}_5$, donc l'ordre de H est minoré par $1 + 15 + 20 = 36$. Comme l'ordre de H divise 60, il vaut 60. Donc $\mathfrak{A}_5$ est simple. (Cf. l'exercice 10.d.)

Pour $n \geqslant 5$, on se ramène à $\mathfrak{A}_5$, en choisissant un élément σ d'un sous-groupe distingué H de $\mathfrak{A}_5$ et en construisant à partir de σ un élément ayant au moins $n - 5$ points fixes, donc agissant sur $\{1, ..., 5\}$.

Quant au groupe $\mathfrak{A}_4$, on vérifie que ses bitranspositions forment, avec l'identité, un sous-groupe distingué $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. □

Remarque : En degré $\geqslant 5$, l'ensemble des bitranspositions n'est pas stable par composition, puisque

$$(23)(45)(12)(34) = (13542).$$

Le sous-groupe distingué K de $\mathfrak{A}_4$ formé par les bitranspositions s'appelle le *groupe de Klein*. Il est d'ordre 12 et est isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_2$ (exercice),

11.k Exercice. Montrer que si $n \leqslant 4$, $\mathfrak{S}_n$ est résoluble.

11.l Exercice. Montrer que, si $n \geqslant 5$, $\mathfrak{S}_n$ n'est pas résoluble. *Indication :* Montrer qu'un 3-cycle est un commutateur.

12 Notion de corps

12.1 Définition. Un *corps* K est un ensemble muni de deux opérations (lois de compostion internes), appelées *addition* et *multiplication* et notées $(a, b) \mapsto a + b$ et $(a, b) \mapsto ab$, vérifiant les axiomes suivants :

1. $(K, +)$ est un groupe commutatif (dont l'élément neutre est noté 0)
2. $(K^\times = K\backslash\{0\}, \times)$ est un groupe commutatif (dont l'élément neutre est noté 1 et dont on néglige de noter le signe $\times$), le *groupe des inversibles* de K [23]
3. la multiplication est distributive sur l'addition :

$$a(b + c) = ab + ac.$$

12.2 Définition. Un *anneau* A est un ensemble muni de deux opérations, vérifiant les mêmes axiomes que pour un corps, si ce n'est que le deuxième axiome est affaibli de la façon suivante :

23. Dans la définition d'un *corps non commutatif*, cet axiome est remplacé par le fait que $(K^\times, \times)$ est un groupe non commutatif.

2'. $\times$ est une loi associative possédant un élément neutre (on dit que $(K^\times, \times)$ est un *monoïde*). [24]

Un sous-anneau de A est une partie $B \subset A$ stable par $+$, $-$ et $\times$, et contenant le neutre 1 de la multiplication.

Remarquons une propriété importante vis-à-vis du produit, pour le neutre de l'addition, dans un anneau : pour tout $a \in A$, $0a = (0+0)a$ donc, en simplifiant on voit que $0a = 0$, i.e. 0 est *absorbant* pour la multiplication.

12.a Exercice. Les ensembles suivants :

$$\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{C}[X],\ M_n(\mathbb{C}),$$

sont-il des corps ? Des anneaux ?

12.3 Exemple (Anneau des polynômes sur une courbe). Si $F(x,y)$ est un polynôme réel à deux indéterminées, et si C est la courbe de $\mathbb{R}^2$ d'équation $F(x,y) = 0$, un *polynôme sur* C est la restriction d'une fonction polynomiale $f \in \mathbb{R}[x,y]$ à C. L'ensemble $\mathbb{R}[C]$ de ces polynômes est un anneau. [25]

12.4 Exemple. Soit K un corps. Une expression algébrique obtenue à partir d'une inconnue x et d'éléments arbitraires de K par additions, soustractions, multiplications et divisions est de la forme

$$\frac{a_0 + a_1 x + \cdots + a_n x^n}{b_0 + b_1 x + \cdots + b_m x^m},$$

où $a_i, b_i \in K$ et les b_i ne sont pas tous nuls. Une expression de cette forme s'appelle une *fraction rationnelle* en x. On peut la considérer comme une fonction sur K à valeurs dans K, ou sur n'importe quel corps L contenant K, tant que le dénominateur ne s'annule pas. L'ensemble des telles expressions est le *corps des fractions rationnelles* et se note $K(x)$. De façon similaire on définit le corps $K(x,y)$ des fractions rationnelles à deux variables, etc.

12.b Exercice. Un nombre complexe z est *constructible* (à la règle et au compas) s'il peut être construit, en partant de 0 et de 1, par intersections successives : de droites passant par deux points déjà construits, et de cercles dont le centre et le rayon ont déjà été construits. On note $\mathcal{C}$ l'ensemble des nombres constructibles.

1. Montrer que $\mathbb{Z} \subset \mathcal{C}$.

2. Montrer que $\sqrt{2} \in \mathcal{C}$; on pourra utiliser le théorème de Pythagore.

3. Montrer que $\mathcal{C}$ est stable par produit et inversion ; on pourra utiliser le théorème de Thalès.

4. En déduire que $\mathcal{C}$ est un corps contenant $\mathbb{Q}$.

12.5 Définition. Une application $f : A \to B$ entre deux anneaux est un *morphisme d'anneaux* si

$$f(x+y) = f(x) + f(y), \quad f(xy) = f(x)f(y), \quad \text{et} \quad f(1_A) = 1_B.$$

24. De rares auteurs n'imposent pas l'existence d'un élément neutre à $(A, \times)$, et utilisent le terme d'*anneau commutatif* pour désigner ce que nous appelons ici un anneau.

