Théorie de Galois

Des groupes de permutations à l'impossibilité de la formule du cinquième degré

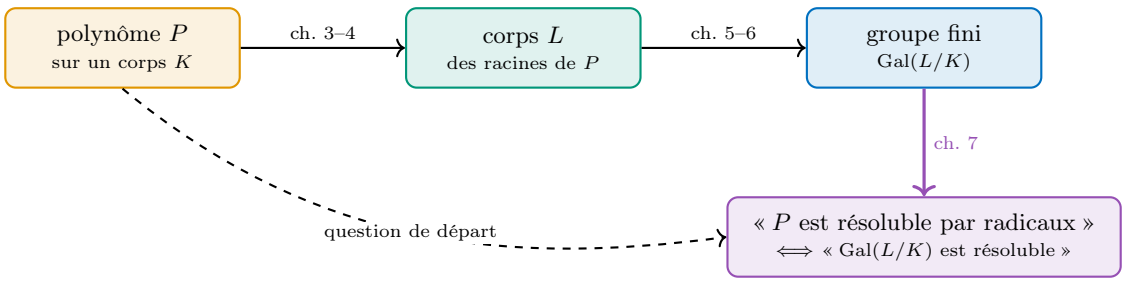
> *Tu prieras publiquement Jacobi ou Gauss de donner leur avis, non sur la vérité, mais sur l'importance des théorèmes. Après cela, il y aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.*
>
> Évariste Galois, lettre à Auguste Chevalier, 29 mai 1832
> (*Œuvres mathématiques d'Évariste Galois*, Gauthier-Villars, 1897, p. 32)

On résout l'équation du second degré depuis les scribes babyloniens ; celles du troisième et du quatrième degré depuis les algébristes italiens du XVI^{e} siècle. Il était donc raisonnable d'espérer une formule pour le cinquième degré, et deux siècles et demi d'efforts y ont été consacrés. La réponse, obtenue par **Ruffini** en 1799, complétée par **Abel** en 1824, puis expliquée par **Galois** en 1831, est négative : *aucune* formule composée d'additions, de multiplications et d'extractions de racines ne peut exprimer les solutions de l'équation générale de degré cinq.

Ce qui fait le prix de la réponse de Galois n'est pas la négation, c'est la méthode. À chaque équation, Galois associe un *groupe* de permutations de ses racines : celles qui respectent toutes les relations algébriques que ces racines vérifient. Ce groupe mesure exactement l'« ambiguïté » de l'équation, c'est-à-dire ce qu'il reste d'indiscernable entre les racines une fois écrites toutes les équations à coefficients rationnels qu'elles satisfont. La résolubilité par radicaux devient alors une propriété purement algébrique de ce groupe fini. La question analytique s'est transformée en question de théorie des groupes — et cette transformation, plus que le résultat lui-même, a façonné l'algèbre des deux siècles suivants.

Le cours part de la définition d'un groupe et ne suppose rien d'autre que l'arithmétique élémentaire et le maniement des polynômes. Les deux premiers chapitres construisent l'outillage des groupes finis, jusqu'à la notion de *groupe résoluble* et à la non-résolubilité de $\mathfrak{S}_n$ pour $n \geqslant 5$. Les chapitres 3 à 5 construisent l'outillage des corps : anneaux de polynômes, extensions, degrés, séparabilité, normalité. Le chapitre 6 les fait se rencontrer dans la *correspondance de Galois*, qui traduit un treillis de corps en un treillis de groupes. Le chapitre 7 en tire les conséquences : le critère de résolubilité, le théorème d'Abel-Ruffini, la classification des polygones réguliers constructibles, et une démonstration purement algébrique du théorème fondamental de l'algèbre.

Chaque définition est suivie d'exemples, et chaque énoncé d'une démonstration complète. Deux résultats seulement sont admis, parce que leur preuve relève d'un autre domaine : l'existence de la clôture algébrique, qui repose sur un argument ensembliste de maximalité, et la transcendance de π, qui relève de l'analyse. Ils sont signalés comme tels à l'endroit où ils servent.



Le fil du cours en une image : on traduit un problème sur les polynômes en un problème sur les corps, puis un problème sur les corps en un problème sur les groupes finis — où il devient décidable.

Chapitre 1

Groupes

Un groupe est ce qui reste d'une figure quand on ne retient que ses symétries, d'une équation quand on ne retient que les échanges possibles entre ses racines. La notion s'est dégagée lentement : elle apparaît en filigrane chez **Lagrange** (1771) dans l'étude des fonctions des racines, prend corps chez **Galois** (1831) qui en fixe le nom, et n'est axiomatisée sous la forme abstraite que nous allons donner qu'à la fin du XIX$^{\text{e}}$ siècle, par **Weber** et **von Dyck**. Ce chapitre construit l'outillage minimal : sous-groupes, morphismes, groupe symétrique, théorème de Lagrange. Tout y est fini ou presque, et tout servira.

1.1 Lois de composition et groupes

Définition : Soit E un ensemble. Une **loi de composition interne** sur E est une application $* : E \times E \to E$. On note $x * y$ l'image du couple $(x\,;y)$.

La loi $*$ est dite **associative** lorsque $(x * y) * z = x * (y * z)$ pour tous $x, y, z \in E$, et **commutative** lorsque $x * y = y * x$ pour tous $x, y \in E$. Un élément $e \in E$ est un **élément neutre** si $e * x = x * e = x$ pour tout $x \in E$.

Exemple : L'addition et la multiplication sont des lois internes sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$; elles y sont associatives et commutatives, de neutres respectifs 0 et 1. La composition $\circ$ est une loi interne sur l'ensemble des applications de E dans E : elle est associative, de neutre id_E, mais non commutative dès que E possède au moins deux éléments. Sur l'ensemble $\mathcal{P}(E)$ des parties de E, la réunion et l'intersection sont internes, associatives et commutatives, de neutres $\varnothing$ et E.

En revanche, la division n'est pas une loi interne sur $\mathbb{Z}$, car $\frac{1}{2} \notin \mathbb{Z}$, et la moyenne $(x\,;y) \mapsto \frac{x+y}{2}$ n'en est pas une non plus, pour la même raison. Vérifier l'internalité est toujours le premier réflexe, et la remarque ci-dessous y revient.

Remarque : Le mot *interne* n'est pas décoratif : il exige que $x * y$ appartienne encore à E. C'est la première chose à vérifier, et l'erreur la plus répandue est de l'oublier. Ainsi la soustraction est une loi interne sur $\mathbb{Z}$ mais pas sur $\mathbb{N}$, et le produit vectoriel est une loi interne sur $\mathbb{R}^3$ alors que le produit scalaire n'en est pas une, puisqu'il produit un nombre et non un vecteur.

Définition : Un **groupe** est un couple $(G\,;*)$ où G est un ensemble non vide et $*$ une loi de composition interne sur G vérifiant :

- **associativité :** pour tous $x, y, z \in G$, $(x * y) * z = x * (y * z)$;
- **existence d'un neutre :** il existe $e \in G$ tel que $e * x = x * e = x$ pour tout $x \in G$;
- **existence des symétriques :** pour tout $x \in G$, il existe $x' \in G$ tel que $x * x' = x' * x = e$.

Le groupe est dit **abélien** (ou commutatif) si de plus $x * y = y * x$ pour tous $x, y \in G$.

Remarque : On utilise deux jeux de notations. En *notation multiplicative*, on écrit xy pour $x * y$, 1 ou e pour le neutre et x^{-1} pour le symétrique, appelé alors **inverse**. En *notation additive*, réservée par convention aux groupes abéliens, on écrit $x+y$, 0 et $-x$, appelé **opposé**. Ce ne sont que des habillages : les axiomes sont les mêmes. Dans tout ce cours, la notation multiplicative est la règle, sauf pour $(\mathbb{Z}\,;+)$ et $(\mathbb{Z}/n\mathbb{Z}\,;+)$.

Exemple : Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de l'addition sont des groupes abéliens, de neutre 0. En revanche $(\mathbb{N}\,;+)$ n'en est pas un : l'entier 1 n'y a pas d'opposé. De même $(\mathbb{Q}\,;\times)$ n'est pas un groupe, car 0 n'est pas inversible ; mais $(\mathbb{Q}^*\,;\times)$ en est un, où $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. On retiendra que retirer un seul élément peut transformer un non-groupe en groupe.

Exemple : Soit X un ensemble. L'ensemble $\mathfrak{S}(X)$ des *bijections* de X dans lui-même, muni de la composition, est un groupe : la composée de deux bijections est une bijection, la composition est associative, l'identité est neutre, et la bijection réciproque fournit le symétrique. Ce groupe n'est pas abélien dès que X possède au moins trois éléments, comme on le vérifiera au paragraphe 1.4. C'est le groupe fondamental de tout le cours : le groupe de Galois d'une équation en sera un sous-groupe.

Exemple : Pour $n \geqslant 1$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence modulo n, muni de l'addition $\overline{a} + \overline{b} = \overline{a+b}$, est un groupe abélien à n éléments. La vérification que l'addition est bien définie — c'est-à-dire indépendante des représentants choisis — repose sur le fait que si $a \equiv a'$ et $b \equiv b'$ modulo n, alors $a + b \equiv a' + b'$ modulo n. On dispose ainsi, pour chaque entier n, d'un groupe fini explicite.

Propriété 1.1 : Dans un groupe $(G\,;*)$, l'élément neutre est unique, et chaque élément possède un unique symétrique.

∘ *Démonstration :* Soit $(G\,;*)$ un groupe. Supposons que e et e' soient deux éléments neutres de G. Puisque e est neutre, $e * e' = e'$. Puisque e' est neutre, $e * e' = e$. Ces deux égalités portent sur le même élément $e * e'$, donc $e = e'$.

Soit maintenant $x \in G$, et soient x' et x'' deux symétriques de x. On calcule le produit $x' * x * x''$ de deux manières, ce que l'associativité autorise :

$$x' * (x * x'') = x' * e = x' \qquad \text{et} \qquad (x' * x) * x'' = e * x'' = x''$$

Les deux membres de gauche sont égaux par associativité, donc $x' = x''$. Remarquons que l'associativité est ici essentielle : c'est elle, et elle seule, qui permet de faire glisser les parenthèses. □

Propriété 1.2 : Soit $(G\,;\cdot)$ un groupe. Pour tous $x, y, z \in G$:

- $xy = xz \Longrightarrow y = z$ et $yx = zx \Longrightarrow y = z$ (**régularité**) ;
- $\left(x^{-1}\right)^{-1} = x$ et $(xy)^{-1} = y^{-1}x^{-1}$;
- pour tout $a, b \in G$, l'équation $ax = b$ possède l'unique solution $x = a^{-1}b$.

∘ *Démonstration :* Soient $x, y, z \in G$. Pour la régularité à gauche, on compose l'égalité $xy = xz$ par x^{-1} à gauche :

$$x^{-1}(xy) = x^{-1}(xz) \quad \text{soit} \quad \left(x^{-1}x\right)y = \left(x^{-1}x\right)z \quad \text{soit} \quad ey = ez \quad \text{soit} \quad y = z$$

La régularité à droite se traite de même en composant par x^{-1} à droite.

Soient à nouveau $x, y \in G$. L'égalité $xx^{-1} = x^{-1}x = e$ dit exactement que x est un symétrique de x^{-1} ; par unicité du symétrique, $\left(x^{-1}\right)^{-1} = x$. Ensuite :

$$(xy)\left(y^{-1}x^{-1}\right) = x\left(yy^{-1}\right)x^{-1} = xex^{-1} = xx^{-1} = e$$

et le calcul symétrique donne $\left(y^{-1}x^{-1}\right)(xy) = e$. Par unicité du symétrique, $(xy)^{-1} = y^{-1}x^{-1}$.

Soient enfin $a, b \in G$. On a $a\left(a^{-1}b\right) = \left(aa^{-1}\right)b = b$, donc $a^{-1}b$ est bien solution de l'équation $ax = b$; et si $x, x' \in G$ vérifient $ax = b = ax'$, la régularité à gauche donne $x = x'$. □

Remarque : L'ordre est renversé dans $(xy)^{-1} = y^{-1}x^{-1}$, et l'erreur la plus répandue est de l'oublier. L'image concrète est celle de l'habillage : pour défaire « mettre les chaussettes puis les chaussures », il faut retirer les chaussures *puis* les chaussettes.

Définition : L'**ordre** d'un groupe G est son cardinal, noté $|G|$. Lorsque $|G|$ est fini, on dit que G est un **groupe fini**. La **table de Cayley** d'un groupe fini $G = \{g_1, \ldots, g_n\}$ est le tableau à double entrée dont la case $(i\,;j)$ contient $g_i g_j$.

$\mathbb{Z}/4\mathbb{Z}$

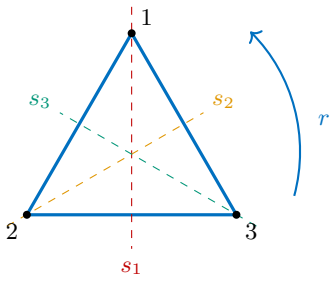
	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$V = \{e, a, b, c\}$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Les deux groupes ci-dessus ont quatre éléments et sont abéliens — leurs tables sont symétriques par rapport à la diagonale — mais ils diffèrent : dans $\mathbb{Z}/4\mathbb{Z}$ la diagonale contient $\overline{0}, \overline{2}, \overline{0}, \overline{2}$, tandis que dans le **groupe de Klein** V elle ne contient que le neutre. Autrement dit, tout élément de V est son propre inverse, ce qui est faux dans $\mathbb{Z}/4\mathbb{Z}$. Dans chaque table, chaque ligne et chaque colonne contient chaque élément exactement une fois : c'est exactement la propriété 1.2, l'équation $ax = b$ ayant une solution unique.

Exemple : Considérons un triangle équilatéral et l'ensemble D_3 des isométries du plan qui le laissent globalement invariant. Il y en a six : l'identité id, les rotations r et r^2 de centre l'isobarycentre et d'angles $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$, et les trois réflexions s_1, s_2, s_3 d'axes les médiatrices. Muni de la composition, D_3 est un groupe d'ordre 6, le **groupe diédral** d'ordre 6. Il n'est pas abélien : en numérotant les sommets $1, 2, 3$ et en notant s_1 la réflexion fixant le sommet 1, on vérifie sur la figure ci-dessous que $r \circ s_1 = s_3$ tandis que $s_1 \circ r = s_2$.



les six permutations des sommets

$$\text{id} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad s_1 \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$r \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad s_2 \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$r^2 \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad s_3 \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

À gauche, le triangle et ses trois axes de symétrie, chacun de sa couleur ; l'axe s_k passe par le sommet k, qui est donc fixé par la réflexion correspondante, et la rotation r tourne dans le sens direct. À droite, l'effet de chaque isométrie sur les numéros des sommets, la seconde ligne indiquant l'image de chaque sommet. Toute isométrie du triangle est déterminée par la permutation qu'elle induit sur les sommets : D_3 s'identifie ainsi au groupe de *toutes* les permutations de $\{1, 2, 3\}$. Cette identification d'un groupe de symétries à un groupe de permutations est le prototype de ce que fera la théorie de Galois avec les racines d'un polynôme.

1.2 Sous-groupes

Définition : Soit $(G\,;\cdot)$ un groupe. Une partie $H \subseteq G$ est un **sous-groupe** de G si H contient le neutre, est stable par produit et par passage à l'inverse. On note $H \leqslant G$.

Exemple : Tout groupe G possède au moins deux sous-groupes, dits *triviaux* : $\{e\}$ et G lui-même. Dans $(\mathbb{C}^*\,;\times)$, l'ensemble $\mathbb{U} = \{z \in \mathbb{C}\ ;\ |z| = 1\}$ est un sous-groupe, puisque $|zz'| = |z||z'|$ et $\left|z^{-1}\right| = |z|^{-1}$. Dans $\mathfrak{S}_3$, la partie $\{\text{id}\,;(1\ 2)\}$ en est un, car $(1\ 2)^2 = \text{id}$.

En revanche $\{\text{id}\,;(1\ 2)\,;(1\ 3)\}$ n'en est pas un : le produit $(1\ 2)(1\ 3)$ vaut $(1\ 3\ 2)$, qui n'y figure pas. Un sous-groupe doit être stable, et non simplement contenir quelques éléments.

Propriété 1.3 : Soit G un groupe et $H \subseteq G$. Alors H est un sous-groupe de G si et seulement si :

$$H \neq \varnothing \qquad \text{et} \qquad \forall x, y \in H,\ xy^{-1} \in H$$

Un sous-groupe est alors lui-même un groupe pour la loi induite, de même neutre que G.

∘ *Démonstration :* Soient G un groupe et $H \subseteq G$ une partie. Supposons d'abord que H soit un sous-groupe de G. Il contient e, donc il est non vide, et si $x, y \in H$ alors $y^{-1} \in H$ puis $xy^{-1} \in H$ par stabilité du produit.

Réciproquement, supposons la condition vérifiée. Comme H est non vide, choisissons $h \in H$; en prenant $x = y = h$, on obtient $hh^{-1} = e \in H$. En prenant ensuite $x = e$ et $y \in H$, on obtient $ey^{-1} = y^{-1} \in H$: H est stable par inverse. Enfin, pour $x, y \in H$, on vient de voir que $y^{-1} \in H$, donc $x\left(y^{-1}\right)^{-1} = xy \in H$: H est stable par produit.

La loi de G se restreint donc en une loi interne sur H, qui reste associative ; $e \in H$ y est neutre, et chaque élément y a son inverse. Ainsi $(H\,;\cdot)$ est un groupe. □

Remarque : Le critère condense les trois vérifications en une seule. Attention toutefois : l'hypothèse $H \neq \varnothing$ ne peut pas être omise, car la partie vide satisfait vacuement la seconde condition sans être un sous-groupe. En pratique on vérifie que $e \in H$, ce qui établit à la fois la non-vacuité et un premier élément.

Exemple : Dans $(\mathbb{Z}\,;+)$, l'ensemble $2\mathbb{Z}$ des entiers pairs est un sous-groupe : il contient 0, et la différence de deux entiers pairs est paire. En revanche l'ensemble des entiers impairs n'en est pas un, ne serait-ce que parce qu'il ne contient pas 0. Dans $(\mathbb{R}^*\,;\times)$, l'ensemble $\{-1\,;1\}$ est un sous-groupe d'ordre 2, et $\mathbb{R}_+^*$ un sous-groupe d'indice 2.

Propriété 1.4 : Toute intersection de sous-groupes de G est un sous-groupe de G. Par conséquent, pour toute partie $S \subseteq G$, il existe un plus petit sous-groupe de G contenant S : c'est l'intersection de tous les sous-groupes contenant S, noté $\langle S \rangle$ et appelé **sous-groupe engendré** par S.

∘ *Démonstration :* Soit $(H_i)_{i\in I}$ une famille de sous-groupes et $H = \bigcap_{i\in I} H_i$. Chaque H_i contient e, donc $e \in H$ et $H \neq \varnothing$. Si $x, y \in H$, alors pour chaque i on a $x, y \in H_i$, donc $xy^{-1} \in H_i$; ceci valant pour tout i, on obtient $xy^{-1} \in H$. La propriété 1.3 conclut.

Pour la seconde assertion, notons $\mathcal{H}$ l'ensemble des sous-groupes de G contenant S. Il est non vide car $G \in \mathcal{H}$, donc $\langle S \rangle = \bigcap_{H\in\mathcal{H}} H$ a un sens ; c'est un sous-groupe par ce qui précède, il contient S, et il est contenu dans tout sous-groupe contenant S puisqu'un tel sous-groupe figure dans l'intersection. □

Remarque : La *réunion* de deux sous-groupes n'est presque jamais un sous-groupe : dans $\mathbb{Z}$, la réunion $2\mathbb{Z} \cup 3\mathbb{Z}$ contient 2 et 3 mais pas 5. On montre d'ailleurs que $H \cup K$ est un sous-groupe si et seulement si $H \subseteq K$ ou $K \subseteq H$. C'est précisément parce que la réunion échoue qu'il faut passer par le sous-groupe *engendré*.

Propriété 1.5 : Soit G un groupe et $x \in G$. Alors $\langle x \rangle = \left\{x^k \ ; \ k \in \mathbb{Z}\right\}$, où l'on pose $x^0 = e$, $x^{k+1} = x^k x$ pour $k \geqslant 0$ et $x^{-k} = \left(x^k\right)^{-1}$.