25. Une idée générale en théorie des anneaux est qu'un anneau commutatif s'interprète souvent comme l'anneau des fonctions (polynomiales, analytiques, continues, etc.) sur un ensemble.

C'est un *isomorphisme* si c'est de plus une bijection (son inverse est automatiquement un morphisme). Un *morphisme de corps* est un morphisme d'anneaux entre deux corps.

12.c Exercice. Soient K un corps et $a \in K$. Montrer que l'application $\varphi_a : K[X] \to K$, $P(X) \mapsto P(a)$ est un morphisme d'anneaux ; on l'appelle le *morphisme d'évaluation*.

12.d Exercice. Soit A est un anneau, intègre au sens où $ab = 0 \Rightarrow a = 0$ ou $b = 0$. Montrer qu'il existe un corps K contenant A, unique à isomorphisme près, tel qu tout élément de K est de la forme ab^{-1}, avec $a, b \in A$ et $b \neq 0$.

12.6 Exemple. Soit D un domaine (ouvert connexe) du plan complexe. Les fonctions méromorphes sur D forment un corps. Il en va de même des fonctions méromorphes sur une variété complexe connexe quelconque.

12.7 Exemple. Les *séries de Laurent* complexes $\sum_{n=-k}^{\infty} a_n z^n$ ($a_n \in \mathbb{C}$, $k \in \mathbb{N}$) convergentes (dans un anneau de la forme $0 < |z| < R$, $R > 0$), forment un corps.

Si K est un corps quelconque, on peut former les séries de Laurent sur K et les additionner et les multiplier en utilisant les mêmes règles formelles qu'avec les séries de Laurent complexe. Ces séries de Laurent forme le corps $K((x))$ des *séries de Laurent formelles sur K*.

12.e Exercice (Idéaux d'un anneau)**.**
Soit A un anneau.

1. Soient $f : A \to B$ est un morphisme d'anneau et $I = \ker f = f^{-1}(0)$. Montrer que I est un *idéal* de A, au sens où

1. I est un sous-groupe de $(A, +)$ (forcément distingué, puisque $(A, +)$ est commutatif)
2. I est *absorbant* : pour tout $a \in A$ et tout $i \in I$, $ia \in I$.

2. Soit I un idéal de A. Comme c'est un sous-groupe additif distingué de A, l'application de passage au quotient $p : A \to A/I$, $a \mapsto a + I$ est un morphisme de groupes additifs. Montrer que le produit sur A passe au quotient par I, ce qui muni A/I d'une structure d'anneau pour laquelle p est un morphisme d'anneaux.

3. Montrer que, pour tout $n \in \mathbb{N}$, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ hérite d'une structure d'anneau de $\mathbb{Z}$.

4. Montrer que A est un corps si et seulement si les idéaux de A sont exactement $\{0\}$ et A.

5. Montrer que $\mathbb{Z}_p$ est un corps si et seulement si p est un entier premier ; ce corps fini se note $\mathbb{F}_p$.

12.f Exercice. Montrer qu'un morphisme de corps est injectif.

12.8 Définition. Une *extension* d'un corps K est un morphisme de corps $K \hookrightarrow L$. On note alors L/K ; attention à ne pas prendre cette notation pour le quotient de L par K !

Quitte à identifier K à son image dans L, on peut toujours supposer que $K \subset L$. Ainsi, $\mathbb{C}$ est une extension de $\mathbb{R}$, qui lui-même est une extension de $\mathbb{Q}$ (ce qui se

note $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$).

Nous allons maintenant décrire trois notions distinctes de "dimension finie" pour les extensions de corps : les extensions de type fini, les extensions de degré fini et les extensions de degré de transcendance fini.

12.9 Définition. Un corps L est une *extension de type fini* d'un corps K si il existe un nombre fini d'éléments $\alpha_1, ..., \alpha_n \in L$ tels que tous les autres éléments de L puissent être obtenus commes fractions rationnelles en $\alpha_1, ..., \alpha_n$ à coefficients dans K, ce qu'on note

$$L = K(\alpha_1, ..., \alpha_n).$$

On dit alors que L est une extension de K engendrée par $\alpha_1, ..., \alpha_n$.

Par exemple :
- Le corps des fractions rationnelles $K(x_1, ..., x_n)$ est une extension de K de type fini.
- Le corps $\mathbb{C}$ des nombres complexes est une extension de type fini du corps $\mathbb{R}$ des nombres réels, puisque tout nombre complexe peut être représenté comme un polynôme de degé 1 en i ($z = a + ib$).
- Si C est une courbe algébrique irréductible (voir le complément 12.16), $K(C)$ est une extension de type fini de K puisque les fonctions dans $K(C)$ sont des fractions rationnelles des coordonnées x et y.

12.10 Définition. Le *degré* de l'extension L/K est la dimension (finie ou infinie) de l'espace vectoriel L sur K ; on le note $[L : K]$. L'extension L/K est *finie* si son degré est fini.

Par exemple, $[\mathbb{C} : \mathbb{R}] = 2$, et $[\mathbb{R} : \mathbb{Q}] = \infty$ (admis).

12.g Exercice. 1. Si L/K et K/k sont deux extensions, on a la formule multiplicative suivante :

$$[L : k] = [L : K][K : k].$$

2. Soit α un nombre constructible (voir l'exercice 12.b). Montrer qu'il existe des extensions successives $L_1/\mathbb{Q}$, L_2/L_1,... , L_n/L_{n-1} telles que $\alpha \in L_n$, $L_{i+1} = L_i(\beta_i)$ avec $\beta_i \in L_{i+1}$ et $[L_{i+1} : L_i] = 2$. En déduire que $[L_n : \mathbb{Q}] = 2^n$.

3. En déduire que la trisection d'un angle (c'est-à-dire construire $\cos \varphi/3$, en supposant $\cos \varphi$ construit) n'est généralement pas possible à la règle et au compas. *Indication :* On pourra relier ce problème à l'équation cubique $4x^3 - 3x - a = 0$.

12.11 Complément. Le même type d'idée permet de montrer une série de théorèmes d'impossibilités géométriques, qui étaient restés des questions ouvertes pendant des siècles avant l'avènement de la théorie de Galois. Il est par exemple impossible de
- carrer un cercle (c'est-à-dire construire un carré d'aire π, donc de côté $\sqrt{\pi}$)
- construire un nombre transcendant (voir la définition ci-dessous)
- dupliquer le cube (c'est-à-dire construire un cube de volume 2, donc de côté $2^{1/3}$) "à la règle et au compas" (même en supposant savoir utiliser un compas dans l'espace !)
- construire le polygône régulier à p côtés si p n'est pas de la forme $p_k = 2^{2^k} + 1$ avec $k \in \mathbb{N}$ (pour $k = 0, 1, 2, 3, 4$, p_k est premier, mais Euler a montré que p_5 ne

l'est pas, et on ne connaît d'ailleurs aucun autre p_k premier...).

12.12 Définition. Soit L une extension de K. Des éléments $\alpha_1, ..., \alpha_n$ de L sont *algébriquement dépendants* sur K si il existe un polynôme irréductible $F \in K[x_1, ..., x_n]$ non nul tel que

$$F(\alpha_1, ..., \alpha_n) = 0;$$

ils sont *algébriquement indépendants* sinon. Si $n = 1$, on dit respectivement que α_1 est *algébrique* ou *transcendant*.

Le *degré de transcendance* d'une extension de type fini L de K est le nombre maximal d'éléments algébriquement indépendants de L sur K.

(Dans une extension de type fini, il existe une borne supérieure pour le nombre d'éléments algébriquement indépendants.)

Quand on ne précise pas l'extension de corps, en arithmétique, c'est qu'on raisonne sur $\mathbb{C}/\mathbb{Q}$.

12.h Exercice. 1. Montrer que $\sqrt{2}$ est algébrique (pour l'extension $\mathbb{C}/\mathbb{Q}$).

2. Montrer que l'ensemble des nombres algébriques est dénombrable.

L'exercice ci-dessus montre que l'ensemble des nombres transcendants est infini non dénombrable (puisque c'est le cas de $\mathbb{C}$. Pourtant, pendant longtemps, on ne connaissait aucun exemple de nombre transcendant. C'est à Liouville, au 19e siècle, qu'il revient d'en avoir construit les premiers exemples, à Hermite d'avoir montré la transcendance de e, et à Lindemann d'avoir montré celle de π, répondant ainsi négativement à la conjecture de la *quadrature du cercle*, qui datait de l'Antiquité grecque.

12.i Exercice. Montrer que le degré de transcendance de $K(x_1, ..., x_n)$ sur K est n.

Nous allons maintenant décrire un procédé fondamental pour donner des racines aux polynômes quand ils n'en ont pas, en grossissant le corps dans lequel on cherche les racines.

12.13 Exemple (Adjonction d'une racine). Soit L une extension de type fini de la forme $L = K(\alpha)$, où α est un élément algébrique sur K i.e. il existe un polynôme $P(x) \in K[x]$ tel que $P(\alpha) = 0$. Parmi les tels polynômes, il en existe un, disons encore $P(x)$, de plus petit degré. Tous les autres sont multiples de $P(x)$ dans $K(x)$ (par division euclidienne), et P est donc unique à multiplication par un élément de K près. P s'appelle le *polynôme minimal* de α. On dit que l'extension L s'obtient par adjonction de la racine α de P. Nous allons décrire les éléments de L de façon très explicite. Considérons le morphisme d'anneaux

$$\varphi : K[x] \to L = K(\alpha), \quad F(x) \mapsto F(\alpha).$$

Le noyau I de φ est un idéal de $K[x]$; c'est le plus petit idéal de $K[x]$ contenant P, à savoir $PK[X]$, soit l'idéal engendré par P, noté (P). L est donc isomorphe à

$K[x]/(P)$. En notant n le degré de P, on voit que tout élément de $L \simeq K[x]/(P)$ est de la forme

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

avec $a_i \in K$, et que cette expression est unique (parce que P est minimal). Il s'avère donc que toute expression rationnelle en α est en fait un expression polynomiale en α, de degré $< n$, de sorte que $K(\alpha) = K[\alpha]$ est une extension de degré fini

$$[K(\alpha) : K] = n.$$

Finalement, α apparaît comme l'image de x par l'application de passage au quotient, et la construction précédente permet donc de donner un racine $\alpha = \bar{x}$ à tout polynôme $P \in K[x]$ irréductible dans K, en se plaçant dans l'extension $L = K[x]/(P)$ de K. L'algorithme de division euclidienne des polynômes montre que P est divisible par $x - \alpha$ sur L. Par récurrence descendante sur le degré de P, on voit qu'il existe une extension de K dans laquelle P est *scindé*, c'est-à-dire se décompose en produit de polynômes de degré 1. On peut montrer que la plus petite telle extension est unique à isomorphisme près. On l'appelle le *corps de décomposition* de P.