∘ *Démonstration :* Notons $P = \left\{x^k \ ; \ k \in \mathbb{Z}\right\}$. Les règles de calcul $x^m x^n = x^{m+n}$ et $(x^m)^{-1} = x^{-m}$, valables pour tous $m, n \in \mathbb{Z}$, se démontrent par récurrence à partir de l'associativité ; nous les admettons ici comme relevant du calcul élémentaire. Elles montrent que P est non vide et que $x^m \left(x^n\right)^{-1} = x^{m-n} \in P$, donc P est un sous-groupe contenant x, d'où $\langle x \rangle \subseteq P$.

Réciproquement, tout sous-groupe H contenant x contient $x^2 = x \cdot x$, puis par récurrence immédiate x^k pour tout $k \geqslant 0$, puis $x^{-k} = \left(x^k\right)^{-1}$ par stabilité par inverse. Donc $P \subseteq H$, et en particulier $P \subseteq \langle x \rangle$. D'où l'égalité. □

Définition : Un groupe G est **cyclique** (on dit aussi *monogène* lorsqu'il est infini) s'il existe $x \in G$ tel que $G = \langle x \rangle$; un tel x est un **générateur** de G.

L'**ordre** d'un élément $x \in G$ est le plus petit entier $n \geqslant 1$ tel que $x^n = e$, s'il existe ; sinon x est dit d'ordre infini. On le note $o(x)$.

Exemple : Le groupe $(\mathbb{Z}\,;+)$ est monogène, engendré par 1 — et aussi par -1, un générateur n'ayant aucune raison d'être unique. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique, engendré par $\overline{1}$.

Dans $(\mathbb{C}^*\,;\times)$, l'élément -1 est d'ordre 2, l'élément i est d'ordre 4, et l'élément 2 est d'ordre infini, aucune de ses puissances 2^n avec $n \geqslant 1$ ne valant 1. Dans $\mathfrak{S}_3$, la transposition (1 2) est d'ordre 2 et le cycle (1 2 3) est d'ordre 3 ; le groupe $\mathfrak{S}_3$ lui-même n'est pas cyclique, car il faudrait pour cela un élément d'ordre 6, et ses six éléments sont d'ordre 1, 2 ou 3.

Théorème 1.1 : sous-groupes de $\mathbb{Z}$:
Les sous-groupes de $(\mathbb{Z}\,;+)$ sont exactement les ensembles $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

∘ *Démonstration :* Chaque $n\mathbb{Z}$ est un sous-groupe : il contient 0, et $na - nb = n(a-b)$.

Réciproquement, soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, H contient un élément $h \neq 0$, et aussi $-h$; l'un des deux est strictement positif, donc l'ensemble $H \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$. Elle admet donc un plus petit élément n.

Comme $n \in H$ et que H est un sous-groupe, $n\mathbb{Z} \subseteq H$ par la propriété 1.5. Inversement, soit $h \in H$. La division euclidienne de h par n s'écrit $h = qn + r$ avec $0 \leqslant r < n$. Alors $r = h - qn$ est différence de deux éléments de H, donc $r \in H$. Si r était strictement positif, ce serait un élément de $H \cap \mathbb{N}^*$ strictement plus petit que n, ce qui contredit la minimalité de n. Donc $r = 0$ et $h = qn \in n\mathbb{Z}$. Ainsi $H = n\mathbb{Z}$. □

Remarque : Cette démonstration est le modèle de toutes celles qui suivront la même stratégie : *prendre le plus petit élément positif, puis faire une division euclidienne pour montrer qu'il engendre tout.* Nous la rencontrerons au chapitre 3 pour montrer que $K[X]$ est principal, et c'est le même argument qui donnera l'existence du polynôme minimal au chapitre 4. Il vaut la peine de la retenir sous cette forme.

Propriété 1.6 : Soit x un élément d'ordre fini n d'un groupe G. Alors :

$$\left\{k \in \mathbb{Z} \ ; \ x^k = e\right\} = n\mathbb{Z} \qquad \text{et} \qquad \langle x \rangle = \left\{e, x, x^2, \ldots, x^{n-1}\right\} \text{ est de cardinal } n$$

Autrement dit, l'ordre d'un élément est l'ordre du sous-groupe qu'il engendre.

∘ *Démonstration :* Posons $A = \{k \in \mathbb{Z} \,;\, x^k = e\}$. C'est un sous-groupe de $\mathbb{Z}$: il contient 0, et si $x^k = x^\ell = e$ alors $x^{k-\ell} = x^k \left(x^\ell\right)^{-1} = e$. Par le théorème 1.1, $A = m\mathbb{Z}$ pour un $m \in \mathbb{N}$, et m est le plus petit élément strictement positif de A, c'est-à-dire $m = n$ par définition de l'ordre.

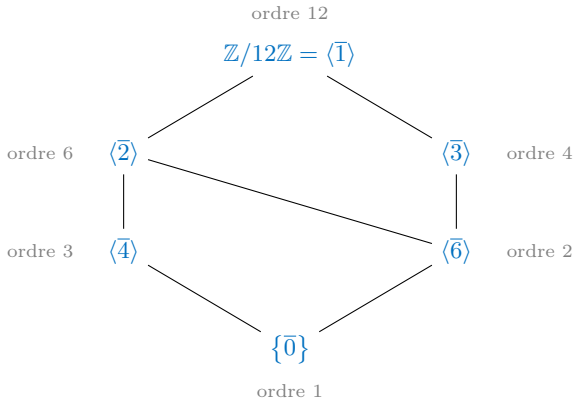
Montrons ensuite que $\langle x\rangle = \{e, x, \dots, x^{n-1}\}$. L'inclusion $\supseteq$ est claire. Pour $\subseteq$, soit $k \in \mathbb{Z}$; écrivons $k = qn + r$ avec $0 \leqslant r \leqslant n-1$. Alors :

$$x^k = x^{qn+r} = (x^n)^q\, x^r = e^q x^r = x^r$$

Enfin ces n éléments sont deux à deux distincts : si $x^i = x^j$ avec $0 \leqslant i \leqslant j \leqslant n-1$, alors $x^{j-i} = e$ avec $0 \leqslant j - i \leqslant n-1$, donc $j - i \in n\mathbb{Z} \cap [\![0\,;n-1]\!] = \{0\}$, soit $i = j$. □

Exemple : Dans $(\mathbb{C}^*\,;\times)$, l'élément i a pour ordre 4, car $\mathrm{i}^1 = \mathrm{i}$, $\mathrm{i}^2 = -1$, $\mathrm{i}^3 = -\mathrm{i}$ et $\mathrm{i}^4 = 1$. Le sous-groupe engendré est $\langle \mathrm{i}\rangle = \{1, \mathrm{i}, -1, -\mathrm{i}\}$, l'ensemble des racines quatrièmes de l'unité. Plus généralement, l'ensemble $\mu_n = \left\{\mathrm{e}^{2\mathrm{i}k\pi/n} \;;\; 0 \leqslant k \leqslant n-1\right\}$ des racines n-ièmes de l'unité est un groupe cyclique d'ordre n, engendré par $\zeta = \mathrm{e}^{2\mathrm{i}\pi/n}$. Ce groupe jouera un rôle central au chapitre 7 : c'est lui qui gouverne le comportement des radicaux.

Exemple : Le groupe $\mathbb{Z}/12\mathbb{Z}$ est cyclique d'ordre 12, engendré par $\overline{1}$. L'élément $\overline{3}$ y est d'ordre 4, car $4 \times 3 = 12$ est le premier multiple de 3 divisible par 12 ; il engendre le sous-groupe $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$. Plus généralement l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ vaut $\frac{n}{\mathrm{pgcd}(n\,;k)}$, et $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier avec n.



Le **treillis** des sous-groupes de $\mathbb{Z}/12\mathbb{Z}$: un trait signifie « est contenu dans », et l'ordre de chaque sous-groupe est indiqué à côté. À chaque diviseur d de 12 correspond un unique sous-groupe d'ordre d, de sorte que la figure reproduit exactement le treillis des diviseurs de 12, renversé. Cette figure est le premier exemple d'un phénomène que le chapitre 6 généralisera considérablement : la correspondance de Galois associera, de la même manière, un treillis de sous-groupes à un treillis de corps intermédiaires.

1.3 Morphismes de groupes

Définition : Soient $(G\,;\cdot)$ et $(G'\,;*)$ deux groupes. Une application $f : G \to G'$ est un **morphisme de groupes** si :

$$\forall\, x, y \in G, \quad f(xy) = f(x) * f(y)$$

Un morphisme bijectif est un **isomorphisme** ; les groupes G et G' sont alors dits **isomorphes**, ce que l'on note $G \simeq G'$. Un morphisme de G dans lui-même est un **endomorphisme**, et un endomorphisme bijectif un **automorphisme**. L'ensemble des automorphismes de G, muni de la composition, est un groupe noté $\mathrm{Aut}(G)$.

Exemple : L'application $k \mapsto 2k$ de $(\mathbb{Z}\,;+)$ dans lui-même est un morphisme, puisque $2(k+\ell) = 2k+2\ell$; elle est injective mais non surjective. La projection $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto \overline{k}$, est un morphisme surjectif mais non injectif dès que $n \geqslant 2$.

La conjugaison complexe $z \mapsto \overline{z}$ est un automorphisme de $(\mathbb{C}\,;+)$ comme de $(\mathbb{C}^*\,;\times)$, puisqu'elle respecte somme et produit et qu'elle est son propre inverse. Enfin le déterminant $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ est un morphisme surjectif, car $\det(AB) = \det(A)\det(B)$.

Attention : l'application $x \mapsto x+1$ de $(\mathbb{Z}\,;+)$ dans lui-même est bijective mais n'est *pas* un morphisme, car elle envoie 0 sur 1 et non sur 0. Être bijectif ne suffit pas.

Propriété 1.7 : Soit $f : G \to G'$ un morphisme de groupes. Alors $f(e) = e'$, et $f\left(x^{-1}\right) = f(x)^{-1}$ pour tout $x \in G$. De plus $f\left(x^k\right) = f(x)^k$ pour tout $k \in \mathbb{Z}$.

∘ *Démonstration :* De l'égalité $e \cdot e = e$ dans G on tire $f(e) * f(e) = f(e) = f(e) * e'$, puis $f(e) = e'$ par régularité dans G'.

Soit maintenant $x \in G$. On a $f(x) * f\left(x^{-1}\right) = f\left(xx^{-1}\right) = f(e) = e'$, et de même dans l'autre sens ; par unicité de l'inverse, $f\left(x^{-1}\right) = f(x)^{-1}$. La dernière assertion, portant sur un entier $k \in \mathbb{Z}$ quelconque, s'obtient par récurrence sur k pour $k \geqslant 0$, puis en passant aux inverses pour $k < 0$. □

Définition : Soit $f : G \to G'$ un morphisme. On appelle **noyau** et **image** de f les ensembles :

$$\mathrm{Ker} f = \left\{x \in G \ ; \ f(x) = e'\right\} \qquad \text{et} \qquad \mathrm{Im} f = \left\{f(x) \ ; \ x \in G\right\}$$

Exemple : Reprenons les morphismes de l'exemple précédent. Pour $k \mapsto 2k$ de $\mathbb{Z}$ dans $\mathbb{Z}$, le noyau est $\{0\}$ et l'image est $2\mathbb{Z}$. Pour la projection $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, le noyau est $n\mathbb{Z}$ — ce sont exactement les entiers de classe nulle — et l'image est $\mathbb{Z}/n\mathbb{Z}$ tout entier. Pour le déterminant $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$, le noyau est le groupe spécial linéaire $\mathrm{SL}_n(\mathbb{R})$ des matrices de déterminant 1, et l'image est $\mathbb{R}^*$.

On observe déjà ce que la propriété suivante va établir : le noyau est réduit au neutre exactement dans le premier cas, qui est aussi le seul où le morphisme est injectif.

Propriété 1.8 : Soit $f : G \to G'$ un morphisme. Alors $\mathrm{Ker} f$ est un sous-groupe de G, $\mathrm{Im} f$ est un sous-groupe de G', et :

$$f \text{ est injectif} \iff \mathrm{Ker} f = \{e\}$$

∘ *Démonstration :* Soit $f : G \to G'$ un morphisme. Le noyau contient e d'après la propriété 1.7. Soient $x, y \in \mathrm{Ker} f$; alors :

$$f\left(xy^{-1}\right) = f(x) * f(y)^{-1} = e' * e'^{-1} = e'$$

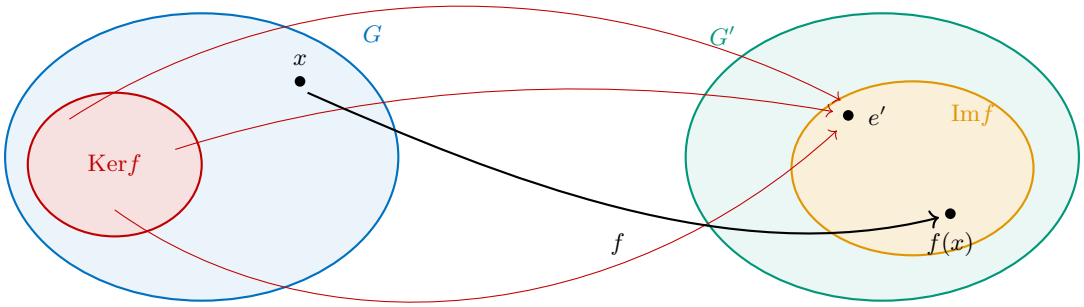
donc $xy^{-1} \in \mathrm{Ker} f$, qui est bien un sous-groupe. De même $e' = f(e) \in \mathrm{Im} f$, et pour $f(x), f(y) \in \mathrm{Im} f$ on a $f(x) * f(y)^{-1} = f\left(xy^{-1}\right) \in \mathrm{Im} f$.

Supposons f injective : si $x \in \mathrm{Ker} f$, alors $f(x) = e' = f(e)$, donc $x = e$; ainsi $\mathrm{Ker} f = \{e\}$. Réciproquement, supposons $\mathrm{Ker} f = \{e\}$ et soient x, y tels que $f(x) = f(y)$. Alors :

$$f\left(xy^{-1}\right) = f(x) * f(y)^{-1} = e'$$

donc $xy^{-1} \in \mathrm{Ker} f = \{e\}$, soit $xy^{-1} = e$, soit $x = y$. Donc f est injective. □

Remarque : Ce critère est d'une efficacité redoutable : pour établir l'injectivité d'un morphisme, on n'a jamais besoin de comparer deux antécédents, il suffit de résoudre une seule équation, $f(x) = e'$. C'est la traduction, au niveau des groupes, de la linéarité en algèbre linéaire, où l'on montre l'injectivité d'une application linéaire en calculant son noyau.



Les trois flèches rouges disent l'essentiel : le noyau tout entier s'écrase sur le neutre e', tandis que G se déverse sur l'image. Le chapitre suivant précisera cette image : elle est en bijection avec le quotient $G/\mathrm{Ker} f$, ce qui donnera le premier théorème d'isomorphisme.

Exemple : L'exponentielle $\exp : (\mathbb{R} ; +) \to (\mathbb{R}_+^* ; \times)$ est un morphisme, puisque $\mathrm{e}^{x+y} = \mathrm{e}^x \mathrm{e}^y$. Son noyau est $\{0\}$ et son image $\mathbb{R}_+^*$ tout entier : c'est un isomorphisme, de réciproque le logarithme népérien. Cet isomorphisme est ce qui rend les tables de logarithmes utiles : il transforme des produits en sommes.

Exemple : L'application $\varphi : (\mathbb{Z}\,;+) \to (\mathbb{C}^*\,;\times)$ définie par $\varphi(k) = \mathrm{e}^{2\mathrm{i}k\pi/n}$ est un morphisme d'image μ_n et de noyau $n\mathbb{Z}$. Il n'est ni injectif ni surjectif, mais il montre déjà que μ_n « ressemble » à $\mathbb{Z}$ privé de son excès : le chapitre 2 formalisera cette idée sous la forme $\mathbb{Z}/n\mathbb{Z} \simeq \mu_n$.

Propriété 1.9 : Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, et tout groupe monogène infini est isomorphe à $\mathbb{Z}$.

∘ *Démonstration :* Soit $G = \langle x\rangle$. L'application $\varphi : \mathbb{Z} \to G$, $k \mapsto x^k$, est un morphisme surjectif d'après la propriété 1.5. Son noyau est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ par le théorème 1.1.

Si $n = 0$, alors φ est injective par la propriété 1.8, donc bijective : $G \simeq \mathbb{Z}$, et G est infini. Si $n \geqslant 1$, alors x est d'ordre n et l'application $\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to G$, $\overline{k} \mapsto x^k$, est bien définie : si $\overline{k} = \overline{\ell}$, alors $k - \ell \in n\mathbb{Z} = \mathrm{Ker}\varphi$, donc $x^k = x^\ell$. C'est un morphisme, surjectif comme φ, et injectif car $x^k = e$ entraîne $k \in n\mathbb{Z}$, soit $\overline{k} = \overline{0}$. C'est donc un isomorphisme. □

Remarque : Ce résultat est le premier théorème de *classification* du cours : il dit qu'à isomorphisme près, il n'existe qu'un seul groupe cyclique de chaque ordre. Toute la difficulté de la théorie des groupes finis vient de ce que rien de tel ne vaut au-delà : il existe deux groupes d'ordre 4 (on l'a vu avec $\mathbb{Z}/4\mathbb{Z}$ et V), cinq d'ordre 8, et 49 487 365 422 groupes d'ordre 1024.

1.4 Le groupe symétrique

Définition : Pour $n \geqslant 1$, le **groupe symétrique** $\mathfrak{S}_n$ est le groupe des bijections de $[\![1\,;n]\!]$ dans lui-même, muni de la composition. Ses éléments sont appelés **permutations**. On les note :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Exemple : Le groupe $\mathfrak{S}_1$ est réduit à l'identité, et $\mathfrak{S}_2 = \{\mathrm{id}\,;\tau\}$ où τ échange 1 et 2 : il est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Le groupe $\mathfrak{S}_3$ compte six éléments, que la figure du paragraphe 1.1 a déjà fait apparaître comme les symétries du triangle. En voici deux :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \text{et} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

La composée $\sigma \circ \tau$ se lit de droite à gauche : τ envoie 1 sur 1, puis σ envoie 1 sur 2, donc $(\sigma \circ \tau)(1) = 2$; de même $(\sigma \circ \tau)(2) = \sigma(3) = 1$ et $(\sigma \circ \tau)(3) = \sigma(2) = 3$. Ainsi $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Propriété 1.10 : Le groupe $\mathfrak{S}_n$ est d'ordre $n!$. Il est abélien si et seulement si $n \leqslant 2$.

∘ *Démonstration :* Construire une bijection σ revient à choisir $\sigma(1)$ parmi n valeurs, puis $\sigma(2)$ parmi les $n-1$ restantes, et ainsi de suite : cela fait $n \times (n-1) \times \cdots \times 1 = n!$ choix, tous distincts et tous admissibles.

Pour $n \leqslant 2$, le groupe a au plus deux éléments et est donc abélien. Pour $n \geqslant 3$, considérons τ qui échange 1 et 2 en fixant le reste, et ρ qui échange 2 et 3 en fixant le reste. Alors :

$$(\tau \circ \rho)(1) = \tau(1) = 2 \qquad \text{tandis que} \qquad (\rho \circ \tau)(1) = \rho(2) = 3$$

Les deux composées diffèrent donc, et $\mathfrak{S}_n$ n'est pas abélien. □

Remarque : La composition se lit *de droite à gauche* : dans $\sigma \circ \tau$, c'est τ qui agit en premier. L'erreur la plus répandue dans les calculs de permutations est d'inverser cet ordre ; on la détecte en vérifiant un cas simple sur un seul élément, comme ci-dessus.

Définition : Le **support** d'une permutation σ est l'ensemble $\mathrm{supp}(\sigma) = \{i\ ;\ \sigma(i) \neq i\}$.

Soient $a_1, \ldots, a_k$ des éléments deux à deux distincts de $[\![1\,;n]\!]$ avec $k \geqslant 2$. Le **cycle** $(a_1\ a_2\ \cdots\ a_k)$ est la permutation qui envoie a_1 sur a_2, a_2 sur a_3, …, a_k sur a_1, et fixe tous les autres éléments. L'entier k est sa **longueur**. Un cycle de longueur 2 est une **transposition**.