L'exemple le plus connu est celui de $\mathbb{C} \simeq \mathbb{R}[x]/(x^2 + 1) = \mathbb{R}[i]$, corps de décomposition de $x^2 + 1$.

12.j Exercice. Montrer que $\mathbb{R}[x]/(x^2 - 1)$ n'est pas un corps.

12.14 Complément (Clôture algébrique)**.** On peut même construire une extension de K, notée $\bar{K}$ et appelée la *clôture algébrique* de K, dans laquelle *tout* polynôme sur K est scindé et qui soit minimale pour cette propriété.[26] Par exemple, $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$, comme le montre le théorème de d'Alembert-Gauss (il est remarquable qu'en donnant une racine à $x^2 + 1$ on donne automatiquement des racines à tous les polynômes réels). Celle de $\mathbb{Q}$, notée donc $\bar{\mathbb{Q}}$, est l'ensemble des *nombres algébriques* ; elle est beaucoup plus mystérieuse.

Terminons cette section par la notion importante de caractéristique. Soient K un corps et $f : \mathbb{Z} \to K$, $n \mapsto n\,1$ (où "1" désigne le neutre de K, pas celui de $\mathbb{Z}$; cette notation est définie par $0.1 = 0$, par la récurrence positive $(n+1)\,1 = n\ 1+1$ et par la récurrence négative $-(n+1)\,1 = -n\,1 - 1$). Le noyau de f est un sous-groupe de $\mathbb{Z}$.

12.15 Définition. La *caractéristique* de K est 0 si $\ker f = \{0\}$; elle est p si $\ker f = p\mathbb{Z}$ (on sait qu'alors p est un nombre premier).

12.k Exercice. Parmi ces corps, lesquels sont de caractéristique nulle ou p :

$$\mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{Q}(x),\ \mathbb{R}(x),\ \mathbb{C}(x),\ \mathbb{Z}_p,\ \mathbb{Z}_p(x),\ \mathbb{Z}_p(x,y)?$$

12.16 Complément (Courbes algébriques [Sha05])**.** Soient $F \in \mathbb{C}[x,y]$ et C la courbe plane d'équation $F(x,y) = 0$ dans $\mathbb{C}^2$; C s'appelle une *courbe algébrique*. On suppose que F ne se factorise pas en un produit de polynômes non constant ; alors F et C sont

26. Ne pas confondre la notation $\bar{K}$ avec d'autres usage d'une barre au-dessus des lettres, par exemple pour l'adhérence d'une partie d'un espace topologique.

qualifiés d'*irréductibles*. Parmi toutes les telles courbes, on peut caractériser la courbe C par les coefficients de F ; c'est une façon très primitive de munir de coordonnées l'ensemble des courbes, et nous allons en voir une autre qui est plus intéressante.

Considérons une fracion rationnelle $R \in \mathbb{C}(X, Y)$ de la forme

$$\varphi(x, y) = \frac{P(x, y)}{Q(x, y)},$$

où le dénominateur Q n'est pas divisible par F. Considérons φ comme une fonction $(x, y) \mapsto \varphi(x, y)$, en restriction aux points de C uniquement. Cette fonction n'est pas définie aux points de C où Q s'annule. Sous nos hypothèses, on peut montrer que les tels points sont en nombre fini, alors que C est infinie. (Si on avait la même discussion pour une courbe algébrique dans $\mathbb{R}^2$, on supposerait que C est infinie.) Une telle fonction s'appelle une *fonction rationnelle* sur C ; elle définit vraiment une fonction complexe sur C privée d'un nombre fini de points. On montre que l'ensemble des fonctions rationnelles sur C forme un corps ; par exemple, φ est non nulle si et seulement si P n'est pas divisible par F, et alors la fonction $\varphi^{-1} = Q/P$ vérifie les conditions requises pour φ, ce qui montre l'existenc de l'inverse des éléments non nuls. Ce corps s'appelle le *corps des fonctions rationnelles sur* C et se note $K(C)$.

L'association du corps $K(C)$ à la courbe C est une méthode beaucoup plus précise pour "coordinatiser" C que de prendre les coefficients de F. Pour commencer, si l'on passe de coordonnées (x, y) dans $\mathbb{C}^2$ à d'autres coordonnées (x', y') (par changement de coordonnées linéaire f), l'équation de la courbe change (et il est difficile de reconnaître que les coefficients de la nouvelle équation correspondent à ceux de l'ancienne équation),tandis que le corps $K(C)$ est remplacé par un corps qui lui est isomorphe, comme on le voit facilement (l'isomorphisme étant $R \mapsto R \mapsto R \circ f$). Un autre point important est que si les corps $K(C)$ et $K(C')$ de ceux courbes C et C' sont isomorphes, cela a des conséquences cruciales sur la relation entre C et C'.

Par exemple, si C est l'axe des x, donc définie par l'équation $F(x, y) = y = 0$. La restriction d'une fonction φ à C donne une fonction de x :

$$\varphi(x, 0) = \frac{P(x, 0)}{Q(x, 0)}.$$

Le corps obtenu $K(C)$ est donc isomorphe au corps $K(x)$. La même conclusion vaut si C est une droite affine quelconque.

Examinons maintenant le cas des courbes C de degré 2 (c'est-à-dire que le polynôme F est de degré total 2 en x et y), et montrons que dans ce cas aussi le corps $K(C)$ est isomorphe au corps des fractions rationnelles d'une variable $K[t]$. Choisissons pour cela un point (a, b) arbitraire sur C, et soit t la pente de la droite joignant (x_0, y_0) à $(x, y) \in C$:

$$t = \frac{y - y_0}{x - x_0}.$$

C'est une fonction sur C, privée du nombre fini de points qui sont à la verticale de (x_0, y_0). Mais x et y eux-mêmes sont des fonctions rationnelles de t. En effet, comme $y - y_0 = t(x - x_0)$, sur C on a

$$F(x, y_0 + t(x - x_0)) = 0,$$

identiquement sur C. Comme C est de degré deux, cette équation est de degré 2, de la forme

$$a(t)x^2 + b(t)x + c(t) = 0,$$

où les coefficients sont des fonctions rationnelles de t. L'une des racines est connue, à savoir $x = x_0$. L'autre racine est obtenue par exemple en écrivant que la somme des racines vaut $-\frac{b(t)}{a(t)}$, et l'on obtient bien l'expression de x comme fonction rationnelle $x = f(t)$ de t, et de même pour $y = g(t)$. La correspondance $\varphi(x, y) \leftrightarrow \varphi(f(t), g(t))$ donne un isomorphisme de corps entre $K(C)$ et $K(t)$.

La signification géométrique de cet isomorphisme est que C peut être paramétrée par des fonctions rationnelles

$$x = f(t), \quad y = g(t).$$

Par exemple, si C a pour équation $y^2 = ax^2 + bx + c$, alors sur C on a $y = \sqrt{ax^2 + bx + c}$ et ce qui précède montre qu'à la fois x et $\sqrt{ax^2 + bx + c}$ peuvent s'exprimer comme des fonctions rationnelles d'une troisiemme variable t. Cette expression est utile, par exemple, pour calculer des intégrales indéterminées : toute intégrale

$$\int \varphi(x, \sqrt{ax^2 + bx + c})\, dx,$$

où φ est une fonction rationnelles, se réduit à l'intégrale d'une fonction rationnelle en t et peut donc ainsi s'exprimer en terme de fonctions élémentaires. Le changement de variable ainsi effectué s'appelle une *substitution d'Euler*.

Déjà pour la courbe C d'équation $y^2 = x^3 + 1$, le corps $K(C)$ n'est pas isomorphe au corps des fonctions rationnelles. Ceci est à rapprocher du fait que "intégrale elliptique"

$$\int \frac{dx}{x^3 + 1}$$

ne s'exprime pas en terme des fonctions élémentaires.

13 Introduction à la théorie de Galois [Sha05]

Soit L/K une extension d'un corps de caractéristique nulle. [27]

13.1 Définition. Un *automorphismes* d'une extension L/K est un automorphisme du corps L qui fixe chaque élément de K. Les automorphismes de K/L forment un groupe pour la composition, noté $\mathrm{Aut}(L/K)$.

Dans la suite, nous supposerons que L est une extension finie, i.e. $[L : K] < \infty$. En particulier, elle est de type fini, i.e. $L = K(\alpha_1, ..., \alpha_n)$, avec $\alpha_1, ..., \alpha_n \in K$.

13.2 Théorème. *Il existe $\alpha \in L$ tel que $L = K(\alpha)$; α s'appelle un* élément primitif *de l'extension.* [28]

Comme L/K est finie, α est algébrique : il existe un polynôme $P(x) \in K[x]$ non nul dont α soit une racine. On peut choisir $P(x)$ de degré minimal, donc irréductible sur K.

27. Les résultats principaux restent valables sous des hypothèses moins contraignantes, en particulier pour les corps finis.

28. En fait, la démonstration montre que la plupart des éléments de L sont primitifs.

Un automorphisme σ d'une extension $K(\alpha)/K$ est uniquement déterminé par la donnée de $\beta = \sigma(\alpha)$, puisque tout élément de l'extension est une expression polynomiale en α (exemple 12.13). Par ailleurs, β est aussi une racine de P : en notant $P(x) = \sum a_i x^i$, on a en effet

$$P(\beta) = \sum_i a_i \beta^i = \sum a_i \sigma(\alpha)^i = \sigma\left(\sum a_i \alpha^i\right) = \sigma(0) = 0.$$

Donc les automorphismes de $K(\alpha)/K$ apparaissent comme des "symétries" des racines de P (au sens où ils s'identifient à des permutations de ces racines). La subtilité est qu'il n'existe pas forcément d'automorphisme associé à chaque permutation.