Exemple : La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$ de $\mathfrak{S}_5$ fixe 2 et 4, donc son support est $\{1\,;3\,;5\}$. Elle envoie 1 sur 3, 3 sur 5 et 5 sur 1 : c'est le cycle (1 3 5), de longueur 3.

En revanche, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ a pour support $\{1\,;2\,;3\,;4\}$ tout entier, mais n'est pas un cycle : elle échange 1 et 2 d'une part, 3 et 4 d'autre part, sans jamais relier les deux paires. C'est le produit des deux transpositions (1 2) et (3 4), dont les supports sont disjoints. Toute permutation n'est donc pas un cycle — le théorème 1.2 dira qu'elle en est toujours un produit.

Propriété 1.11 : Un cycle de longueur k est d'ordre k dans $\mathfrak{S}_n$. Deux permutations à supports disjoints commutent.

∘ *Démonstration :* Soit $c = (a_1 \ \cdots \ a_k)$. Une récurrence immédiate donne $c^m(a_i) = a_{i+m}$, les indices étant pris modulo k dans $[\![1\,;k]\!]$. Ainsi $c^k = \mathrm{id}$, et pour $1 \leqslant m < k$ on a $c^m(a_1) = a_{1+m} \neq a_1$, donc $c^m \neq \mathrm{id}$. L'ordre de c vaut donc k.

Soient maintenant σ, τ de supports disjoints et $i \in [\![1\,;n]\!]$. Trois cas se présentent. Si $i \notin \mathrm{supp}(\sigma) \cup \mathrm{supp}(\tau)$, alors $\sigma(\tau(i)) = i = \tau(\sigma(i))$. Si $i \in \mathrm{supp}(\sigma)$, alors $i \notin \mathrm{supp}(\tau)$ donc $\tau(i) = i$ et $\sigma(\tau(i)) = \sigma(i)$; par ailleurs $\sigma(i) \in \mathrm{supp}(\sigma)$ — car si $\sigma(i)$ était fixe par σ, on aurait $\sigma(\sigma(i)) = \sigma(i)$, donc $\sigma(i) = i$ par injectivité, contredisant $i \in \mathrm{supp}(\sigma)$ — donc $\sigma(i) \notin \mathrm{supp}(\tau)$ et $\tau(\sigma(i)) = \sigma(i)$. Les deux composées coïncident en i. Le troisième cas, $i \in \mathrm{supp}(\tau)$, est symétrique. □

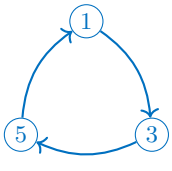
Théorème 1.2 : décomposition en cycles :
Toute permutation $\sigma \in \mathfrak{S}_n$ différente de l'identité s'écrit comme produit de cycles à supports deux à deux disjoints. Cette décomposition est unique à l'ordre des facteurs près.

∘ *Démonstration :* **Existence.** Considérons sur $[\![1\,;n]\!]$ la relation $i\mathcal{R}j$ définie par : il existe $m \in \mathbb{Z}$ tel que $j = \sigma^m(i)$. C'est une relation d'équivalence : elle est réflexive avec $m = 0$, symétrique en changeant m en $-m$, et transitive en additionnant les exposants. Ses classes d'équivalence, appelées **orbites** de σ, forment donc une partition de $[\![1\,;n]\!]$.

Soit O une orbite de cardinal $k \geqslant 2$ et $a \in O$. L'ensemble $\{m \in \mathbb{Z}\ ;\ \sigma^m(a) = a\}$ est un sous-groupe de $\mathbb{Z}$, donc égal à $d\mathbb{Z}$ pour un $d \geqslant 1$ — il est non nul car σ est d'ordre fini, $\mathfrak{S}_n$ étant fini. Les éléments $a, \sigma(a), \ldots, \sigma^{d-1}(a)$ sont alors deux à deux distincts et forment O tout entier, par le même raisonnement de division euclidienne qu'à la propriété 1.6 ; donc $d = k$. On associe à O le cycle $c_O = \big(a\ \sigma(a)\ \cdots\ \sigma^{k-1}(a)\big)$, dont le support est exactement O.

Notons $O_1, \ldots, O_r$ les orbites de cardinal au moins 2. Elles sont disjointes, donc les cycles $c_{O_1}, \ldots, c_{O_r}$ le sont aussi, et l'on vérifie que $\sigma = c_{O_1} \circ \cdots \circ c_{O_r}$: en effet, si i appartient à une orbite O_j de cardinal $\geqslant 2$, seul c_{O_j} le déplace et l'envoie sur $\sigma(i)$; et si i est dans une orbite réduite à un point, alors $\sigma(i) = i$ et aucun cycle ne le déplace.

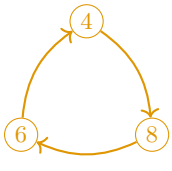
Unicité. Supposons $\sigma = c_1 \circ \cdots \circ c_s$ avec des cycles à supports disjoints. Le support de σ est la réunion des supports des c_j. Si $i \in \mathrm{supp}(c_j)$, alors $\sigma(i) = c_j(i)$, et par récurrence $\sigma^m(i) = c_j^m(i)$ pour tout m, puisque c_j stabilise son support. L'orbite de i sous σ est donc exactement $\mathrm{supp}(c_j)$, et c_j est déterminé par cette orbite. Les c_j sont donc les c_O construits plus haut, à l'ordre près. □



(1 3 5)



(2 7)



(4 8 6)

La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 8 & 1 & 4 & 2 & 6 \end{pmatrix}$ de $\mathfrak{S}_8$, décomposée en ses trois orbites non triviales. Chaque orbite est représentée par le cycle qu'elle porte, et les trois supports $\{1, 3, 5\}$, $\{2, 7\}$ et $\{4, 6, 8\}$ partitionnent bien $[\![1\,;8]\!]$. On lit directement $\sigma = (1\ 3\ 5)(2\ 7)(4\ 8\ 6)$.

Remarque : La décomposition en cycles disjoints donne immédiatement l'ordre d'une permutation : si $\sigma = c_1 \cdots c_r$ avec des cycles disjoints de longueurs $k_1, \ldots, k_r$, alors ces cycles commutent, donc $\sigma^m = c_1^m \cdots c_r^m$; et comme les supports sont disjoints, $\sigma^m = \mathrm{id}$ équivaut à $c_j^m = \mathrm{id}$ pour tout j, c'est-à-dire à $k_j \mid m$ pour tout j. Ainsi $o(\sigma) = \mathrm{ppcm}\,(k_1\,;\ldots\,;k_r)$. Pour la permutation ci-dessus, $o(\sigma) = \mathrm{ppcm}(3\,;2\,;3) = 6$.

Propriété 1.12 : Pour $n \geqslant 2$, les transpositions engendrent $\mathfrak{S}_n$: toute permutation est un produit de transpositions.

∘ *Démonstration :* D'après le théorème 1.2, il suffit de traiter le cas d'un cycle. Or on vérifie directement, en évaluant les deux membres sur chaque a_i, que :

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_k)\,(a_1\ a_{k-1})\cdots(a_1\ a_2)$$

Vérifions-le. Le membre de droite, appliqué à a_1, donne d'abord a_2 par la transposition la plus à droite, et a_2 n'est plus déplacé ensuite : on obtient a_2. Appliqué à a_i avec $2 \leqslant i \leqslant k-1$, il laisse a_i inchangé jusqu'à la transposition $(a_1\ a_i)$, qui l'envoie sur a_1, puis $(a_1\ a_{i+1})$ envoie a_1 sur a_{i+1}, qui n'est plus touché : on obtient a_{i+1}. Enfin a_k est envoyé sur a_1 par $(a_1\ a_k)$, qui est la dernière appliquée : on obtient a_1. C'est bien l'action du cycle.

L'identité, quant à elle, s'écrit (1 2)(1 2) dès que $n \geqslant 2$. □

Définition : On considère le polynôme à n indéterminées et on fait agir $\sigma \in \mathfrak{S}_n$ dessus en permutant les indices :

$$\Delta = \prod_{1\leqslant i<j\leqslant n} (X_j - X_i) \qquad \text{et} \qquad \sigma\cdot\Delta = \prod_{1\leqslant i<j\leqslant n} \left(X_{\sigma(j)} - X_{\sigma(i)}\right)$$

La **signature** de σ est l'unique élément $\varepsilon(\sigma) \in \{-1\,;1\}$ tel que $\sigma\cdot\Delta = \varepsilon(\sigma)\,\Delta$. La permutation σ est dite **paire** lorsque $\varepsilon(\sigma) = 1$, et **impaire** lorsque $\varepsilon(\sigma) = -1$.

Exemple : Prenons $n = 3$, de sorte que $\Delta = (X_2 - X_1)\,(X_3 - X_1)\,(X_3 - X_2)$.

Pour la transposition $\tau = (1\ 2)$, qui échange les indices 1 et 2 et fixe 3 :

$$\tau\cdot\Delta = (X_1 - X_2)\,(X_3 - X_2)\,(X_3 - X_1) = -\Delta$$

un seul facteur ayant changé de signe. Donc $\varepsilon(\tau) = -1$ et τ est impaire.

Pour le cycle $\sigma = (1\ 2\ 3)$, qui envoie 1 sur 2, 2 sur 3 et 3 sur 1 :

$$\sigma\cdot\Delta = (X_3 - X_2)\,(X_1 - X_2)\,(X_1 - X_3) = (X_3 - X_2)\times(-1)\,(X_2 - X_1)\times(-1)\,(X_3 - X_1) = \Delta$$

Deux facteurs ont changé de signe, qui se compensent : $\varepsilon(\sigma) = 1$ et σ est paire.

Théorème 1.3 : signature :
La signature est bien définie, et $\varepsilon : \mathfrak{S}_n \to (\{-1\,;1\}\,;\times)$ est un morphisme de groupes. Toute transposition est de signature -1 ; par conséquent, si σ s'écrit comme produit de p transpositions, alors $\varepsilon(\sigma) = (-1)^p$, et la parité de p ne dépend pas de la décomposition choisie.

∘ *Démonstration :* **Bonne définition.** Soit $\sigma \in \mathfrak{S}_n$. L'application $\{i\,;j\} \mapsto \{\sigma(i)\,;\sigma(j)\}$ est une bijection de l'ensemble des paires d'éléments distincts de $[\![1\,;n]\!]$ sur lui-même, car σ est bijective. Chaque facteur $\left(X_{\sigma(j)} - X_{\sigma(i)}\right)$ vaut donc, au signe près, un facteur $(X_\ell - X_k)$ avec $k < \ell$, et chacun de ces facteurs apparaît exactement une fois. Ainsi $\sigma\cdot\Delta = \pm\Delta$, le signe valant $(-1)^{I(\sigma)}$ où $I(\sigma)$ est le nombre de paires $\{i\,;j\}$ avec $i < j$ et $\sigma(i) > \sigma(j)$ — les **inversions** de σ.

Morphisme. Pour $\sigma, \tau \in \mathfrak{S}_n$, on calcule :

$$(\sigma\tau)\cdot\Delta = \prod_{i<j}\left(X_{\sigma(\tau(j))} - X_{\sigma(\tau(i))}\right) = \sigma\cdot\left(\prod_{i<j}\left(X_{\tau(j)} - X_{\tau(i)}\right)\right) = \sigma\cdot(\varepsilon(\tau)\Delta) = \varepsilon(\tau)\,\varepsilon(\sigma)\,\Delta$$

où l'avant-dernière égalité utilise que l'action de σ consiste à remplacer chaque indice k par $\sigma(k)$, opération qui laisse inchangé le scalaire $\varepsilon(\tau)$. D'où $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

Cas d'une transposition. Supposons $n \geqslant 2$ et traitons d'abord la transposition $\tau_0 = (1\ 2)$. Ses inversions sont les paires $\{i\,;j\}$, $i < j$, telles que $\tau_0(i) > \tau_0(j)$: seule la paire $\{1\,;2\}$ convient, car pour $j \geqslant 3$ les images sont inchangées et l'ordre est préservé. Donc $I(\tau_0) = 1$ et $\varepsilon(\tau_0) = -1$.

Soient maintenant $a, b \in [\![1\,;n]\!]$ distincts et $\tau = (a\ b)$ la transposition correspondante. Choisissons $\rho \in \mathfrak{S}_n$ telle que $\rho(1) = a$ et $\rho(2) = b$: une telle bijection existe puisque $a \neq b$. On vérifie que $\tau = \rho\,\tau_0\,\rho^{-1}$, en évaluant les deux membres sur a, sur b, et sur tout autre élément. Le morphisme ε étant à valeurs dans un groupe abélien :

$$\varepsilon(\tau) = \varepsilon(\rho)\,\varepsilon(\tau_0)\,\varepsilon(\rho)^{-1} = \varepsilon(\tau_0) = -1$$

Conclusion. Soit $\sigma \in \mathfrak{S}_n$. Si $\sigma = \tau_1\cdots\tau_p$ est un produit de p transpositions, alors $\varepsilon(\sigma) = (-1)^p$ par multiplicativité. Comme $\varepsilon(\sigma)$ ne dépend que de σ, la parité de p est la même pour toutes les décompositions. □

Définition : Le **groupe alterné** $\mathfrak{A}_n$ est le noyau de la signature : c'est l'ensemble des permutations **paires**. C'est un sous-groupe de $\mathfrak{S}_n$, d'ordre $\frac{n!}{2}$ pour $n \geqslant 2$.

∘ *Démonstration :* C'est un sous-groupe comme noyau d'un morphisme (propriété 1.8). Pour le cardinal, fixons $\tau = (1\ 2)$. L'application $\sigma \mapsto \tau\sigma$ est une bijection de $\mathfrak{A}_n$ sur l'ensemble des permutations impaires, de réciproque $\sigma \mapsto \tau\sigma$ elle-même. Les deux ensembles ont donc même cardinal, et leur réunion disjointe est $\mathfrak{S}_n$: chacun a $\frac{n!}{2}$ éléments. □

Remarque : Le polynôme Δ n'est pas un artifice de démonstration : son carré Δ^2, évalué aux racines d'un polynôme, est le **discriminant**, que nous retrouverons au chapitre 7. Le fait que Δ change de signe sous une transposition et que Δ^2 soit invariant est précisément ce qui permettra de reconnaître, sur le discriminant, si le groupe de Galois d'un polynôme est contenu dans le groupe alterné.

Exemple : Reprenons $\sigma = (1\ 3\ 5)(2\ 7)(4\ 8\ 6)$ de la figure précédente. Un cycle de longueur k s'écrit comme produit de $k-1$ transpositions, donc sa signature vaut $(-1)^{k-1}$. Ici :

$$\varepsilon(\sigma) = (-1)^2 \times (-1)^1 \times (-1)^2 = -1$$

La permutation σ est donc impaire : elle n'appartient pas à $\mathfrak{A}_8$. On retiendra la règle pratique : *un cycle de longueur paire est une permutation impaire*, ce qui déroute au premier abord mais se vérifie sur la transposition, cycle de longueur 2 et de signature -1.

1.5 Classes modulo un sous-groupe et théorème de Lagrange

Définition : Soient G un groupe et $H \leqslant G$. Pour $x \in G$, on appelle **classe à gauche** de x modulo H l'ensemble :

$$xH = \{xh\ ;\ h \in H\}$$

L'ensemble des classes à gauche est noté G/H. On définit de même les **classes à droite** Hx, dont l'ensemble est noté $H\backslash G$.

Exemple : Prenons $G = (\mathbb{Z}\,;+)$ et $H = n\mathbb{Z}$. La loi étant notée additivement, la classe à gauche de x s'écrit $x + n\mathbb{Z}$: c'est l'ensemble des entiers congrus à x modulo n. Il y a donc exactement n classes, celles de $0, 1, \ldots, n-1$, et l'on retrouve les classes de congruence.

Prenons maintenant $G = \mathfrak{S}_3$ et $H = \{\mathrm{id}\,;(1\ 2)\}$. Les trois classes à gauche sont :

$$H = \{\mathrm{id}\,;(1\ 2)\}, \qquad (1\ 3)H = \{(1\ 3)\,;(1\ 2\ 3)\}, \qquad (2\ 3)H = \{(2\ 3)\,;(1\ 3\ 2)\}$$

Elles comptent deux éléments chacune et recouvrent les six permutations sans se chevaucher. En revanche la classe à droite $H(1\ 3) = \{(1\ 3)\,;(1\ 3\ 2)\}$ diffère de $(1\ 3)H$: les deux partitions ne coïncident pas. C'est cette dissymétrie qui, au chapitre 2, distinguera les sous-groupes ordinaires des sous-groupes distingués.

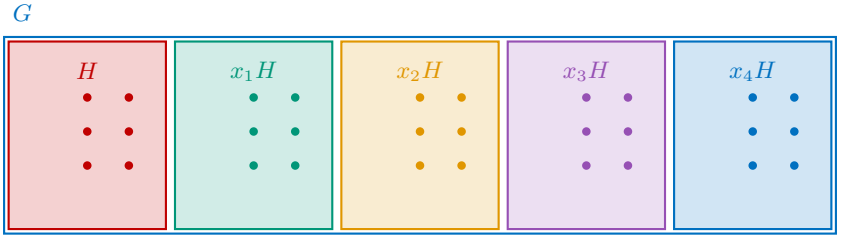
Propriété 1.13 : Soient G un groupe et $H \leqslant G$. La relation $x \sim y \iff x^{-1}y \in H$ est une relation d'équivalence sur G, dont les classes sont exactement les classes à gauche modulo H. En particulier, les classes à gauche forment une *partition* de G, et $xH = yH$ si et seulement si $x^{-1}y \in H$.

∘ *Démonstration :* Soient $x, y, z \in G$. **Réflexivité :** $x^{-1}x = e \in H$, donc $x \sim x$. **Symétrie :** si $x^{-1}y \in H$, alors son inverse $y^{-1}x$ appartient aussi à H, donc $y \sim x$. **Transitivité :** si $x^{-1}y \in H$ et $y^{-1}z \in H$, alors leur produit $\left(x^{-1}y\right)\left(y^{-1}z\right) = x^{-1}z$ est dans H, donc $x \sim z$.

Soit $x \in G$. Sa classe d'équivalence est $\left\{y \in G\ ;\ x^{-1}y \in H\right\}$. Or $x^{-1}y \in H$ équivaut à l'existence de $h \in H$ tel que $y = xh$, c'est-à-dire à $y \in xH$. La classe de x est donc xH. Les classes d'une relation d'équivalence formant une partition, il en va de même des classes à gauche. □

Propriété 1.14 : Soient G un groupe et $H \leqslant G$. Toutes les classes à gauche modulo H ont le même cardinal, à savoir $|H|$.

∘ *Démonstration :* Fixons $x \in G$ et considérons $\lambda_x : H \to xH$, $h \mapsto xh$. Elle est surjective par définition de xH, et injective par régularité : si $xh = xh'$, alors $h = h'$. C'est donc une bijection, et $|xH| = |H|$. □



G est la réunion disjointe de $[G:H] = 5$ classes, chacune de cardinal $|H| = 6$: ici $|G| = 30$

La figure dit tout du théorème de Lagrange : les classes à gauche pavent le groupe sans se recouvrir, et toutes ont la taille du sous-groupe. Le cardinal du groupe est donc le produit de deux entiers, celui du sous-groupe et celui du nombre de cases.

Théorème 1.4 : théorème de Lagrange :
Soit G un groupe fini et H un sous-groupe de G. Alors $|H|$ divise $|G|$, et plus précisément :

$$|G| = [G : H] \times |H|$$

où $[G : H]$, appelé **indice** de H dans G, désigne le nombre de classes à gauche modulo H.

∘ *Démonstration :* D'après la propriété 1.13, les classes à gauche modulo H forment une partition de G. Notons-les $x_1H, \ldots, x_rH$, deux à deux disjointes, avec $r = [G : H]$. Alors :

$$|G| = \sum_{k=1}^{r} |x_kH| = \sum_{k=1}^{r} |H| = r \times |H|$$

la deuxième égalité résultant de la propriété 1.14. Donc $|H|$ divise $|G|$ et le quotient vaut r. □

Propriété 1.15 : Soit G un groupe fini d'ordre n et $x \in G$. Alors :
- $o(x)$ divise n ;
- $x^n = e$;
- si n est un nombre premier, alors G est cyclique, et tout élément $\neq e$ en est un générateur.

∘ *Démonstration :* Soit $x \in G$. Le sous-groupe $\langle x \rangle$ a pour cardinal $o(x)$ d'après la propriété 1.6 ; le théorème de Lagrange donne donc $o(x) \mid n$. Écrivons $n = o(x) \times m$ avec $m \in \mathbb{N}^*$: alors $x^n = \left(x^{o(x)}\right)^m = e^m = e$.