De fait,

$$|\operatorname{Aut}(L/K)| \leqslant \deg P(x) = [K(\alpha), K].$$

Plus le groupe $\operatorname{Aut}(L/K)$ est grand, plus l'extension L/K apparaît symmétrique. Le cas limite est le cas d'égalité.

13.3 Définition. L'extension $L = K(\alpha)/K$ est *galoisienne* si

$$|\operatorname{Aut}(L/K)| = [K(\alpha), K].$$

On montre que L/K est galoisienne si et seulement si P se factorise sur L en facteurs de degré 1, i.e. P est *scindé* sur L.

13.4 Exemple (Extension galoisienne). Le groupe $\operatorname{Aut}(\mathbb{C}/\mathbb{R})$ contient l'identité et la conjugaison complexe $i \mapsto -i$, donc est d'ordre $2 = [\mathbb{C} : \mathbb{R}]$.

13.5 Exemple (Extension maximalement asymétrique). Soient $\gamma = 2^{1/3}$ la racine réelle de $\gamma^3 - 2 = 0$, et $L = \mathbb{Q}(\gamma)$. Un automorphisme σ de $L/\mathbb{Q}$ est déterminé par $\sigma(\gamma)$, qui doit être une racine de $x^3 - 2$ appartenant à $L \subset \mathbb{R}$. Il n'existe qu'une seule telle racine, à savoir γ elle-même. Donc $\sigma = \mathrm{id}$ et $\operatorname{Aut}(\mathbb{Q}(\gamma)/\mathbb{Q})$ est trivial, tandis que $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 3$.

13.6 Théorème. *Toute extension finie est contenue dans une extension galoisienne.*

Idée de démonstration. Sur L, écrivons $P(x) = (x - \alpha)P_1(x)$ avec $P_1(x) \in L[x]$. On construit une extension $L_1 = L(\alpha_1)$ avec $P_1(\alpha_1) = 0$, etc., jusqu'à obtenir un corps dans lequel P se factorise en facteurs de degré 1. L'extension obtenue est galoisienne. □

13.7 Définition. Le *groupe de Galois* de L/K est le groupe des automorphismes $\operatorname{Aut}(\bar{L}/K)$ de la plus petite extension galoisienne (contenant toutes les autres) contenant L/K ; on le note $\operatorname{Gal}(L/K)$. On parle aussi du *groupe de Galois* d'un polynôme $P(x) \in K[x]$, pour désigner le groupe de Galois de $L/K = K(\alpha)$ avec $P(\alpha) = 0$.

Tout automorphisme $\sigma \in \operatorname{Gal}(L/K)$ est déterminé par les images des racines α_i de $P(x)$, à choisir parmi les racines de $P(x)$. Donc σ s'identifie à une permutation des racines de $P(x)$, et $\operatorname{Gal}(L/K)$ agit ainsi sur cet ensemble de racines.

13.8 Exemple (Suite de l'exemple 13.5). Pour l'extension $\mathbb{Q}(\alpha)$ précédente,

$$P(x) = x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2).$$

Mais le polynôme $x^2 - \alpha x + \alpha^2$ n'a pas de racines dans $\mathbb{Q}(\alpha)$. Donc on pose $\bar{L} = L(\alpha_1)$ avec $\alpha_1^2 + \alpha\alpha_1 + \alpha^2 = 0$, donc $\alpha_1 = \left(\frac{-1+i\sqrt{3}}{2}\right)\alpha$. Ainsi, $\bar{L} = L(i\sqrt{3})$, et tout élément de L peut s'écrire $\xi + i\eta\sqrt{3}$, avec $\xi, \eta \in \mathbb{Q}(\alpha)$. Un automorphisme $\sigma \in \mathrm{Aut}(\bar{L}/\mathbb{Q})$ est déterminé par les valeurs de $\sigma(\alpha)$ et de $\sigma(i\sqrt{3})$. À cause de la contrainte que $(\sigma(\alpha))^3 = 2$, $\sigma(\alpha)$ est de la forme

$$\sigma(\alpha) = j^k\alpha,\ k = 0, 1, 2,$$

où $j = e^{i2\pi/3}$ est une racine troisième de l'unité. L'autre valeur à déterminer de σ, à savoir $\sigma(i\sqrt{3})$, vérfie la contrainte $\sigma(i\sqrt{3})^2 = -3$, donc elle est de la forme

$$\sigma(i\sqrt{3}) = \pm i\sqrt{3}.$$

On peut vérifier que n'importe quelle combinaison de ces valeurs de $\sigma(\alpha)$ et de $\sigma(i\sqrt{3})$ définissent bien un automorphisme de $\bar{L}/\mathbb{Q}$, de sorte que $|\mathrm{Aut}(\bar{L}/\mathbb{Q})| = 6$, et, comme $[\bar{L} : \mathbb{Q}] = 6$, l'extension $\bar{L}/\mathbb{Q}$ est galoisienne. Son groupe de Galois agit sur les racines de P, et n'importe quelle permutation de ses racines est ainsi atteinte, comme le montre le tableau suivant :

$\sigma(\alpha)$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$j\sqrt[3]{2}$	$j\sqrt[3]{2}$	$j^2\sqrt[3]{2}$	$j^2\sqrt[3]{2}$
$\sigma(i\sqrt{3})$	$i\sqrt{3}$	$-i\sqrt{3}$	$i\sqrt{3}$	$-i\sqrt{3}$	$i\sqrt{3}$	$-i\sqrt{3}$
permutation	(1)	(23)	(123)	(12)	(132)	(13)

Donc $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathfrak{S}_3$.