Supposons enfin $n = p$ premier et soit $x \in G$ avec $x \neq e$. Alors $o(x)$ divise p et vaut 1 ou p ; comme $x \neq e$, on a $o(x) \neq 1$, donc $o(x) = p$ et $\langle x \rangle$ est un sous-groupe de cardinal $p = |G|$, donc égal à G. □

Remarque : La réciproque du théorème de Lagrange est *fausse* : ce n'est pas parce que d divise $|G|$ qu'il existe un sous-groupe d'ordre d. Le contre-exemple minimal est $\mathfrak{A}_4$, d'ordre 12, qui ne possède aucun sous-groupe d'ordre 6. On le vérifie ainsi : un tel sous-groupe H serait d'indice 2, donc distingué (propriété 2.2), et le quotient $\mathfrak{A}_4/H$ serait d'ordre 2 ; tout carré serait alors dans H. Or les huit 3-cycles de $\mathfrak{A}_4$ sont des carrés, puisque $c = \left(c^2\right)^2$ pour c d'ordre 3, ce qui donnerait $|H| \geqslant 9$. Contradiction.

Exemple : Appliquons la propriété 1.15 au groupe $G = ((\mathbb{Z}/p\mathbb{Z})^* ; \times)$ des classes inversibles modulo un nombre premier p, dont on verra au chapitre 3 qu'il est d'ordre $p - 1$. Pour tout entier a non divisible par p, on obtient $\overline{a}^{\,p-1} = \overline{1}$, c'est-à-dire :

$$a^{p-1} \equiv 1 \pmod{p}$$

C'est le *petit théorème de Fermat*, démontré ici sans le moindre calcul arithmétique : il n'est qu'un cas particulier du théorème de Lagrange. Pour $p = 7$ et $a = 3$, on vérifie que $3^6 = 729 = 104 \times 7 + 1$.

Remarque : Le théorème de Lagrange est un outil de *contrainte* : il ne construit rien, mais il interdit. C'est en ce sens qu'il servira dans tout le cours. Au chapitre 6, il dira par exemple qu'un corps intermédiaire entre K et une extension L de degré 8 ne peut avoir qu'un degré divisant 8 ; et au chapitre 7, c'est lui qui rendra impossible la construction du polygone régulier à sept côtés à la règle et au compas.

Chapitre 2

Quotients, actions et groupes résolubles

Le chapitre précédent a montré comment un sous-groupe découpe un groupe en classes. Il reste à munir l'ensemble de ces classes d'une structure de groupe — ce qui n'est pas toujours possible, et la condition d'obstruction porte un nom : la *distinction*. Ce chapitre construit les groupes quotients, en tire les théorèmes d'isomorphisme, puis introduit la notion qui donnera son sens à tout le cours : celle de **groupe résoluble**. Le résultat final — la non-résolubilité de $\mathfrak{S}_n$ pour $n \geqslant 5$ — est, à lui seul, la moitié du théorème d'Abel-Ruffini ; l'autre moitié sera fournie par la théorie des corps.

2.1 Sous-groupes distingués

Définition : Soit G un groupe. Un sous-groupe $H \leqslant G$ est dit **distingué** (ou *normal*) dans G si :

$$\forall\, g \in G, \quad gHg^{-1} = H \qquad \text{où} \qquad gHg^{-1} = \left\{ghg^{-1}\ ;\ h \in H\right\}$$

On note alors $H \trianglelefteq G$. L'élément ghg^{-1} est le **conjugué** de h par g.

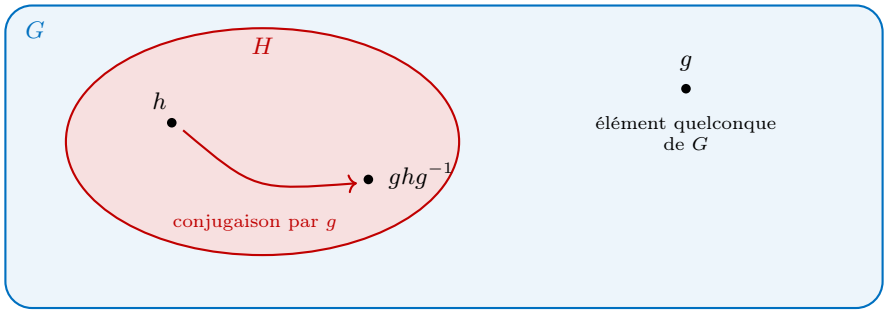
Propriété 2.1 : Soit $H \leqslant G$. Les assertions suivantes sont équivalentes :

- $H \trianglelefteq G$;
- pour tout $g \in G$, $gHg^{-1} \subseteq H$;
- pour tout $g \in G$, $gH = Hg$: les classes à gauche et à droite coïncident.

∘ *Démonstration :* Soient G un groupe et $H \leqslant G$. La première assertion entraîne évidemment la deuxième. Supposons la deuxième vérifiée et fixons $g \in G$; en l'appliquant à g^{-1}, on obtient $g^{-1}Hg \subseteq H$, d'où en multipliant à gauche par g et à droite par g^{-1} : $H \subseteq gHg^{-1}$. Avec l'inclusion inverse, on obtient $gHg^{-1} = H$, donc la première assertion.

Enfin, pour $g \in G$ fixé, l'égalité $gHg^{-1} = H$ équivaut, en multipliant à droite par g, à $gH = Hg$; les deuxième et troisième assertions sont donc équivalentes. □

Remarque : La troisième caractérisation est la plus parlante : un sous-groupe est distingué lorsque la partition en classes à gauche et la partition en classes à droite sont *la même*. C'est exactement ce dont on aura besoin pour définir une multiplication sur l'ensemble des classes. L'erreur la plus répandue est de croire que $ghg^{-1} = h$; la définition demande seulement que ghg^{-1} reste *dans* H, ce qui est bien plus faible.



Un sous-groupe distingué est un sous-groupe *stable par toutes les conjugaisons* : on peut le déplacer par n'importe quel élément du groupe sans en sortir. C'est cette rigidité qui permettra de quotienter.

Propriété 2.2 : Soit G un groupe.
- $\{e\}$ et G sont distingués dans G ; si G est abélien, tout sous-groupe est distingué.
- Le noyau de tout morphisme $f : G \to G'$ est distingué dans G.
- Tout sous-groupe d'indice 2 est distingué.

∘ *Démonstration :* Soit G un groupe. Les deux premiers points de la première assertion sont immédiats. Si G est abélien, alors pour tous $g \in G$ et $h \in H$ on a $ghg^{-1} = gg^{-1}h = h \in H$, donc tout sous-groupe H est distingué.

Pour le noyau : soit $f : G \to G'$ un morphisme, et soient $h \in \mathrm{Ker} f$ et $g \in G$. Alors $f\left(ghg^{-1}\right) = f(g)f(h)f(g)^{-1} = f(g)\,e'\,f(g)^{-1} = e'$, donc $ghg^{-1} \in \mathrm{Ker} f$.

Soient enfin $H \leqslant G$ d'indice 2 et $g \in G$. Si $g \in H$, alors $gH = H = Hg$. Sinon, les deux classes à gauche sont H et gH, qui forment une partition de G, donc $gH = G \setminus H$; de même $Hg = G \setminus H$. Dans les deux cas $gH = Hg$. □

Exemple : Le groupe alterné $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$, à double titre : c'est le noyau de la signature, et il est d'indice 2. En revanche, le sous-groupe $H = \{\mathrm{id}\,;(1\ 2)\}$ de $\mathfrak{S}_3$ n'est *pas* distingué : en conjuguant par $\sigma = (1\ 3)$, on obtient $\sigma(1\ 2)\sigma^{-1} = (3\ 2)$, qui n'appartient pas à H. C'est le plus petit contre-exemple, et il montre que la propriété d'être distingué dépend du groupe ambiant, pas seulement de H.

Propriété 2.3 (formule de conjugaison) : Soient $\sigma \in \mathfrak{S}_n$ et $c = (a_1\ a_2\ \cdots\ a_k)$ un cycle. Alors :

$$\sigma c \sigma^{-1} = (\sigma(a_1)\ \ \sigma(a_2)\ \ \cdots\ \ \sigma(a_k))$$

Par conséquent, deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont le même **type** — c'est-à-dire la même liste de longueurs de cycles.

∘ *Démonstration :* Posons $c' = (\sigma(a_1)\ \cdots\ \sigma(a_k))$ et montrons que les permutations $\sigma c \sigma^{-1}$ et c' coïncident en tout point $x \in [\![1\,;n]\!]$. Soit donc $x \in [\![1\,;n]\!]$.

Si $x = \sigma(a_i)$ pour un indice $i \in [\![1\,;k]\!]$, alors $\sigma c \sigma^{-1}(x) = \sigma(c(a_i)) = \sigma(a_{i+1})$ (indices modulo k), ce qui est bien $c'(x)$. Sinon, $\sigma^{-1}(x)$ n'est aucun des a_i, donc c le fixe et $\sigma c \sigma^{-1}(x) = x$; et c' fixe également x. D'où l'égalité.

Pour la seconde assertion, soient $\tau, \sigma \in \mathfrak{S}_n$: si $\sigma' = \sigma\tau\sigma^{-1}$ et si $\tau = c_1 \cdots c_r$ est la décomposition de τ en cycles disjoints, alors $\sigma' = \left(\sigma c_1 \sigma^{-1}\right) \cdots \left(\sigma c_r \sigma^{-1}\right)$, produit de cycles de mêmes longueurs et encore disjoints puisque σ est injective : σ' a le même type que τ. Réciproquement, soient $\tau, \tau' \in \mathfrak{S}_n$ de même type ; on les écrit en cycles disjoints de mêmes longueurs, en complétant par les points fixes, et l'on définit σ comme la bijection envoyant chaque symbole de l'écriture de τ sur celui qui lui correspond dans celle de τ' ; la formule ci-dessus donne alors $\sigma\tau\sigma^{-1} = \tau'$. □

Exemple : Dans $\mathfrak{S}_5$, les permutations $(1\ 2\ 3)(4\ 5)$ et $(2\ 5\ 1)(3\ 4)$ ont toutes deux le type $(3,2)$: elles sont donc conjuguées. Un conjugateur explicite s'obtient en superposant les deux écritures, ce qui donne $\sigma : 1 \mapsto 2,\ 2 \mapsto 5,\ 3 \mapsto 1,\ 4 \mapsto 3,\ 5 \mapsto 4$. Les classes de conjugaison de $\mathfrak{S}_5$ sont ainsi en bijection avec les partitions de 5, au nombre de sept.

2.2 Groupes quotients

Théorème 2.1 : groupe quotient :
Soit $H \trianglelefteq G$. Alors l'ensemble G/H des classes à gauche est muni d'une unique structure de groupe telle que la **projection canonique** $\pi : G \to G/H$, $g \mapsto gH$, soit un morphisme. Sa loi est :

$$(xH)\,(yH) = (xy)H$$

Le neutre est $H = eH$, l'inverse de xH est $x^{-1}H$, et π est un morphisme surjectif de noyau H.

∘ *Démonstration :* **La loi est bien définie.** C'est le seul point délicat, et c'est là qu'intervient l'hypothèse. Soient $x, x', y, y' \in G$ et supposons $xH = x'H$ et $yH = y'H$; il faut montrer $(xy)H = (x'y')\,H$, c'est-à-dire $(xy)^{-1}\,(x'y') \in H$. Par hypothèse, $x^{-1}x' = h_1 \in H$ et $y^{-1}y' = h_2 \in H$. Alors :

$$(xy)^{-1}\left(x'y'\right) = y^{-1}x^{-1}x'y' = y^{-1}h_1y' = y^{-1}h_1\,(yh_2) = \left(y^{-1}h_1y\right)h_2$$

Or $y^{-1}h_1y \in H$ puisque H est distingué, donc le produit est dans H. La loi est donc bien définie sur les classes.

C'est un groupe. Soient $x, y, z \in G$. L'associativité se lit sur les représentants :

$$\big((xH)(yH)\big)(zH) = (xyz)H = (xH)\big((yH)(zH)\big)$$

La classe $eH = H$ est neutre, car $(eH)(xH) = (ex)H = xH$, et l'on a $\left(x^{-1}H\right)(xH) = \left(x^{-1}x\right)H = H$ pour tout $x \in G$.

Projection. Pour tous $x, y \in G$, on a par construction $\pi(xy) = (xy)H = (xH)(yH) = \pi(x)\pi(y)$: π est un morphisme, visiblement surjectif. Son noyau est $\{x \in G\ ;\ xH = H\} = H$ d'après la propriété 1.13.

Unicité. Si $*$ est une autre loi rendant π morphisme, alors, pour tous $x, y \in G$, $xH * yH = \pi(x) * \pi(y) = \pi(xy) = (xy)H$: c'est la même loi. □

Remarque : On voit précisément *où* l'hypothèse « H distingué » est utilisée : à l'unique endroit où il a fallu faire traverser h_1 à travers y. Sans elle, la formule $(xH)(yH) = (xy)H$ dépendrait des représentants choisis et ne définirait rien. Réciproquement, on montre que si cette formule définit une loi, alors H est distingué : la condition n'est pas seulement suffisante, elle est nécessaire.

Exemple : Pour $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, distingué car $\mathbb{Z}$ est abélien, on retrouve exactement le groupe $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence. La notation quotient n'est donc pas une nouveauté : elle généralise le passage aux congruences.

Exemple : Prenons $G = \mathfrak{S}_3$ et $H = \mathfrak{A}_3 = \{\mathrm{id}\,;(1\ 2\ 3)\,;(1\ 3\ 2)\}$, distingué car d'indice 2. Le quotient $\mathfrak{S}_3/\mathfrak{A}_3$ a deux éléments, la classe des permutations paires et celle des impaires, et sa loi reproduit la règle des signes : pair × impair = impair. Ce quotient est donc isomorphe à $(\{-1\,;1\}\,;\times)$ — ce qui n'est pas un hasard, comme le théorème suivant va le montrer.

2.3 Théorèmes d'isomorphisme

Théorème 2.2 : premier théorème d'isomorphisme :
Soit $f : G \to G'$ un morphisme de groupes. Alors f induit un isomorphisme :

$$\overline{f} : G/\mathrm{Ker}f \xrightarrow{\sim} \mathrm{Im}f, \qquad \overline{f}\,(x\,\mathrm{Ker}f) = f(x)$$

En particulier, si G est fini, $|G| = |\mathrm{Ker}f| \times |\mathrm{Im}f|$.

∘ *Démonstration :* Posons $K = \mathrm{Ker}f$, distingué d'après la propriété 2.2, de sorte que G/K est un groupe.

$\overline{f}$ est bien définie. Soient $x, y \in G$ tels que $xK = yK$. Alors $x^{-1}y \in K$, donc $f\left(x^{-1}y\right) = e'$, soit $f(x)^{-1}f(y) = e'$, soit $f(x) = f(y)$. La valeur $\overline{f}(xK)$ ne dépend donc pas du représentant.

Morphisme. Pour tous $x, y \in G$, $\overline{f}\,((xK)(yK)) = \overline{f}((xy)K) = f(xy) = f(x)f(y) = \overline{f}(xK)\,\overline{f}(yK)$.

Injectivité. Soit $x \in G$ tel que $\overline{f}(xK) = e'$. Alors $f(x) = e'$, donc $x \in K$, donc $xK = K$: le noyau de $\overline{f}$ est réduit au neutre de G/K, et la propriété 1.8 conclut.

Surjectivité sur l'image. Tout élément de $\mathrm{Im}f$ s'écrit $f(x)$ pour un $x \in G$, c'est-à-dire $\overline{f}(xK)$.

Enfin, si G est fini, le théorème de Lagrange donne $|G| = [G : K] \times |K| = |G/K| \times |K| = |\mathrm{Im}f| \times |\mathrm{Ker}f|$. □

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow \\ G/\mathrm{Ker}f & \xrightarrow[\sim]{\ \overline{f}\ } & \mathrm{Im}f \end{array}$$

Le diagramme est *commutatif* : partir de G et descendre puis aller à droite et remonter donne le même résultat que d'aller directement à droite. Tout morphisme se factorise ainsi en une surjection suivie d'une injection, la partie intéressante étant l'isomorphisme central. C'est l'énoncé que l'on utilisera le plus dans ce cours.

Exemple : Le morphisme $\varphi : \mathbb{Z} \to \mathbb{C}^*$, $k \mapsto \mathrm{e}^{2\mathrm{i}k\pi/n}$, a pour noyau $n\mathbb{Z}$ et pour image μ_n. Le théorème donne aussitôt $\mathbb{Z}/n\mathbb{Z} \simeq \mu_n$, ce qui était annoncé au chapitre 1. De même, la signature $\varepsilon : \mathfrak{S}_n \to \{-1\,;1\}$ a pour noyau $\mathfrak{A}_n$ et est surjective pour $n \geqslant 2$, d'où $\mathfrak{S}_n/\mathfrak{A}_n \simeq \mathbb{Z}/2\mathbb{Z}$ et, en repassant aux cardinaux, $|\mathfrak{A}_n| = \frac{n!}{2}$ — la démonstration du chapitre 1 se trouve ainsi replacée dans son cadre naturel.

Théorème 2.3 : théorème de correspondance :
Soient G un groupe, $H \trianglelefteq G$ et $\pi : G \to G/H$ la projection canonique. Notons :

$$\mathscr{S}_H = \{K \ ; \ K \leqslant G \ \text{ et } \ H \subseteq K\} \qquad \text{et} \qquad \mathscr{S} = \left\{\overline{K} \ ; \ \overline{K} \leqslant G/H\right\}$$

c'est-à-dire l'ensemble des sous-groupes de G *qui contiennent* H, et l'ensemble de *tous* les sous-groupes du quotient. Alors les deux applications :

$$\Phi : \mathscr{S}_H \longrightarrow \mathscr{S}, \quad K \longmapsto \pi(K) = K/H \qquad \text{et} \qquad \Psi : \mathscr{S} \longrightarrow \mathscr{S}_H, \quad \overline{K} \longmapsto \pi^{-1}\left(\overline{K}\right)$$

sont bien définies et réciproques l'une de l'autre. Elles sont **croissantes**, au sens où, pour tous $K, K' \in \mathscr{S}_H$:

$$K \subseteq K' \iff \Phi(K) \subseteq \Phi\left(K'\right)$$

Enfin, pour tout $K \in \mathscr{S}_H$, on a $K \trianglelefteq G$ si et seulement si $\Phi(K) \trianglelefteq G/H$.

∘ *Démonstration :* **Les deux applications sont bien définies.** Soit $K \in \mathscr{S}_H$. Alors $\pi(K)$ est un sous-groupe de G/H, comme image d'un sous-groupe par un morphisme : $\Phi(K) \in \mathscr{S}$. Soit maintenant $\overline{K} \in \mathscr{S}$. Alors $\pi^{-1}\left(\overline{K}\right)$ est un sous-groupe de G, comme image réciproque d'un sous-groupe, et il contient $\pi^{-1}\left(\{\overline{e}\}\right) = \mathrm{Ker}\pi = H$: donc $\Psi\left(\overline{K}\right) \in \mathscr{S}_H$.

Elles sont réciproques l'une de l'autre. Soit $\overline{K} \in \mathscr{S}$. Comme π est surjective :

$$\Phi\left(\Psi\left(\overline{K}\right)\right) = \pi\left(\pi^{-1}\left(\overline{K}\right)\right) = \overline{K}$$

Soit réciproquement $K \in \mathscr{S}_H$. L'inclusion $K \subseteq \pi^{-1}(\pi(K)) = \Psi(\Phi(K))$ est toujours vraie. Pour l'inclusion inverse, soit $x \in \pi^{-1}(\pi(K))$: par définition, $\pi(x) \in \pi(K)$, donc il existe $k \in K$ tel que $xH = kH$, c'est-à-dire $k^{-1}x \in H$. Or $H \subseteq K$ par hypothèse, donc $k^{-1}x \in K$, et $x = k\left(k^{-1}x\right) \in K$. C'est ici, et seulement ici, que l'hypothèse $H \subseteq K$ intervient — sans elle, $\Psi(\Phi(K))$ serait le sous-groupe KH, strictement plus grand que K en général.