Le coeur de la théorie de Galois est une relation remarquable entre les extensions intermédiaires $K \subset L' \subset L$ d'une extension L/K et entre les sous-groupes de son groupe de Galois $G = \mathrm{Gal}(L/K)$. Cette relation permet de ramener les questions qu'on peut se poser sur les sous-extensions à des questions sur les sous-groupes, pour lesquelles on est a priori mieux armés.

Pour tout sous-groupe $H \leqslant \mathrm{Gal}(L/K)$, soit $L(H)$ le sous-corps de L constitué des points fixes de H. Pour tout sous corps L' intermédaire entre K et L, soit $G(L')$ le sous-groupe $\mathrm{Aut}(L/L')$ de $\mathrm{Gal}(L/K)$ (c'est l'ensemble des automorphismes de l'extension L/K qui fixent non seulement K mais L').

13.9 Théorème (Galois)**.** *Les applications $H \mapsto L(H)$ et $L' \mapsto G(L')$ sont inverses l'une de l'autre. Elles définissent donc une bijection entre les sous-groupes $H \leqslant \mathrm{Gal}(L/K)$ et les sous-corps L' de L contenant K. Cette correspondance est décroissante pour l'inclusion :*

$$H \subset H_1 \Leftrightarrow L(H_1) \subset L(H).$$

En outre,

$$[L(H) : K] = (G : H).$$

Enfin, une extension L' de K contenue dans L est galoisienne si et seulement si $G(L') \leqslant G$ est distingué, et dans ce cas

$$\mathrm{Gal}(L'/K) \simeq G/G(L').$$

L'application la plus classique de ce théorème concerne la résolubilité des équations polynomiales : existe-t-il une formule (les opérations permises étant $+$, $-$, $\times$, $/$, $\sqrt[n]{}$) donnant les racines d'un polynôme en fonction de ses coefficients ?

Commençons par le cas de $P(x) = x^n - 1$. Soit K le corps des nombres complexes engendré sur $\mathbb{Q}$ par la racine n-ièmes primitive l'unité $\zeta = e^{i2\pi/n}$; K est le *corps cyclotomique*. (Si F est un sou-corps quelconque de $\mathbb{C}$, $F(\zeta_n)$ s'appelle aussi une *extension cyclotomique* de F.) Comme les racines de P sont les puissances de ζ, K est le corps de décomposition de $x^n - 1$. Dans la suite, concentrons-nous sur le cas où n est un nombre premier $p \geqslant 3$. Le polynôme $x^{p-1} + \cdots + x + 1$ est irréductible sur $\mathbb{Q}$ et $\zeta = e^{i2\pi/p}$ est l'une de ses racines. Donc c'est le polynôme irréductible de P sur $\mathbb{Q}$, et ses racines sont ζ, ζ^2, ..., ζ^{p-1}. Donc le groupe de Galois de $\mathbb{Q}(\zeta)/\mathbb{Q}$ est d'ordre $p-1$.

13.a Exercice.
1. Montrer que $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ est isomorphe au groupe multiplicatif des inversibles de $\mathbb{F}_p$; c'est un groupe cyclique d'ordre $p-1$.

2. Montrer que, pour tout sous-corps F de $\mathbb{C}$, $\mathrm{Gal}(F(\zeta)/F)$ est cyclique.

Supposons que $F = \mathbb{Q}$. Alors le groupe de Galois G de l'extension $K = \mathbb{Q}(\zeta)$ de $\mathbb{Q}$ possède exactement un sous-groupe d'ordre k pour chaque entier k qui divise $p-1$. Si l'on note $r = \frac{p-1}{k}$ et si σ engendre G, le sous-groupe d'ordre k est engendré par σ^r. D'après le théorème de Galois, il existe donc exactement un cors L intermédiaire entre $\mathbb{Q}$ et K avec $[L : \mathbb{Q}] = r$. Ces corps sont engendrés par certaines puissances de ζ.

De même, on peut montrer que, si K est une extension de $\mathbb{Q}$ qui contient toutes les racines n-ièmes de l'unité, une extension $K(\sqrt[n]{a})$ (appelée *extension radicale*) est précisément une extension donc le groupe de Galois est cyclique. Ceci étant établi, les propriétés simples des groupes résolubles permettent de montrer le théorème suivant.

13.10 Théorème. *Une extension L/K est contenue dans une extension Λ de K obtenue par extensions radicales successives :*

$$\Lambda = \Lambda_1 \supset \Lambda_2 \supset \cdots \supset \Lambda_r = K, \quad \textit{avec} \quad \Lambda_{i-1} = \Lambda_i(\lambda_i^{1/n}),\ \lambda_i \in \Lambda_i,$$

si et seulement si son groupe de Galois est résoluble.

C'est ce théorème qui a conduit à définir les groupes résolubles tels que nous les avons définis, et qui a déterminé cette terminologie.