Croissance. Soient $K, K' \in \mathscr{S}_H$. Si $K \subseteq K'$, alors $\Phi(K) = \pi(K) \subseteq \pi\left(K'\right) = \Phi\left(K'\right)$, l'image directe préservant l'inclusion. Réciproquement, si $\Phi(K) \subseteq \Phi\left(K'\right)$, alors $\Psi(\Phi(K)) \subseteq \Psi\left(\Phi\left(K'\right)\right)$ — l'image réciproque préserve elle aussi l'inclusion —, c'est-à-dire $K \subseteq K'$ d'après le point précédent. Les deux ensembles ordonnés $(\mathscr{S}_H\,;\subseteq)$ et $(\mathscr{S}\,;\subseteq)$ sont donc isomorphes comme ensembles ordonnés.

Sous-groupes distingués. Soit $K \in \mathscr{S}_H$. Supposons $K \trianglelefteq G$ et soient $\overline{g} \in G/H$ et $\overline{k} \in \Phi(K)$; écrivons $\overline{g} = \pi(g)$ avec $g \in G$ et $\overline{k} = \pi(k)$ avec $k \in K$. Alors :

$$\overline{g}\,\overline{k}\,\overline{g}^{-1} = \pi\left(gkg^{-1}\right) \in \pi(K) = \Phi(K)$$

puisque $gkg^{-1} \in K$. Donc $\Phi(K) \trianglelefteq G/H$. Réciproquement, supposons $\Phi(K) \trianglelefteq G/H$ et soient $g \in G$ et $k \in K$. Alors $\pi\left(gkg^{-1}\right) = \pi(g)\pi(k)\pi(g)^{-1} \in \Phi(K)$, donc $gkg^{-1} \in \pi^{-1}(\Phi(K)) = \Psi(\Phi(K)) = K$. Donc $K \trianglelefteq G$. □

Remarque : Ce théorème est le premier exemple d'une *correspondance* entre deux familles d'objets ordonnées par l'inclusion. Le lecteur est invité à le garder en mémoire : le théorème fondamental de la théorie de Galois, au chapitre 6, aura exactement cette forme, à ceci près que la correspondance y reliera des corps à des groupes et qu'elle sera *décroissante* : elle renversera les inclusions au lieu de les préserver.

Exemple : Prenons $G = \mathbb{Z}$ et $H = 12\mathbb{Z}$. Les sous-groupes de $\mathbb{Z}$ contenant $12\mathbb{Z}$ sont les $d\mathbb{Z}$ pour $d \mid 12$, soit $d \in \{1, 2, 3, 4, 6, 12\}$; ils correspondent aux six sous-groupes de $\mathbb{Z}/12\mathbb{Z}$ représentés sur le treillis du chapitre 1. La correspondance est bien décroissante pour la divisibilité et croissante pour l'inclusion : $d\mathbb{Z} \subseteq d'\mathbb{Z}$ si et seulement si $d' \mid d$.

2.4 Actions de groupes

Définition : Une **action** d'un groupe G sur un ensemble X est une application $G \times X \to X$, notée $(g\,;x) \mapsto g \cdot x$, telle que $e \cdot x = x$ et $g \cdot (h \cdot x) = (gh) \cdot x$ pour tous $g, h \in G$ et $x \in X$.

L'**orbite** de x est $\mathcal{O}(x) = \{g \cdot x \ ; \ g \in G\}$, et son **stabilisateur** est $\mathrm{Stab}(x) = \{g \in G \ ; \ g \cdot x = x\}$. L'action est **transitive** s'il n'y a qu'une seule orbite.

Exemple : Le groupe $\mathfrak{S}_n$ agit sur $X = [\![1\,;n]\!]$ par $\sigma \cdot i = \sigma(i)$. L'action est transitive, car pour $i \neq j$ la transposition $(i\ j)$ envoie i sur j : il n'y a qu'une seule orbite, X tout entier. Le stabilisateur d'un point i est formé des permutations le fixant, c'est-à-dire des bijections de $X \setminus \{i\}$: il est isomorphe à $\mathfrak{S}_{n-1}$.

Tout groupe G agit aussi sur lui-même par translation à gauche, $g \cdot x = gx$. Cette action est transitive — l'équation $gx = y$ a toujours la solution $g = yx^{-1}$ — et tous les stabilisateurs sont réduits au neutre, puisque $gx = x$ entraîne $g = e$.

Enfin le groupe diédral D_4 des isométries du carré agit sur ses quatre sommets, sur ses quatre côtés, et sur l'ensemble des deux diagonales : une même action de groupe peut porter sur des ensembles très différents, et c'est ce choix qui en fait l'utilité.

Théorème 2.4 : orbite-stabilisateur :
Soient G un groupe agissant sur un ensemble X, et $x \in X$. Alors $\mathrm{Stab}(x)$ est un sous-groupe de G, et l'application $g\,\mathrm{Stab}(x) \mapsto g \cdot x$ est une bijection de $G/\mathrm{Stab}(x)$ sur $\mathcal{O}(x)$. En particulier, si G est fini :

$$|\mathcal{O}(x)| = \frac{|G|}{|\mathrm{Stab}(x)|}$$

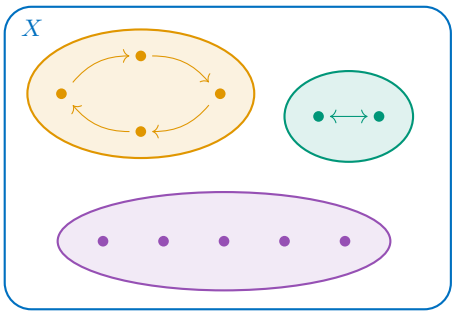
En particulier, *le cardinal de toute orbite divise l'ordre du groupe qui agit.*

∘ *Démonstration :* Soient $x \in X$ et $g, h \in G$. Le stabilisateur $\mathrm{Stab}(x)$ contient e, puisque $e \cdot x = x$. Supposons $g \cdot x = x$ et $h \cdot x = x$; alors $h^{-1} \cdot x = h^{-1} \cdot (h \cdot x) = \left(h^{-1}h\right) \cdot x = x$, puis $\left(gh^{-1}\right) \cdot x = g \cdot \left(h^{-1} \cdot x\right) = g \cdot x = x$: c'est un sous-groupe.

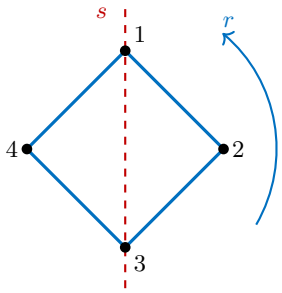
Notons $S = \mathrm{Stab}(x)$ et considérons l'application Φ définie sur G/S par $\Phi(gS) = g \cdot x$. Elle est bien définie et injective, car pour tous $g, g' \in G$:

$$gS = g'S \iff g^{-1}g' \in S \iff \left(g^{-1}g'\right) \cdot x = x \iff g' \cdot x = g \cdot x$$

la dernière équivalence s'obtenant en faisant agir g ou g^{-1}. Elle est surjective sur $\mathcal{O}(x)$ par définition de l'orbite. Ainsi $|\mathcal{O}(x)| = |G/S| = [G : S]$, et le théorème de Lagrange donne $[G : S] = \frac{|G|}{|S|}$, qui est bien un diviseur de $|G|$. □



les orbites partitionnent X



$\mathrm{Stab}(1) = \{\mathrm{id}\,; s\}$ *et* $|\mathcal{O}(1)| = 4 = 8/2$

À gauche, la situation générale : une action découpe X en orbites disjointes, à l'intérieur desquelles le groupe déplace les points, et qu'aucun élément du groupe ne permet de quitter. À droite, le groupe diédral D_4 d'ordre 8 agissant sur les quatre sommets d'un carré : l'action est transitive, il n'y a qu'une orbite de cardinal 4, et le stabilisateur du sommet 1 est formé de l'identité et de la réflexion s d'axe la diagonale $(1\,3)$. Le théorème 2.4 se lit sur la figure : $4 = \frac{8}{2}$.

Exemple : Faisons agir G sur lui-même par conjugaison, c'est-à-dire $g \cdot x = gxg^{-1}$. Les orbites sont les **classes de conjugaison**, et le stabilisateur de x est son **centralisateur** $C(x) = \{g \ ; \ gx = xg\}$. Le théorème donne alors : le nombre de conjugués de x vaut $\frac{|G|}{|C(x)|}$, et divise donc $|G|$.

Dans $\mathfrak{S}_5$, la classe de conjugaison des 5-cycles est de cardinal $\frac{5!}{5} = 24$: en effet un 5-cycle c commute exactement avec les puissances de lui-même, soit $|C(c)| = 5$. On vérifie ce compte directement : il y a $4! = 24$ manières d'écrire un 5-cycle sur $\{1, \ldots, 5\}$ à rotation près.

Définition : Soit G un groupe. Le **centre** de G est l'ensemble des éléments qui commutent avec *tous* les autres :

$$Z(G) = \{z \in G \ ; \ \forall g \in G, \ zg = gz\}$$

C'est l'intersection de tous les centralisateurs, donc un sous-groupe de G ; et il est distingué, car pour $z \in Z(G)$ et $g \in G$ on a $gzg^{-1} = zgg^{-1} = z \in Z(G)$.

Exemple : Un groupe G est abélien si et seulement si $Z(G) = G$: le centre mesure donc, comme le groupe dérivé du paragraphe suivant, le défaut de commutativité — mais par l'autre bout, en recensant les éléments qui commutent avec tout plutôt que les obstructions à commuter.

À l'opposé, $Z(\mathfrak{S}_n) = \{\mathrm{id}\}$ dès que $n \geqslant 3$. En effet, soit $\sigma \neq \mathrm{id}$; il existe a tel que $\sigma(a) = b \neq a$, et comme $n \geqslant 3$ on peut choisir $c \notin \{a\,; b\}$. Posons $\tau = (b\ c)$; alors :

$$(\sigma\tau)(a) = \sigma(a) = b \qquad \text{tandis que} \qquad (\tau\sigma)(a) = \tau(b) = c \neq b$$

donc σ ne commute pas avec τ et n'appartient pas au centre.

Entre ces deux extrêmes, le groupe diédral D_4 d'ordre 8 a pour centre $\left\{\mathrm{id}\,; r^2\right\}$, où r est la rotation d'un quart de tour : seule la rotation d'un demi-tour commute avec toutes les symétries du carré.

Remarque : **L'équation aux classes.** Faisons agir un groupe *fini* G sur lui-même par conjugaison. Les orbites sont les classes de conjugaison, et celle de x est réduite au seul point x exactement lorsque $gxg^{-1} = x$ pour tout g, c'est-à-dire lorsque $x \in Z(G)$. En regroupant d'un côté les orbites ponctuelles, qui sont au nombre de $|Z(G)|$, et de l'autre les orbites à plusieurs éléments :

$$|G| = |Z(G)| + \sum_{|\mathcal{O}|>1} |\mathcal{O}|$$

chaque terme de la somme étant un diviseur de $|G|$ strictement supérieur à 1, d'après le théorème 2.4. Cette égalité, appelée **équation aux classes**, nous servira deux fois : à la propriété 2.12 pour montrer qu'aucun groupe simple non abélien n'a un ordre inférieur à 60, et à la propriété 7.7 pour établir que tout p-groupe possède un centre non trivial.

Exemple : Faisons agir $\mathfrak{S}_n$ sur $[\![1\,;n]\!]$ de manière naturelle. L'action est transitive, et le stabilisateur d'un point i est isomorphe à $\mathfrak{S}_{n-1}$. La formule donne $n = \frac{n!}{(n-1)!}$, ce qui est rassurant. Cette action anodine deviendra essentielle au chapitre 7 : le groupe de Galois d'un polynôme agit sur ses racines, et l'*irréductibilité* du polynôme se traduira exactement par la *transitivité* de cette action.

Théorème 2.5 : théorème de Cauchy :
Soient G un groupe fini et p un nombre premier divisant $|G|$. Alors G possède un élément d'ordre p.

∘ *Démonstration :* Considérons l'ensemble :

$$X = \{(g_1, \dots, g_p) \in G^p \ ; \ g_1 g_2 \cdots g_p = e\}$$

Soit $(g_1, \dots, g_p) \in G^p$. Les $p-1$ premières coordonnées peuvent être choisies librement, la dernière étant alors imposée par $g_p = (g_1 \cdots g_{p-1})^{-1}$; donc $|X| = |G|^{p-1}$, qui est divisible par p.

Faisons agir $\mathbb{Z}/p\mathbb{Z}$ sur X par permutation circulaire, $\overline{1} \cdot (g_1, \dots, g_p) = (g_2, \dots, g_p, g_1)$. Cette action est bien définie : si $g_1 \cdots g_p = e$, alors :

$$g_2 \cdots g_p g_1 = g_1^{-1} (g_1 g_2 \cdots g_p) g_1 = g_1^{-1} e g_1 = e$$

Prenons bien garde au groupe qui agit : ce n'est pas G, mais le groupe $\mathbb{Z}/p\mathbb{Z}$, dont l'ordre vaut p. Le théorème 2.4, appliqué à cette action, affirme que le cardinal de toute orbite divise l'ordre du groupe agissant, c'est-à-dire divise p. Comme p est premier, chaque orbite a donc pour cardinal 1 ou p.

Les orbites partitionnant X, notons f le nombre de celles qui sont réduites à un point et k le nombre de celles qui ont p éléments. En sommant les cardinaux :

$$|X| = f \times 1 + k \times p = f + pk$$

Or p divise $|X|$ et divise pk : il divise donc f.

Or une orbite est réduite à un point exactement lorsque le p-uplet est constant, c'est-à-dire de la forme $(g, \dots, g)$ avec $g^p = e$. Comme $(e, \dots, e)$ en est un, on a $f \geqslant 1$, donc $f \geqslant p \geqslant 2$: il existe $g \neq e$ tel que $g^p = e$. Cet élément est d'ordre p, puisque son ordre divise p premier et n'est pas 1. □

Remarque : Ce théorème est une réciproque partielle du théorème de Lagrange : la remarque du chapitre 1 montrait qu'un diviseur quelconque de $|G|$ n'est pas nécessairement l'ordre d'un sous-groupe, mais un diviseur *premier* l'est toujours. Nous l'utiliserons au chapitre 7 pour repérer un cycle d'ordre 5 dans le groupe de Galois d'une équation du cinquième degré.

Théorème 2.6 : théorème de Sylow, existence :
Soit G un groupe fini d'ordre $p^a m$, où p est premier et ne divise pas m. Alors G possède un sous-groupe d'ordre p^a, appelé **p-sous-groupe de Sylow**.

∘ *Démonstration :* **Un lemme arithmétique :** le coefficient binomial $\binom{p^a m}{p^a}$ n'est pas divisible par p. Écrivons en effet, en posant $N = p^a m$ et $k = p^a$:

$$\binom{N}{k} = \prod_{j=0}^{k-1} \frac{N-j}{k-j}$$

Le facteur d'indice $j = 0$ vaut $\frac{N}{k} = m$, non divisible par p. Soit maintenant un indice j tel que $1 \leqslant j \leqslant p^a - 1$; écrivons $j = p^b u$ où $b \in \mathbb{N}$ et $u \in \mathbb{N}^*$ vérifient $p \nmid u$, ce qui force $b < a$. Alors :

$$N - j = p^b \left(p^{a-b} m - u\right) \qquad \text{et} \qquad k - j = p^b \left(p^{a-b} - u\right)$$

et dans les deux parenthèses le premier terme est divisible par p tandis que u ne l'est pas : ces parenthèses sont premières à p. Numérateur et dénominateur portent donc exactement la même puissance p^b, qui se simplifie. Au total, la valuation p-adique de $\binom{N}{k}$ est celle de m, c'est-à-dire nulle.

L'action. Soit Ω l'ensemble des parties de G de cardinal p^a, de sorte que $|\Omega| = \binom{p^a m}{p^a}$ n'est pas divisible par p. Faisons agir G sur Ω par translation à gauche, $g \cdot A = gA = \{ga \ ; \ a \in A\}$ — c'est bien une action, et gA a encore p^a éléments par régularité.

Ici encore, le groupe qui agit est G lui-même, d'ordre $p^a m$: le théorème 2.4 dit que le cardinal de chaque orbite divise $p^a m$. Les orbites partitionnent Ω ; si toutes avaient un cardinal divisible par p, il en irait de même de $|\Omega|$. Il existe donc une orbite $\mathcal{O}$ de cardinal non divisible par p. Choisissons $A \in \mathcal{O}$ et posons $H = \mathrm{Stab}(A) = \{g \in G \ ; \ gA = A\}$.

Conclusion. Le théorème 2.4 donne $|\mathcal{O}| = \frac{p^a m}{|H|}$. Comme p ne divise pas $|\mathcal{O}|$, la puissance p^a doit tout entière figurer au dénominateur : p^a divise $|H|$. Par ailleurs, fixons $a_0 \in A$; l'application $H \to A$, $h \mapsto h\,a_0$, est bien définie car $hA = A$, et injective par régularité. Donc $|H| \leqslant |A| = p^a$. Les deux inégalités donnent $|H| = p^a$. □

Remarque : Le théorème de Cauchy est le cas $a = 1$ de cet énoncé, à ceci près qu'il fournit un élément et non un sous-groupe — mais un sous-groupe d'ordre p est cyclique, donc engendré par un élément d'ordre p. L'existence ne fait que la moitié du travail : c'est le dénombrement des sous-groupes de Sylow, objet du théorème suivant, qui donne à cet outil sa force. Nous en tirerons le théorème de Wilson dès ce paragraphe, puis, au paragraphe 2.6, le fait que $\mathfrak{A}_5$ est d'ordre minimal parmi les groupes simples non abéliens ; le chapitre 7 s'en servira enfin pour démontrer le théorème fondamental de l'algèbre.

Définition : Soient G un groupe et $H \leqslant G$. Le **normalisateur** de H dans G est :

$$N_G(H) = \left\{ g \in G \ ; \ gHg^{-1} = H \right\}$$

C'est le stabilisateur de H pour l'action de G par conjugaison sur l'ensemble de ses sous-groupes ; c'est donc un sous-groupe de G d'après le théorème 2.4. Il contient H, et $H \trianglelefteq N_G(H)$: c'est le plus grand sous-groupe de G dans lequel H est distingué.

Exemple : Par construction, $N_G(H) = G$ si et seulement si H est distingué dans G : le normalisateur mesure exactement le défaut de distinction. Ainsi $N_{\mathfrak{S}_n}(\mathfrak{A}_n) = \mathfrak{S}_n$, puisque $\mathfrak{A}_n$ est distingué.

À l'opposé, prenons $G = \mathfrak{S}_3$ et $H = \{\mathrm{id} \, ; (1\ 2)\}$, qui n'est pas distingué. Le théorème 2.4 appliqué à l'action par conjugaison sur les sous-groupes donne $[G : N_G(H)]$ = nombre de conjugués de H. Or les conjugués de H sont les trois sous-groupes engendrés par une transposition, donc $[G : N_G(H)] = 3$ et $|N_G(H)| = 2$: le normalisateur est H lui-même, le plus petit possible.

Théorème 2.7 : théorèmes de Sylow, conjugaison et dénombrement :
Soit G un groupe fini d'ordre $p^a m$, où p est premier et ne divise pas m. Notons $\mathrm{Syl}_p(G)$ l'ensemble des p-sous-groupes de Sylow de G et $n_p = \left|\mathrm{Syl}_p(G)\right|$. Alors :

- tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow, et deux p-sous-groupes de Sylow sont toujours conjugués ;
- pour tout $P \in \mathrm{Syl}_p(G)$, on a $n_p = [G : N_G(P)]$, et :

$$n_p \mid m \qquad \text{et} \qquad n_p \equiv 1 \pmod{p}$$

∘ *Démonstration :* Fixons $P \in \mathrm{Syl}_p(G)$, ce que le théorème 2.6 autorise, et notons $X = G/P$ l'ensemble des classes à gauche modulo P, de cardinal $[G : P] = m$.

Premier point. Soit Q un p-sous-groupe de G, c'est-à-dire un sous-groupe dont l'ordre est une puissance de p. Faisons agir Q sur X par translation à gauche, $q \cdot (gP) = (qg)P$. Par le théorème 2.4, chaque orbite a pour cardinal un diviseur de $|Q|$, donc une puissance de p. Si toutes les orbites avaient un cardinal divisible par p, il en irait de même de $|X| = m$, ce qui est exclu. Il existe donc une orbite réduite à un point, c'est-à-dire une classe gP telle que :

$$\forall\, q \in Q, \quad qgP = gP \qquad \text{soit} \qquad g^{-1}Qg \subseteq P \qquad \text{soit} \qquad Q \subseteq gPg^{-1}$$

Ainsi Q est contenu dans le p-sous-groupe de Sylow gPg^{-1} — c'en est bien un, la conjugaison préservant le cardinal. Si de plus Q est lui-même de Sylow, alors $|Q| = p^a = \left|gPg^{-1}\right|$ et l'inclusion est une égalité : $Q = gPg^{-1}$. Deux p-sous-groupes de Sylow sont donc conjugués.

L'indice du normalisateur. Faisons maintenant agir G par conjugaison sur $\mathrm{Syl}_p(G)$ — l'action est bien définie, un conjugué d'un sous-groupe de Sylow en étant un. Le premier point dit exactement qu'elle est transitive : il n'y a qu'une orbite, de cardinal n_p. Le stabilisateur de P est $N_G(P)$, et le théorème 2.4 donne $n_p = [G : N_G(P)]$.

n_p divise m. Comme $P \subseteq N_G(P)$, le cardinal $|N_G(P)|$ est divisible par p^a. Écrivons $|N_G(P)| = p^a d$; alors :

$$n_p = \frac{|G|}{|N_G(P)|} = \frac{p^a m}{p^a d} = \frac{m}{d}$$

qui divise m.

$n_p \equiv 1 \pmod p$**.** Faisons cette fois agir le seul sous-groupe P par conjugaison sur $\mathrm{Syl}_p(G)$. Les orbites ont pour cardinal un diviseur de $|P| = p^a$, donc 1 ou un multiple de p. Il suffit donc de montrer qu'il y a exactement un point fixe.

Le sous-groupe P est évidemment fixe. Réciproquement, soit $Q \in \mathrm{Syl}_p(G)$ fixe, c'est-à-dire $xQx^{-1} = Q$ pour tout $x \in P$: cela signifie $P \subseteq N_G(Q)$. Posons $N = N_G(Q)$. Les sous-groupes P et Q sont deux p-sous-groupes de N d'ordre p^a, qui est la plus grande puissance de p divisant $|G|$ donc *a fortiori* $|N|$: ce sont deux p-sous-groupes de Sylow de N. Le premier point, appliqué au groupe N, fournit $x \in N$ tel que $P = xQx^{-1}$; or $Q \trianglelefteq N$, donc $xQx^{-1} = Q$ et $P = Q$.

L'unique point fixe étant P, on obtient $n_p = 1 +$ (somme de multiples de p), soit $n_p \equiv 1 \pmod p$. □

Propriété 2.4 (théorème de Wilson) : Pour tout nombre premier p :

$$(p-1)! \equiv -1 \pmod p$$

∘ *Démonstration :* Plaçons-nous dans $\mathfrak{S}_p$, d'ordre $p!$. Comme p est premier et qu'aucun des entiers $1, \dots, p-1$ n'est divisible par p, l'écriture $p! = p \times (p-1)!$ montre que la plus grande puissance de p divisant $|\mathfrak{S}_p|$ est p^1. Les p-sous-groupes de Sylow de $\mathfrak{S}_p$ sont donc d'ordre p : ils sont cycliques (propriété 1.15) et engendrés par un élément d'ordre p.

Les éléments d'ordre p de $\mathfrak{S}_p$ sont les p-cycles. Soit $\sigma \in \mathfrak{S}_p$ d'ordre p, de décomposition en cycles disjoints de longueurs $k_1, \dots, k_r$. Son ordre vaut $\mathrm{ppcm}\,(k_1\,; \dots\,; k_r) = p$ (chapitre 1), donc p divise ce ppcm et, p étant premier, l'une des longueurs vaut p. Comme il n'y a que p symboles en tout, ce cycle les épuise et il est seul : σ est un p-cycle.

Comptage. Il y a $(p-1)!$ cycles de longueur p dans $\mathfrak{S}_p$: en écrivant les p symboles dans un ordre quelconque on obtient $p!$ écritures, et chaque cycle est ainsi écrit p fois, une par choix du symbole de départ.

Chaque p-sous-groupe de Sylow contient $p-1$ éléments d'ordre p, à savoir ses générateurs. Deux tels sous-groupes distincts se coupent trivialement, leur intersection étant un sous-groupe propre d'un groupe d'ordre premier. Les $(p-1)!$ cycles se répartissent donc en paquets de $p-1$, un par sous-groupe :

$$n_p = \frac{(p-1)!}{p-1} = (p-2)!$$

Conclusion. Le théorème 2.7 donne $n_p \equiv 1 \pmod p$, soit $(p-2)! \equiv 1 \pmod p$. En multipliant par $p-1 \equiv -1$:

$$(p-1)! = (p-1) \times (p-2)! \equiv (-1) \times 1 = -1 \pmod p$$

□

Exemple : Pour $p = 7$, le comptage annonce $n_7 = 5! = 120$ sous-groupes de Sylow d'ordre 7 dans $\mathfrak{S}_7$, et l'on vérifie que $120 = 17 \times 7 + 1 \equiv 1 \pmod 7$. Le théorème de Wilson donne alors $6! = 720 = 102 \times 7 + 6 \equiv -1 \pmod 7$. Il est piquant qu'un énoncé d'arithmétique élémentaire s'obtienne ainsi par un dénombrement de sous-groupes ; c'est, en miniature, le mouvement que toute la théorie de Galois accomplira.

2.5 Groupes résolubles

Définition : Soit G un groupe. Le **commutateur** de x et y est $[x\,; y] = xyx^{-1}y^{-1}$. Le **groupe dérivé** $D(G)$ est le sous-groupe engendré par tous les commutateurs.

Exemple : Un groupe G est abélien si et seulement si $D(G) = \{e\}$: en effet $[x\,; y] = e$ équivaut à $xy = yx$.

Calculons $D(\mathfrak{S}_3)$. Le commutateur de $(1\ 2)$ et $(1\ 3)$ vaut, ces deux transpositions étant involutives :

$$[(1\ 2)\,; (1\ 3)] = (1\ 2)(1\ 3)(1\ 2)(1\ 3) = ((1\ 2)(1\ 3))^2 = (1\ 3\ 2)^2 = (1\ 2\ 3)$$

Le groupe dérivé contient donc un 3-cycle, donc le sous-groupe $\mathfrak{A}_3$ qu'il engendre. Réciproquement, le quotient $\mathfrak{S}_3/\mathfrak{A}_3$ est d'ordre 2 donc abélien, et la propriété suivante donnera $D(\mathfrak{S}_3) \subseteq \mathfrak{A}_3$. Ainsi $D(\mathfrak{S}_3) = \mathfrak{A}_3$. On montre plus généralement que $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour tout $n \geqslant 2$.

Propriété 2.5 : Soit G un groupe. Alors $D(G) \trianglelefteq G$, le quotient $G/D(G)$ est abélien, et pour tout $H \trianglelefteq G$:

$$G/H \text{ est abélien} \iff D(G) \subseteq H$$

∘ *Démonstration :* **Distinction.** Soient $g, x, y \in G$. On a $g[x\,;y]g^{-1} = \left[gxg^{-1}\,;gyg^{-1}\right]$, comme on le vérifie en développant :

$$g\,xyx^{-1}y^{-1}\,g^{-1} = \left(gxg^{-1}\right)\left(gyg^{-1}\right)\left(gx^{-1}g^{-1}\right)\left(gy^{-1}g^{-1}\right)$$

en insérant $g^{-1}g$ entre chaque facteur. Ainsi la conjugaison par g permute les commutateurs, donc laisse stable le sous-groupe qu'ils engendrent : $D(G) \trianglelefteq G$.

Le critère. Soit $H \trianglelefteq G$. Le quotient G/H est abélien si et seulement si $(xH)(yH) = (yH)(xH)$ pour tous $x, y \in G$, c'est-à-dire $(xy)H = (yx)H$, c'est-à-dire $(yx)^{-1}(xy) = x^{-1}y^{-1}xy \in H$. Comme x et y parcourent tout G, cela équivaut à ce que H contienne tous les commutateurs, donc le sous-groupe qu'ils engendrent : $D(G) \subseteq H$.

En appliquant ce critère à $H = D(G)$, on obtient que $G/D(G)$ est abélien. □

Remarque : Le groupe dérivé mesure le défaut de commutativité : $D(G) = \{e\}$ si et seulement si G est abélien. Et le quotient $G/D(G)$, appelé **abélianisé** de G, est le *plus grand* quotient abélien de G : tout autre s'obtient en quotientant encore davantage.

Définition : Un groupe G est **résoluble** s'il existe une chaîne finie de sous-groupes :

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G$$

telle que chaque quotient G_{i+1}/G_i soit abélien. Une telle chaîne est appelée **suite de résolubilité**.

Remarque : Attention : on demande seulement que G_i soit distingué dans G_{i+1}, pas dans G. La relation « être distingué dans » n'est d'ailleurs pas transitive, et c'est l'un des pièges classiques de la théorie des groupes : dans $\mathfrak{S}_4$, le sous-groupe $\{\mathrm{id}\,;(1\ 2)(3\ 4)\}$ est distingué dans le groupe de Klein V, lui-même distingué dans $\mathfrak{S}_4$, sans être distingué dans $\mathfrak{S}_4$.

Propriété 2.6 : Tout groupe abélien est résoluble. Tout groupe d'ordre premier est résoluble. Un groupe simple est résoluble si et seulement s'il est cyclique d'ordre premier.

∘ *Démonstration :* Si G est abélien, la chaîne $\{e\} \trianglelefteq G$ convient. Un groupe d'ordre premier est cyclique (propriété 1.15), donc abélien.

Rappelons qu'un groupe G est dit **simple** s'il est non trivial et si ses seuls sous-groupes distingués sont $\{e\}$ et G. Soit G simple et résoluble, et $\{e\} = G_0 \trianglelefteq \cdots \trianglelefteq G_r = G$ une suite de résolubilité que l'on peut supposer sans répétition. Alors G_{r-1} est distingué dans G et différent de G, donc $G_{r-1} = \{e\}$, et $G = G/G_{r-1}$ est abélien. Un groupe abélien simple n'a d'autre sous-groupe que $\{e\}$ et lui-même — tout sous-groupe y étant distingué — donc il est engendré par n'importe lequel de ses éléments non neutres, donc cyclique ; et son ordre ne peut avoir de diviseur strict, sans quoi la propriété 1.6 fournirait un sous-groupe propre. Il est donc d'ordre premier. La réciproque vient d'être établie. □

Théorème 2.8 : stabilité de la résolubilité :
Soient G un groupe et $H \trianglelefteq G$.

- Si G est résoluble, tout sous-groupe de G est résoluble, et tout quotient de G est résoluble.
- Réciproquement, si H et G/H sont résolubles, alors G est résoluble.

∘ *Démonstration :* **Sous-groupes.** Soit $\{e\} = G_0 \trianglelefteq \cdots \trianglelefteq G_r = G$ une suite de résolubilité et $K \leqslant G$. Posons $K_i = K \cap G_i$. Alors $K_i \trianglelefteq K_{i+1}$: pour $k \in K_{i+1}$ et $x \in K_i$, l'élément kxk^{-1} est dans K et dans G_i (car $G_i \trianglelefteq G_{i+1}$ et $k \in G_{i+1}$). De plus, l'application :

$$K_{i+1} \longrightarrow G_{i+1}/G_i, \qquad k \longmapsto k\,G_i$$

est un morphisme de noyau $K_{i+1} \cap G_i = K_i$. Par le théorème 2.2, K_{i+1}/K_i est isomorphe à un sous-groupe du groupe abélien G_{i+1}/G_i, donc est abélien. La chaîne des K_i est donc une suite de résolubilité de K.

Quotients. Soit $\pi : G \to G/H$ la projection et $\overline{G_i} = \pi(G_i)$. Comme π est surjective, $\overline{G_i} \trianglelefteq \overline{G_{i+1}}$: pour $\overline{k} = \pi(k)$ avec $k \in G_{i+1}$ et $\overline{x} = \pi(x)$ avec $x \in G_i$, on a $\overline{k}\,\overline{x}\,\overline{k}^{-1} = \pi\left(kxk^{-1}\right) \in \overline{G_i}$. Ensuite, l'application composée $G_{i+1} \to \overline{G_{i+1}} \to \overline{G_{i+1}}/\overline{G_i}$ est surjective et son noyau contient G_i, donc elle induit une surjection de G_{i+1}/G_i sur $\overline{G_{i+1}}/\overline{G_i}$. Un quotient de groupe abélien étant abélien, les $\overline{G_i}$ forment une suite de résolubilité de G/H.

Réciproque. Soit $\{e\} = H_0 \trianglelefteq \cdots \trianglelefteq H_s = H$ une suite de résolubilité de H, et $\{\overline{e}\} = \overline{Q_0} \trianglelefteq \cdots \trianglelefteq \overline{Q_t} = G/H$ une suite de résolubilité de G/H. Posons $Q_j = \pi^{-1}\left(\overline{Q_j}\right)$. Le théorème de correspondance assure que $Q_j \trianglelefteq Q_{j+1}$, et le premier théorème d'isomorphisme appliqué à la composée $Q_{j+1} \to \overline{Q_{j+1}} \to \overline{Q_{j+1}}/\overline{Q_j}$, qui est surjective de noyau Q_j, donne :

$$Q_{j+1}/Q_j \simeq \overline{Q_{j+1}}/\overline{Q_j} \quad \text{abélien}$$

Comme $Q_0 = \pi^{-1}(\{\overline{e}\}) = H$ et $Q_t = G$, la chaîne :

$$\{e\} = H_0 \trianglelefteq \cdots \trianglelefteq H_s = H = Q_0 \trianglelefteq Q_1 \trianglelefteq \cdots \trianglelefteq Q_t = G$$

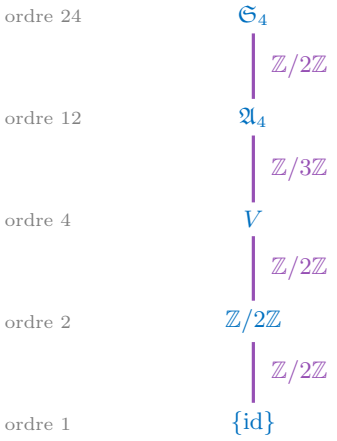
est une suite de résolubilité de G. □

Exemple : Le groupe $\mathfrak{S}_3$ est résoluble : la chaîne $\{\mathrm{id}\} \trianglelefteq \mathfrak{A}_3 \trianglelefteq \mathfrak{S}_3$ a pour quotients successifs $\mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ et $\mathfrak{S}_3/\mathfrak{A}_3 \simeq \mathbb{Z}/2\mathbb{Z}$, tous deux abéliens.

Exemple : Le groupe $\mathfrak{S}_4$ est résoluble. Posons $V = \{\mathrm{id}\,;(1\ 2)(3\ 4)\,;(1\ 3)(2\ 4)\,;(1\ 4)(2\ 3)\}$. C'est un sous-groupe : le produit de deux doubles transpositions distinctes de cette liste est la troisième, comme on le vérifie sur la table de Klein du chapitre 1. Il est distingué dans $\mathfrak{S}_4$ car la conjugaison préserve le type $(2,2)$ et que V contient *toutes* les permutations de ce type. La chaîne :

$$\{\mathrm{id}\} \trianglelefteq \mathbb{Z}/2\mathbb{Z} \trianglelefteq V \trianglelefteq \mathfrak{A}_4 \trianglelefteq \mathfrak{S}_4$$

où $\mathbb{Z}/2\mathbb{Z}$ désigne $\{\mathrm{id}\,;(1\ 2)(3\ 4)\}$, a pour quotients successifs des groupes d'ordres 2, 2, 3 et 2, tous premiers donc cycliques. Ainsi $\mathfrak{S}_4$ est résoluble.



À chaque étage, le quotient est cyclique d'ordre premier.

Le chapitre 7 lira cette chaîne comme la suite des extractions de racines qui résolvent l'équation du quatrième degré.

La suite de résolubilité de $\mathfrak{S}_4$, avec ses quotients à droite et les ordres à gauche. Le produit $2\times3\times2\times2 = 24$ des ordres des quotients redonne l'ordre du groupe, conformément au théorème de Lagrange appliqué à chaque étage.

2.6 Simplicité du groupe alterné

Ce paragraphe établit le résultat qui, au chapitre 7, interdira toute formule par radicaux au-delà du quatrième degré. Il est un peu plus long que les précédents, et nous le découpons en quatre lemmes.

Définition : Un groupe G est **simple** s'il n'est pas réduit au neutre et si ses seuls sous-groupes distingués sont $\{e\}$ et G.

Exemple : Pour p premier, le groupe $\mathbb{Z}/p\mathbb{Z}$ est simple : le théorème de Lagrange lui interdit tout sous-groupe autre que $\{\overline{0}\}$ et lui-même, distingué ou non. Ce sont là les seuls groupes simples abéliens, comme l'a montré la propriété 2.6.

En revanche $\mathbb{Z}/6\mathbb{Z}$ n'est pas simple : le sous-groupe $\{\overline{0}\,;\overline{3}\}$ est propre, non trivial, et distingué puisque le groupe est abélien. De même $\mathfrak{S}_3$ n'est pas simple, $\mathfrak{A}_3$ y étant distingué d'indice 2, ni $\mathfrak{S}_4$, qui contient le groupe de Klein V distingué. Le théorème 2.9 montrera que $\mathfrak{A}_5$, lui, est simple : c'est le premier groupe simple non abélien.

Propriété 2.7 (lemme 1) : Pour $n \geqslant 3$, le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles.

∘ *Démonstration :* Un 3-cycle est pair, donc appartient à $\mathfrak{A}_n$. Réciproquement, soit $\sigma \in \mathfrak{A}_n$. D'après le chapitre 1, σ est produit d'un nombre *pair* de transpositions ; groupons-les deux par deux et traitons chaque paire $\tau\tau'$. Si $\tau = \tau'$, le produit vaut id et disparaît. Si τ et τ' ont exactement un point commun, écrivons $\tau = (a\ b)$ et $\tau' = (a\ c)$ avec $a, b, c \in [\![1\,;n]\!]$ deux à deux distincts ; alors $\tau\tau' = (a\ c\ b)$, comme on le vérifie en évaluant en a, b et c. Si τ et τ' sont disjointes, écrivons $\tau = (a\ b)$ et $\tau' = (c\ d)$ avec a, b, c, d deux à deux distincts ; alors :

$$(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$$

ce que l'on vérifie point par point : le membre de droite envoie a sur c puis c sur b, soit $a \mapsto b$; il envoie b sur b puis b sur a, soit $b \mapsto a$; il envoie c sur d puis d sur d, soit $c \mapsto d$; et d sur a puis a sur c, soit $d \mapsto c$. C'est bien l'action de $(a\ b)(c\ d)$. □

Propriété 2.8 (lemme 2) : Pour $n \geqslant 5$, deux 3-cycles quelconques sont conjugués *dans* $\mathfrak{A}_n$.

∘ *Démonstration :* Soient $(a\ b\ c)$ et $(a'\ b'\ c')$ deux 3-cycles. Par la formule de conjugaison (propriété 2.3), il existe $\sigma \in \mathfrak{S}_n$ avec $\sigma(a) = a'$, $\sigma(b) = b'$, $\sigma(c) = c'$, et alors $\sigma(a\ b\ c)\sigma^{-1} = (a'\ b'\ c')$.

Si σ est paire, c'est terminé. Sinon, comme $n \geqslant 5$, choisissons deux éléments distincts $d, e \notin \{a\,;b\,;c\}$ et posons $\sigma' = \sigma\,(d\ e)$, qui est paire. La transposition $(d\ e)$ commute avec $(a\ b\ c)$, leurs supports étant disjoints, donc :

$$\sigma'(a\ b\ c)\sigma'^{-1} = \sigma\,(d\ e)(a\ b\ c)(d\ e)\,\sigma^{-1} = \sigma(a\ b\ c)\sigma^{-1} = \left(a'\ b'\ c'\right)$$

C'est ici que l'hypothèse $n \geqslant 5$ est indispensable : dans $\mathfrak{A}_4$, les 3-cycles (1 2 3) et (1 3 2) ne sont *pas* conjugués, faute de place pour corriger la parité. □

Propriété 2.9 (lemme 3) : Soit $n \geqslant 5$ et $N \trianglelefteq \mathfrak{A}_n$. Si N contient un 3-cycle, alors $N = \mathfrak{A}_n$.