Considérons par exemple le corps des fractions rationnelles $L = k(x_1, ..., x_n)$ sur un corps k, et le sous-corps K des fractions rationnelles symétriques (c'est-à-dire invariantes par permutation des n arguments). Un résultat classique est que $K = k(\sigma_1, ..., \sigma_n)$, où les σ_i sont les polynômes symétriques élémentaires. [29]

29. Les polynômes σ_i sont définis par

$$\sigma_i = \sum_{1 \leqslant j_1 < j_2 < \ldots < j_i} x_{j_1} x_{j_2} \ldots x_{j_i}.$$

L'application qui prolonge $\sigma_i \mapsto y_i$ définit un isomorphisme entre $k(\sigma_1, ..., \sigma_n)$ avec $k(y_1, ..., y_n)$. Le groupe de Galois $\mathrm{Gal}(L/K) = \mathfrak{S}_n$ contient toutes les permutations des x_i. Mais les x_i sont les racines de l'équation

$$x^n - \sigma_1 x^{n-1} + ... \pm \sigma_n = 0.$$

Donc on voit que le groupe de Galois de l'équation

$$x^n - y_1 x^{n-1} + ... \pm y_n = 0 \tag{7}$$

sur le corps $k(y_1, ..., y_n)$, où y_1, ..., y_n sont n indéterminées, est le groupe symétrique $\mathfrak{S}_n$. L'équation (7) s'appelle l'*équation générique* de degré n. En combinant le l'exercice 11.l et le théorème 13.10, on obtient le résultat suivant.

13.11 Théorème. *L'équation générique de degré n est résoluble par radicaux si $n \leqslant 4$, et non résoluble pour $n \geqslant 5$.*

La structure des formules pour résoudre par radicaux les équations de degrés 2, 3 ou 4 peut être prédite par les propriétés du groupe symétrique $\mathfrak{S}_n$ pour $n = 2$, 3 ou 4, décrites dans le théorème 11.7.

Pour (beaucoup) plus de détails sur cette belle théorie, nous renvoyons à l'excellent livre de M. Artin [Art91]. Les exposés de V. Arnold [Ale04] en donnent une version géométrique et topologique, tandis que le livre de A. et R. Douady [DD04] fait le lien entre les points de vue.

L'application $(x_1, ..., x_n) \mapsto (\sigma_1, ..., \sigma_n)$ est l'*appication de Viète*.

Liste des symboles

$R_g x$	action à droite de G sur X, 20
$L_g x$	action à gauche de G sur X, 20
$Ad_g x$	action adjointe de G sur X, 20
$\mathbb{Z}/n\mathbb{Z}$	anneau des entiers modulo n, 24
$K(x)$	corps des fractions rationnelles en x sur K, 51
$\mathcal{C}$	corps des nombres constructibles, 51
$K((x))$	corps des séries de Laurent formelles, 53
$\mathbb{F}_p$	corps fini de cardinal p, 53
$[L : K]$	degré de l'extension L/K, 55
$\mathcal{H}^2(G, A)$	2e groupe de cohomologie de l'extension G de A, 38
$G\backslash X$	espace des orbites de G sur X, 17
$K(\alpha_1, ..., \alpha_n)$	extension de type fini de K, 54
$\mathfrak{A}_n$	groupe alterné de degré n, 49
C_n	groupe cyclique d'ordre n, 4
$\mathrm{Gal}(L/K)$	groupe de Galois de L/K, 61
K	groupe de Klein, 50
DG	groupe dérivé de G, 43
$\mathrm{Aut}(L/K)$	groupe des automorphismes de l'extension L/K, 60
$D(E)$	groupe des déplacements de E, 5
T	groupe des symétries du tétraèdre, 22
T^+	groupe des rotations du tétraèdre, 22
$\mathrm{Trans}(X)$	groupe des transformations de X, 4
D_n	groupe dihédral d'ordre $2n$, 4
O	groupe du dodécahèdre régulier, 44
$GL(E)$	groupe general linéaire de E, 4
$O(E)$	groupe orthogonal de E, 6
Q_8	groupe quaternionique, 41
$\mathfrak{S}_n$	groupe symétrique de degré n, 19
(P)	idéal engendré par l'élément P d'un anneau, 57
$(G : H)$	indice de H dans G, 20
$G \hookrightarrow G'$	monomorphisme de G dans G', 11
$G \twoheadrightarrow G'$	épimorphisme de G dans G', 11
σ_i	polynôme symétrique élémentaire, 63
$\pi_1(X, \xi)$	premier groupe d'homotopie de X, 13
$X/\sim$	quotient d'un ensemble, 22
$\epsilon(\sigma)$	signature d'une permutation σ, 48
$\langle X \rangle$	sous-groupe engendré par X, 11
$H \leqslant G$	H sous-groupe de G, 10
$M^T = {}^tM$	transposée de M, 6

Références

[Ale04] V.B. Alekseev. *Abel's Theorem in Problems and Solutions : Based on the lectures of Professor V.I. Arnold*. Kluwer International Series in. Springer Netherlands, 2004.

[Art91] Michael Artin. *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[DD04] Adrien Douady and Régine Douady. *Algèbre et théorie galoisiennes*. Cassini, 2004.

[Hat02] Allen Hatcher. *Algebraic topology*. Cambridge University Press, Cambridge, 2002. Version électronique : `http://www.math.cornell.edu/~hatcher/AT/ATpage.html`.

[Sha05] Igor R. Shafarevich. *Basic notions of algebra*, volume 11 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2005.

[Ste94] Shlomo Sternberg. *Group theory and physics*. Cambridge University Press, Cambridge, 1994.

Index