∘ *Démonstration :* Soit $c \in N$ un 3-cycle et c' un 3-cycle quelconque. Par le lemme 2, il existe $\sigma \in \mathfrak{A}_n$ tel que $c' = \sigma c \sigma^{-1}$, et ce dernier appartient à N puisque N est distingué. Ainsi N contient tous les 3-cycles, donc le sous-groupe qu'ils engendrent, qui est $\mathfrak{A}_n$ par le lemme 1. □

Propriété 2.10 (lemme 4) : Soit $n \geqslant 5$ et $N \trianglelefteq \mathfrak{A}_n$ avec $N \neq \{\mathrm{id}\}$. Alors N contient un 3-cycle.

∘ *Démonstration :* Choisissons dans $N \setminus \{\mathrm{id}\}$ un élément σ dont le support est de cardinal minimal, et notons r ce cardinal. Comme σ est paire et distincte de l'identité, $r \neq 1$ et $r \neq 2$, donc $r \geqslant 3$. Nous allons montrer que $r = 3$, ce qui signifie précisément que σ est un 3-cycle.

L'outil est le suivant : pour tout 3-cycle $\tau = (x\ y\ z)$, l'élément $\rho = \sigma^{-1}\left(\tau\sigma\tau^{-1}\right)$ appartient à N, car $\tau\sigma\tau^{-1} \in N$ par distinction. En écrivant $\rho = \left(\sigma^{-1}\tau\sigma\right)\tau^{-1}$ et en appliquant la formule de conjugaison à σ^{-1} :

$$\rho = \left(\sigma^{-1}(x)\ \sigma^{-1}(y)\ \sigma^{-1}(z)\right)\ (x\ z\ y)$$

C'est un produit de deux 3-cycles : son support a au plus six éléments, et l'on va à chaque fois le rendre plus petit que r, contredisant la minimalité. Supposons donc $r \geqslant 4$ et examinons la décomposition de σ en cycles disjoints.

Cas 1 : σ possède un cycle de longueur $\ell \geqslant 4$. Écrivons ce cycle $(a_1\ a_2\ a_3\ a_4\ \cdots)$ et posons $b = \sigma^{-1}(a_1)$, dernier terme de ce cycle, de sorte que $b \notin \{a_1\,;a_2\,;a_3\}$ puisque $\ell \geqslant 4$. Prenons $\tau = (a_1\ a_2\ a_3)$; la formule donne :

$$\rho = (b\ a_1\ a_2)\,(a_1\ a_3\ a_2)$$

dont le support est contenu dans $\{b\,;a_1\,;a_2\,;a_3\}$, de cardinal au plus 4. De plus $\rho \neq \mathrm{id}$, car $\rho(a_3) = b \neq a_3$. Or σ est paire : si $\ell = 4$, le cycle seul serait impair et σ possède donc un autre cycle, d'où $r \geqslant 6$; et si $\ell \geqslant 5$, alors $r \geqslant 5$. Dans tous les cas $r \geqslant 5 > 4$, ce qui contredit la minimalité.

Cas 2 : tous les cycles de σ sont de longueur $\leqslant 3$ et au moins deux sont de longueur 3. Écrivons $\sigma = (a_1\ a_2\ a_3)\,(a_4\ a_5\ a_6)\cdots$, de sorte que $r \geqslant 6$. Avec $\tau = (a_1\ a_2\ a_4)$, on a $\sigma^{-1}(a_1) = a_3$, $\sigma^{-1}(a_2) = a_1$ et $\sigma^{-1}(a_4) = a_6$, donc :

$$\rho = (a_3\ a_1\ a_6)\,(a_1\ a_4\ a_2)$$

de support contenu dans $\{a_1\,;a_2\,;a_3\,;a_4\,;a_6\}$, de cardinal au plus $5 < 6 \leqslant r$. Et $\rho \neq \mathrm{id}$ puisque $\rho(a_2) = a_6 \neq a_2$. Contradiction.

Cas 3 : σ possède exactement un cycle de longueur 3, les autres étant des transpositions. Écrivons $\sigma = (a_1\ a_2\ a_3)\,t_1\cdots t_m$ avec $m \geqslant 1$, d'où $r = 3 + 2m \geqslant 5$. Les facteurs étant disjoints, ils commutent, et :

$$\sigma^2 = (a_1\ a_2\ a_3)^2\,t_1^2\cdots t_m^2 = (a_1\ a_3\ a_2)$$

qui appartient à N, est distinct de l'identité et a un support de cardinal $3 < r$. Contradiction.

Cas 4 : tous les cycles de σ sont des transpositions. Écrivons $\sigma = (a_1\ a_2)\,(a_3\ a_4)\cdots$, avec r pair, $r \geqslant 4$. Prenons $\tau = (a_1\ a_2\ a_3)$; alors $\sigma^{-1}(a_1) = a_2$, $\sigma^{-1}(a_2) = a_1$, $\sigma^{-1}(a_3) = a_4$, et :

$$\rho = (a_2\ a_1\ a_4)\,(a_1\ a_3\ a_2) = (a_1\ a_3)\,(a_2\ a_4)$$

la dernière égalité s'obtenant en évaluant les deux membres sur a_1, a_2, a_3, a_4. Le support de ρ a quatre éléments ; si $r > 4$, c'est une contradiction.

Reste le cas $r = 4$, où $\sigma = (a_1\ a_2)\,(a_3\ a_4)$ exactement. Comme $n \geqslant 5$, choisissons a_5 hors de $\{a_1\,;a_2\,;a_3\,;a_4\}$ et posons $\gamma = (a_4\ a_5)\,(a_1\ a_2) \in \mathfrak{A}_n$. La formule de conjugaison donne :

$$w = \gamma\sigma\gamma^{-1} = (\gamma\,(a_1)\ \ \gamma\,(a_2))\,(\gamma\,(a_3)\ \ \gamma\,(a_4)) = (a_2\ a_1)\,(a_3\ a_5) = (a_1\ a_2)\,(a_3\ a_5)$$

qui appartient à N. Le produit σw est alors dans N, et comme $(a_1\ a_2)$ commute avec les autres facteurs et est involutive :

$$\sigma w = (a_3\ a_4)\,(a_3\ a_5) = (a_3\ a_5\ a_4)$$

On obtient un 3-cycle dans N, de support de cardinal $3 < 4 = r$: contradiction encore.

Tous les cas sont contradictoires, donc $r = 3$ et σ est un 3-cycle appartenant à N. □

Théorème 2.9 : simplicité du groupe alterné :
Pour tout $n \geqslant 5$, le groupe $\mathfrak{A}_n$ est simple.

∘ *Démonstration :* Le groupe $\mathfrak{A}_n$ n'est pas réduit à l'identité. Soit $N \trianglelefteq \mathfrak{A}_n$ avec $N \neq \{\mathrm{id}\}$. Le lemme 4 assure que N contient un 3-cycle, et le lemme 3 en déduit $N = \mathfrak{A}_n$. □

Théorème 2.10 : non-résolubilité :
Pour tout $n \geqslant 5$, les groupes $\mathfrak{A}_n$ et $\mathfrak{S}_n$ ne sont pas résolubles.

∘ *Démonstration :* Le groupe $\mathfrak{A}_n$ est simple pour $n \geqslant 5$, d'ordre $\frac{n!}{2} \geqslant 60$. S'il était résoluble, la propriété 2.6 le rendrait cyclique d'ordre premier ; or 60, 360, … ne sont pas premiers, et plus directement $\mathfrak{A}_n$ n'est pas abélien pour $n \geqslant 4$, puisque $(1\ 2\ 3)(1\ 2\ 4) = (1\ 3)(2\ 4)$ tandis que $(1\ 2\ 4)(1\ 2\ 3) = (1\ 4)(2\ 3)$. Donc $\mathfrak{A}_n$ n'est pas résoluble.

Si $\mathfrak{S}_n$ était résoluble, le théorème 2.8 rendrait résoluble son sous-groupe $\mathfrak{A}_n$: contradiction. □

Remarque : La frontière est nette et mérite d'être soulignée : $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$ et $\mathfrak{S}_4$ sont résolubles, $\mathfrak{S}_n$ ne l'est plus dès $n = 5$. C'est exactement la frontière que l'on observe pour les équations : formules de résolution jusqu'au degré 4, aucune au-delà. La coïncidence n'en est pas une, et l'établir est l'objet du chapitre 7. Il reste à construire le pont : c'est le rôle des quatre chapitres qui suivent.

Remarque : **Une démonstration plus courte pour $\mathfrak{A}_5$.** Le cas $n = 5$ se traite plus rapidement par un comptage, qui repose sur le théorème orbite-stabilisateur appliqué à la conjugaison. Le stabilisateur d'un élément x y est son centralisateur $C(x)$, et sa classe de conjugaison a pour cardinal $\frac{|G|}{|C(x)|}$.

Dans $\mathfrak{A}_5$, d'ordre 60, on obtient ainsi cinq classes. Le centralisateur de $(1\ 2)(3\ 4)$ dans $\mathfrak{S}_5$ est engendré par $(1\ 2)$, $(3\ 4)$ et $(1\ 3)(2\ 4)$, d'ordre 8 ; son intersection avec $\mathfrak{A}_5$ est d'ordre 4, d'où une classe de 15 éléments — les quinze doubles transpositions. Le centralisateur de $(1\ 2\ 3)$ dans $\mathfrak{S}_5$ est engendré par $(1\ 2\ 3)$ et $(4\ 5)$, d'ordre 6, et vaut $\langle(1\ 2\ 3)\rangle$ dans $\mathfrak{A}_5$: la classe compte 20 éléments, soit tous les 3-cycles. Enfin un 5-cycle c ne commute qu'avec ses propres puissances, d'où $|C(c)| = 5$ et une classe de 12 éléments ; comme il y a 24 cycles de longueur 5, ceux-ci se répartissent en *deux* classes de 12. Le compte est bon :

$$60 = 1 + 15 + 20 + 12 + 12$$

Un sous-groupe distingué est une réunion de classes de conjugaison contenant le neutre, et son cardinal divise 60. Or aucune somme partielle contenant le terme 1 ne divise 60, hormis 1 et le total : les valeurs possibles sont 1, 16, 21, 13, 25, 36, 28, 33, 40, 45, 48 et 60. Donc $\mathfrak{A}_5$ est simple.

Ce raccourci est réel, mais il ne s'étend pas. Il repose sur une table de classes que l'on ne sait dresser explicitement que pour un groupe donné, et le passage de $\mathfrak{A}_5$ à $\mathfrak{A}_n$ exige alors une récurrence dont l'étape délicate — trouver dans un sous-groupe distingué un élément non trivial admettant un point fixe — se démontre par les mêmes calculs de commutateurs $\sigma^{-1}\tau\sigma\tau^{-1}$ que ceux du lemme 4. Le théorème de Sylow, quant à lui, offre une variante du comptage ci-dessus pour $\mathfrak{A}_5$, mais n'apporte rien pour $n \geqslant 6$. C'est pourquoi nous avons préféré la démonstration par support minimal, qui traite tous les n d'un seul mouvement et n'exige aucune connaissance préalable du groupe.

Il reste à justifier une affirmation qui circule souvent sans preuve : $\mathfrak{A}_5$ est le *plus petit* groupe simple non abélien. C'est ici que le dénombrement de Sylow devient indispensable, car il s'agit d'exclure cinquante-huit ordres d'un coup, sans rien connaître des groupes concernés sinon leur cardinal. Un lemme préliminaire est nécessaire.

Propriété 2.11 (lemme de plongement) : Soit G un groupe simple et $H \leqslant G$ un sous-groupe d'indice $k \geqslant 2$. Alors G est isomorphe à un sous-groupe de $\mathfrak{S}_k$; en particulier $|G|$ divise $k!$.

∘ *Démonstration :* Faisons agir G sur l'ensemble G/H des classes à gauche, de cardinal k, par translation : $g \cdot (xH) = (gx)H$. En numérotant ces k classes, on obtient un morphisme de groupes $\varphi : G \to \mathfrak{S}_k$.

Son noyau est distingué dans G. Il est de plus contenu dans H : si $g \in \mathrm{Ker}\varphi$, alors en particulier $g \cdot H = H$, c'est-à-dire $gH = H$, donc $g \in H$. Comme $H \neq G$ — l'indice vaut au moins 2 —, le noyau est différent de G ; la simplicité impose donc $\mathrm{Ker}\varphi = \{e\}$.

Ainsi φ est injectif et $G \simeq \varphi(G) \leqslant \mathfrak{S}_k$. Le théorème de Lagrange donne alors $|G| \mid k!$. □

Propriété 2.12 : Il n'existe aucun groupe simple non abélien d'ordre strictement inférieur à 60. Le groupe $\mathfrak{A}_5$ est donc d'ordre minimal parmi les groupes simples non abéliens.

∘ *Démonstration :* Soit G un groupe simple non abélien et $n = |G|$, et supposons $n < 60$; nous allons aboutir à une contradiction.

Étape 1 : n n'est pas premier. Un groupe d'ordre premier est cyclique (propriété 1.15), donc abélien.

Étape 2 : n n'est pas de la forme p^a avec $a \geqslant 2$. Supposons-le et écrivons l'équation aux classes du paragraphe 2.4 :

$$p^a = |Z(G)| + \sum_{|\mathcal{O}|>1} |\mathcal{O}|$$

Chaque terme de la somme est une puissance de p strictement supérieure à 1, donc divisible par p ; il en va de même de p^a, donc p divise $|Z(G)|$ et $Z(G) \neq \{e\}$. Or $Z(G) \trianglelefteq G$ — la conjugaison y agit trivialement —, donc $Z(G) = G$ par simplicité, et G est abélien : contradiction.

Étape 3 : une contrainte sur les facteurs premiers. L'entier n possède donc au moins deux facteurs premiers distincts. Soient p l'un d'eux, a son exposant, $m = n/p^a$, et P un p-sous-groupe de Sylow. Si l'on avait $n_p = 1$, alors P serait son propre unique conjugué, donc distingué (théorème 2.7) ; or $P \neq \{e\}$ puisque $p \mid n$, et $P \neq G$ puisque n n'est pas une puissance de p : cela contredirait la simplicité. Donc $n_p > 1$, et le théorème 2.7 donne $n_p \equiv 1 \pmod p$, d'où $n_p \geqslant p+1$, ainsi que $n_p \mid m$, d'où $m \geqslant n_p$. En résumé :

$$\text{pour tout diviseur premier } p \text{ de } n, \qquad m = \frac{n}{p^a} \geqslant p+1$$

Étape 4 : il ne reste que huit valeurs possibles. Appliquons l'étape 3 au *plus grand* facteur premier p de n. Tous les facteurs premiers de m sont alors strictement inférieurs à p, et l'on a $p^a(p+1) \leqslant p^a m = n \leqslant 59$.

- $p = 2$ est exclu : m serait alors sans facteur premier, donc $m = 1 < 3$.
- $p = 3$: m est une puissance de 2 vérifiant $m \geqslant 4$, et $3^a m \leqslant 59$. Les couples possibles sont $(1\,;4)$, $(1\,;8)$, $(1\,;16)$ et $(2\,;4)$, soit $n \in \{12\,;24\,;48\,;36\}$.
- $p = 5$: $m \geqslant 6$ n'a que 2 et 3 pour facteurs premiers, et $5^a m \leqslant 59$ impose $a = 1$ puis $m \leqslant 11$, donc $m \in \{6\,;8\,;9\}$ et $n \in \{30\,;40\,;45\}$.
- $p = 7$: $m \geqslant 8$ et $7^a m \leqslant 59$ imposent $a = 1$ et $m = 8$, soit $n = 56$.
- $p \geqslant 11$: il faudrait $m \geqslant 12$ et $pm \leqslant 59$, ce qui est impossible.

Restent donc $n \in \{12\,;24\,;30\,;36\,;40\,;45\,;48\,;56\}$.

Étape 5 : élimination des huit cas.

• $n \in \{12\,;24\,;48\}$. Ici $m = 3$ pour $p = 2$, donc n_2 divise 3 et vaut 1 ou 3 ; l'étape 3 donne $n_2 = 3$. Le normalisateur $N_G(P)$ est alors d'indice 3, et le lemme de plongement impose que n divise $3! = 6$: impossible pour $n \geqslant 12$.

• $n = 36$. Pour $p = 3$, on a $m = 4$, donc n_3 divise 4 et vaut 1 (mod 3) : les candidats sont 1 et 4, d'où $n_3 = 4$. Le normalisateur est d'indice 4 et 36 devrait diviser $4! = 24$: impossible.

• $n = 40$. Pour $p = 5$, on a $m = 8$. Les diviseurs de 8 sont $1, 2, 4, 8$, et aucun sauf 1 n'est congru à 1 modulo 5. Donc $n_5 = 1$, ce que l'étape 3 interdit.

• $n = 45$. Pour $p = 3$, on a $m = 5$, de diviseurs 1 et 5 ; or $5 \equiv 2 \pmod 3$. Donc $n_3 = 1$: même contradiction.

• $n = 30$. Pour $p = 5$, $m = 6$ et $n_5 \in \{1\,;6\}$, donc $n_5 = 6$. Pour $p = 3$, $m = 10$ et $n_3 \in \{1\,;10\}$, donc $n_3 = 10$. Deux sous-groupes distincts d'ordre premier se coupent trivialement, leur intersection étant un sous-groupe propre de chacun. Le groupe G contiendrait donc $6 \times 4 = 24$ éléments d'ordre 5 et $10 \times 2 = 20$ éléments d'ordre 3, soit 44 éléments distincts du neutre, alors qu'il n'en compte que 29 : impossible.

• $n = 56$. Pour $p = 7$, $m = 8$ et $n_7 \in \{1\,;8\}$, donc $n_7 = 8$: cela fait $8 \times 6 = 48$ éléments d'ordre 7. Il reste $56 - 48 = 8$ éléments, dont le neutre, et aucun n'est d'ordre 7. Or un 2-sous-groupe de Sylow compte exactement 8 éléments, tous d'ordre une puissance de 2 : il est donc formé précisément de ces huit éléments, et il est par conséquent unique. Cela donne $n_2 = 1$, que l'étape 3 interdit.

Tous les cas étant contradictoires, aucun groupe simple non abélien n'a un ordre inférieur à 60. Comme $\mathfrak{A}_5$ est simple, non abélien et d'ordre 60, le minimum est atteint. □

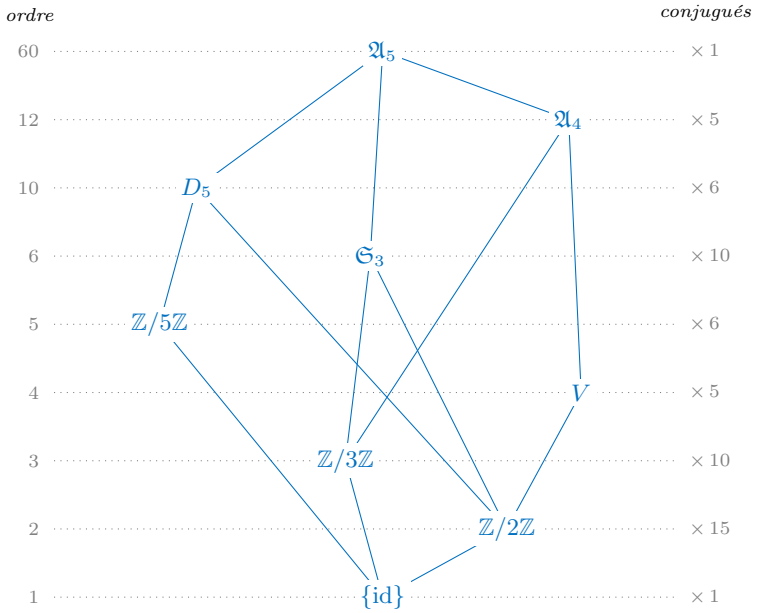
Remarque : On démontre de surcroît qu'à isomorphisme près, $\mathfrak{A}_5$ est le *seul* groupe simple d'ordre 60 : un tel groupe a nécessairement six 5-sous-groupes de Sylow, et son action par conjugaison sur ceux-ci le plonge dans $\mathfrak{S}_6$, d'où l'on tire l'isomorphisme. Nous ne détaillons pas cet argument, qui n'est pas utilisé dans la suite.

Ce résultat explique enfin pourquoi le degré 5 est le premier degré rebelle : c'est le premier pour lequel le groupe des permutations des racines contient un obstacle simple et non commutatif, et la propriété 2.12 dit qu'il ne pouvait pas apparaître plus tôt.

Exemple : **Tous les sous-groupes de $\mathfrak{A}_5$.** La simplicité ne porte que sur les sous-groupes *distingués* : elle n'interdit nullement à $\mathfrak{A}_5$ d'en posséder beaucoup d'autres. Il en compte exactement 59, répartis en neuf classes de conjugaison que le tableau ci-dessous récapitule.

ordre	nombre	structure	description
1	1	—	le sous-groupe trivial
2	15	$\mathbb{Z}/2\mathbb{Z}$	engendré par une double transposition
3	10	$\mathbb{Z}/3\mathbb{Z}$	engendré par un 3-cycle
4	5	V	les doubles transpositions portées par 4 points
5	6	$\mathbb{Z}/5\mathbb{Z}$	engendré par un 5-cycle
6	10	$\mathfrak{S}_3$	$\langle (1\ 2\ 3)\,;(1\ 2)(4\ 5)\rangle$
10	6	D_5	normalisateur d'un 5-sous-groupe de Sylow
12	5	$\mathfrak{A}_4$	stabilisateur d'un point
60	1	—	$\mathfrak{A}_5$ tout entier

Les sous-groupes d'ordres 4, 3 et 5 sont exactement les sous-groupes de Sylow, et l'on retrouve les valeurs prédites par le théorème 2.7 : $n_2 = 5$, $n_3 = 10$ et $n_5 = 6$, toutes congrues à 1 modulo le nombre premier correspondant et divisant m.



Le treillis des classes de conjugaison de sous-groupes de $\mathfrak{A}_5$. Chaque sommet représente une classe entière, et non un sous-groupe isolé ; un trait signifie « est contenu dans ». Les lignes pointillées portent l'ordre des sous-groupes qui s'y trouvent, indiqué dans la colonne de gauche, tandis que la colonne de droite donne le nombre de conjugués — les neuf ordres apparaissant chacun une fois, chaque niveau ne contient qu'une classe. Les trois traits qui se croisent au centre du diagramme, entre les niveaux 3 et 6, n'ont aucune signification : un treillis de sous-groupes ne se met pas à plat sans chevauchement.

Remarque : Ce tableau illustre concrètement l'échec de la réciproque du théorème de Lagrange, déjà signalé au chapitre 1. Les diviseurs de 60 sont 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 et 60 ; trois d'entre eux — 15, 20 et 30 — ne sont l'ordre d'aucun sous-groupe. Le lemme de plongement les élimine tous les trois d'un même argument : un sous-groupe d'ordre d est d'indice $k = \frac{60}{d}$, donc 60 devrait diviser $k!$. Or :

- ordre 30, indice 2 : 60 ne divise pas $2! = 2$ — un sous-groupe d'indice 2 serait d'ailleurs distingué (propriété 2.2), ce que la simplicité interdit directement ;
- ordre 20, indice 3 : 60 ne divise pas $3! = 6$;
- ordre 15, indice 4 : 60 ne divise pas $4! = 24$.

Les ordres 6, 10 et 12 passent en revanche le test, puisque 60 divise $10!$, $6!$ et $5!$, et ils sont effectivement atteints. Le sous-groupe d'ordre 12 est le plus intéressant des trois : d'indice 5, c'est lui qui fournit le plongement $\mathfrak{A}_5 \hookrightarrow \mathfrak{S}_5$ dont nous étions partis.

Remarque : Le treillis devient transparent si l'on se souvient que $\mathfrak{A}_5$ est le groupe des rotations de l'icosaèdre. Les six sous-groupes d'ordre 5 sont les rotations autour des six axes joignant deux sommets opposés, les dix d'ordre 3 celles autour des dix axes de faces opposées, et les quinze d'ordre 2 celles autour des quinze axes d'arêtes opposées — on retrouve bien $6 \times 4 + 10 \times 2 + 15 = 59$ rotations non triviales, soit les 59 éléments de $\mathfrak{A}_5$ distincts de l'identité. Les D_5 et les $\mathfrak{S}_3$ sont les stabilisateurs complets d'un axe de sommets ou de faces, et les cinq copies de $\mathfrak{A}_4$ correspondent aux cinq tétraèdres réguliers inscrits dans le dodécaèdre dual : ce sont eux que $\mathfrak{A}_5$ permute, et cette action sur cinq objets est exactement celle dont nous sommes partis.

Chapitre 3

Anneaux, corps et polynômes

Un groupe ne possède qu'une opération ; les objets sur lesquels on résout des équations en ont deux. Ce chapitre construit donc le second étage de l'édifice : anneaux, idéaux, quotients, puis corps. L'objectif est double. D'une part, disposer de l'anneau $K[X]$ des polynômes et de son arithmétique, entièrement calquée sur celle de $\mathbb{Z}$. D'autre part, disposer du procédé qui, à partir d'un polynôme irréductible, *fabrique* un corps dans lequel ce polynôme a une racine — c'est la clé de voûte de tout ce qui suit, car elle permettra de construire de toutes pièces le corps où vit la solution d'une équation.

3.1 Anneaux et idéaux

Définition : Un **anneau** est un triplet $(A\,;+\,;\times)$ où $(A\,;+)$ est un groupe abélien, où $\times$ est une loi interne associative possédant un élément neutre 1_A, et où la multiplication est distributive sur l'addition :

$$a(b+c)=ab+ac \qquad \text{et} \qquad (b+c)a=ba+ca$$

L'anneau est **commutatif** si $ab=ba$ pour tous a,b. Il est **intègre** s'il est commutatif, si $1_A\neq 0_A$, et si $ab=0$ entraîne $a=0$ ou $b=0$.

Dans tout ce cours, sauf mention expresse, les anneaux considérés sont commutatifs.

Exemple : Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis des opérations usuelles sont des anneaux commutatifs intègres. L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre : $\overline{2}\times\overline{3}=\overline{0}$ alors qu'aucun des deux facteurs n'est nul. L'ensemble $\mathcal{M}_n(\mathbb{R})$ des matrices carrées est un anneau non commutatif dès que $n\geqslant 2$; nous ne l'utiliserons pas.

Définition : Soient A et B deux anneaux. Un **morphisme d'anneaux** est une application $f:A\to B$ telle que $f(a+b)=f(a)+f(b)$, $f(ab)=f(a)f(b)$ et $f\,(1_A)=1_B$.

Un **idéal** de A est un sous-groupe I de $(A\,;+)$ tel que $ax\in I$ pour tous $a\in A$ et $x\in I$. L'idéal **engendré** par $a\in A$ est $(a)=aA=\{ax\ ;\ x\in A\}$; un idéal de cette forme est dit **principal**.

Exemple : La projection $\pi:\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux, de même que l'inclusion $\mathbb{Z}\hookrightarrow\mathbb{Q}$. Un exemple capital pour la suite est le **morphisme d'évaluation** : pour $a\in K$ fixé, l'application $\mathrm{ev}_a:K[X]\to K$, $P\mapsto P(a)$, respecte somme, produit et unité.

Dans $\mathbb{Z}$, l'ensemble $6\mathbb{Z}$ est un idéal : il est stable par somme, et le produit d'un entier quelconque par un multiple de 6 reste un multiple de 6. Dans $K[X]$, l'ensemble des polynômes s'annulant en a, c'est-à-dire $\mathrm{Ker}\,(\mathrm{ev}_a)$, est l'idéal principal $(X-a)$.

En revanche $\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$: il est bien stable par somme, mais $\frac{1}{2}\times 1=\frac{1}{2}$ n'est pas entier. L'absorption est une condition bien plus forte que la stabilité.

Remarque : Un idéal n'est presque jamais un sous-anneau : sauf s'il vaut A tout entier, il ne contient pas 1, car il contiendrait alors $a=a\cdot 1$ pour tout a. L'idéal est *absorbant* là où le sous-anneau est seulement stable ; c'est cette absorption qui rendra le quotient possible. On retiendra le parallèle : les idéaux sont aux anneaux ce que les sous-groupes distingués sont aux groupes.

Propriété 3.1 : Soit $f:A\to B$ un morphisme d'anneaux. Alors $\mathrm{Ker}f=\{a\in A\ ;\ f(a)=0\}$ est un idéal de A, et f est injectif si et seulement si $\mathrm{Ker}f=\{0\}$. Par ailleurs, les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$.

∘ *Démonstration :* Soit $f:A\to B$ un morphisme d'anneaux. Le noyau est un sous-groupe additif d'après le chapitre 1 ; et si $x\in\mathrm{Ker}f$ et $a\in A$, alors $f(ax)=f(a)f(x)=f(a)\cdot 0=0$, donc $ax\in\mathrm{Ker}f$. Le critère d'injectivité est celui du chapitre 1 appliqué au groupe additif.

Un idéal de $\mathbb{Z}$ est en particulier un sous-groupe de $(\mathbb{Z};+)$, donc de la forme $n\mathbb{Z}$ par le théorème 1.1 ; et réciproquement chaque $n\mathbb{Z}$ est bien absorbant. □

Théorème 3.1 : anneau quotient :
Soit A un anneau commutatif et I un idéal de A. Alors le groupe quotient A/I est muni d'une unique structure d'anneau telle que la projection $\pi : A \to A/I$ soit un morphisme d'anneaux ; sa multiplication est $\overline{a}\,\overline{b} = \overline{ab}$.

De plus, tout morphisme d'anneaux $f : A \to B$ induit un isomorphisme $A/\mathrm{Ker}f \simeq \mathrm{Im}f$.

∘ *Démonstration :* Le groupe $(A;+)$ étant abélien, I en est un sous-groupe distingué et A/I est un groupe abélien (théorème 2.1). Reste à définir la multiplication. Soient $a, a', b, b' \in A$ tels que $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$; écrivons $a' = a + x$ et $b' = b + y$ avec $x, y \in I$. Alors :

$$a'b' = (a+x)(b+y) = ab + \underbrace{ay + xb + xy}_{\in\, I}$$

chacun des trois termes soulignés étant dans I par absorption. Donc $\overline{a'b'} = \overline{ab}$: la multiplication est bien définie. L'associativité, la distributivité et la neutralité de $\overline{1}$ se lisent alors sur les représentants : elles résultent des mêmes propriétés dans A, appliquées à des représentants quelconques.

La dernière assertion se démontre exactement comme le théorème 2.2 : l'application $\overline{f}\,(\overline{a}) = f(a)$ est bien définie, bijective sur l'image, et respecte de surcroît la multiplication puisque $\overline{f}\,(\overline{a}\,\overline{b}) = f(ab) = f(a)f(b)$. □

Définition : Un **corps** est un anneau commutatif K tel que $1_K \neq 0_K$ et tel que tout élément non nul soit inversible. Autrement dit, $(K^*;\times)$ est un groupe, où $K^* = K \setminus \{0\}$.

Un idéal I de A est **maximal** si $I \neq A$ et si les seuls idéaux contenant I sont I et A.

Exemple : Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps, ainsi que $\mathbb{Z}/p\mathbb{Z}$ pour p premier. En revanche $\mathbb{Z}$ n'en est pas un : il est intègre, mais 2 n'y est pas inversible. L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'en est pas un non plus, et pour une raison plus grave : il n'est même pas intègre.

Dans $\mathbb{Z}$, l'idéal $5\mathbb{Z}$ est maximal : les idéaux le contenant sont les $d\mathbb{Z}$ avec $d \mid 5$, soit $5\mathbb{Z}$ et $\mathbb{Z}$. L'idéal $6\mathbb{Z}$ ne l'est pas, car $6\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$ fournit un idéal strictement intermédiaire. Le théorème suivant expliquera pourquoi $\mathbb{Z}/5\mathbb{Z}$ est un corps et $\mathbb{Z}/6\mathbb{Z}$ non.

Théorème 3.2 : idéaux maximaux et corps :
Soit A un anneau commutatif et I un idéal de A. Alors :

$$A/I \text{ est un corps} \iff I \text{ est maximal}$$

∘ *Démonstration :* Remarquons d'abord que la projection $\pi : A \to A/I$ établit, exactement comme le théorème de correspondance du chapitre 2, une bijection entre les idéaux de A contenant I et les idéaux de A/I ; la démonstration est identique, l'absorption se transportant dans les deux sens.

Cela ramène l'énoncé à ceci : *un anneau commutatif B tel que $1 \neq 0$ est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et B.* Démontrons-le.

Si B est un corps et $J \neq \{0\}$ un idéal, prenons $x \in J$ non nul ; alors $1 = x^{-1}x \in J$ par absorption, donc $b = b \cdot 1 \in J$ pour tout b, soit $J = B$.

Réciproquement, supposons que B n'ait que les idéaux triviaux et soit $x \neq 0$. L'ensemble $(x) = xB$ est un idéal non nul, car il contient x ; donc $(x) = B$, et $1 \in (x)$: il existe y avec $xy = 1$. Ainsi x est inversible, et B est un corps. □

Exemple : Dans $\mathbb{Z}$, l'idéal $n\mathbb{Z}$ est maximal si et seulement si n est premier. En effet $n\mathbb{Z} \subseteq d\mathbb{Z}$ équivaut à $d \mid n$; les idéaux contenant $n\mathbb{Z}$ correspondent donc aux diviseurs de n, et il n'y en a que deux, 1 et n, exactement lorsque n est premier. Le théorème 3.2 redonne alors le fait bien connu : $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier. On le note $\mathbb{F}_p$.

3.2 Caractéristique d'un corps

Définition : Soit K un corps. Il existe un unique morphisme d'anneaux $\chi : \mathbb{Z} \to K$, à savoir $\chi(n) = n{\cdot}1_K$. Son noyau est un idéal de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$; l'entier $p \geqslant 0$ ainsi défini est la **caractéristique** de K, notée $\mathrm{car}(K)$.

Exemple : On a $\mathrm{car}(\mathbb{Q}) = \mathrm{car}(\mathbb{R}) = \mathrm{car}(\mathbb{C}) = 0$: aucune somme $1+1+\cdots+1$ n'y est nulle. En revanche $\mathrm{car}(\mathbb{F}_p) = p$, puisque $\overline{1}$ ajouté p fois donne $\overline{p} = \overline{0}$, et pas avant.

Le corps $\mathbb{F}_p(T)$ des fractions rationnelles à coefficients dans $\mathbb{F}_p$ est *infini*, et pourtant de caractéristique p : la caractéristique ne mesure pas la taille du corps, mais seulement le comportement de son élément unité. C'est un point sur lequel l'intuition trompe souvent.

Propriété 3.2 : La caractéristique d'un corps est nulle ou égale à un nombre premier. Si $\mathrm{car}(K) = 0$, alors K contient un sous-corps isomorphe à $\mathbb{Q}$; si $\mathrm{car}(K) = p$, alors K contient un sous-corps isomorphe à $\mathbb{F}_p$. Ce sous-corps, le plus petit de K, est appelé **sous-corps premier**.

∘ *Démonstration :* Soit K un corps. L'image $\chi(\mathbb{Z})$ est un sous-anneau de K, donc intègre : si $a, b \in \chi(\mathbb{Z})$ vérifient $ab = 0$ avec $a \neq 0$, alors $b = a^{-1}(ab) = 0$, l'inverse a^{-1} existant dans K. Par le théorème 3.1, $\mathbb{Z}/p\mathbb{Z} \simeq \chi(\mathbb{Z})$ est donc intègre. Or $\mathbb{Z}/p\mathbb{Z}$ n'est intègre que si $p = 0$ ou p premier : en effet si $p = uv$ avec $1 < u, v < p$, alors $\overline{u}\,\overline{v} = \overline{0}$ sans que $\overline{u}$ ni $\overline{v}$ ne soient nuls.

Si $p = 0$, alors χ est injective et $\chi(\mathbb{Z}) \simeq \mathbb{Z}$; comme K est un corps, il contient les inverses des $\chi(n)$ pour $n \neq 0$, donc tous les $\chi(m)\chi(n)^{-1}$: cela fournit un morphisme injectif de $\mathbb{Q}$ dans K, dont l'image est le plus petit sous-corps de K. Si p est premier, $\chi(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est déjà un corps, et tout sous-corps de K contient 1 donc contient $\chi(\mathbb{Z})$. □

Propriété 3.3 (rêve du débutant) : Soit A un anneau commutatif de caractéristique p première, c'est-à-dire tel que $p \cdot 1_A = 0$. Alors :

$$\forall\, x, y \in A, \quad (x+y)^p = x^p + y^p$$

L'application Frob : $x \mapsto x^p$ est donc un morphisme d'anneaux, appelé **morphisme de Frobenius**.

∘ *Démonstration :* Soient $x, y \in A$. La formule du binôme, licite puisque A est commutatif, donne $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$. Il suffit donc de montrer que p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$. Or l'identité $k\binom{p}{k} = p\binom{p-1}{k-1}$, qui se vérifie en écrivant les factorielles, montre que p divise $k\binom{p}{k}$; comme p est premier et ne divise pas k pour $1 \leqslant k \leqslant p-1$, le lemme d'Euclide donne $p \mid \binom{p}{k}$.

Ainsi tous les termes intermédiaires sont nuls dans A, et il reste $(x+y)^p = x^p + y^p$. La compatibilité avec le produit, $(xy)^p = x^p y^p$ pour tous $x, y \in A$, est immédiate par commutativité, et $1^p = 1$. □

Remarque : Le nom de « rêve du débutant » rappelle qu'en caractéristique nulle cette identité est fausse et constitue l'erreur la plus répandue du calcul algébrique. En caractéristique p, elle devient vraie — et loin d'être une curiosité, elle est l'outil central de l'étude des corps finis, au chapitre 5, puis de la notion de séparabilité.

Exemple : Dans $\mathbb{F}_2$, on a bien $(1+1)^2 = 0 = 1^2 + 1^2$. Dans $\mathbb{F}_3[X]$, on obtient $(X+1)^3 = X^3 + 1$, ce que l'on vérifie en développant : $X^3 + 3X^2 + 3X + 1$, et les coefficients 3 sont nuls modulo 3.

3.3 L'anneau des polynômes

Définition : Soit K un corps. Un **polynôme** à coefficients dans K est une suite $(a_0, a_1, \dots)$ d'éléments de K tous nuls à partir d'un certain rang ; on l'écrit $P = \sum_k a_k X^k$. L'ensemble de ces polynômes, muni de l'addition terme à terme et du produit de convolution, est l'anneau $K[X]$.

Le **degré** de $P \neq 0$ est le plus grand k tel que $a_k \neq 0$; on pose $\deg 0 = -\infty$. Le polynôme est **unitaire** si son coefficient de plus haut degré vaut 1.

Exemple : Le polynôme $P = 3X^4 - X + 7$ de $\mathbb{Q}[X]$ est de degré 4 ; il n'est pas unitaire, mais $\frac{1}{3}P = X^4 - \frac{1}{3}X + \frac{7}{3}$ l'est. Diviser par le coefficient dominant permet toujours de se ramener au cas unitaire, ce dont nous userons constamment.

La convention $\deg 0 = -\infty$ n'est pas une coquetterie : elle rend la formule $\deg(PQ) = \deg P + \deg Q$ valable sans exception, y compris lorsque l'un des facteurs est nul.

Sur un corps fini, l'anneau des polynômes reste infini mais se dénombre étage par étage : dans $\mathbb{F}_2[X]$, il y a exactement quatre polynômes de degré au plus 1, à savoir 0, 1, X et $X+1$, et plus généralement 2^{n+1} polynômes de degré au plus n.

Propriété 3.4 : Pour tous $P, Q \in K[X]$, on a $\deg(PQ) = \deg P + \deg Q$. L'anneau $K[X]$ est intègre, et ses éléments inversibles sont exactement les constantes non nulles.

∘ *Démonstration :* Soient $P, Q \in K[X]$. Si P et Q sont non nuls, de degrés respectifs m et n et de coefficients dominants a_m et b_n, le coefficient de X^{m+n} dans PQ vaut $a_m b_n$, non nul puisque K est un corps donc intègre ; et aucun terme de degré supérieur n'apparaît. Donc $\deg(PQ) = m+n$ et $PQ \neq 0$: l'anneau est intègre.

Si $PQ = 1$, alors $\deg P + \deg Q = 0$ avec des degrés positifs, donc $\deg P = \deg Q = 0$: P est une constante non nulle, inversible dans K. Réciproquement ces constantes sont bien inversibles. □

Théorème 3.3 : division euclidienne :
Soient $A, B \in K[X]$ avec $B \neq 0$. Il existe un unique couple $(Q\,;R)$ de polynômes tel que :

$$A = BQ + R \qquad \text{avec} \qquad \deg R < \deg B$$

∘ *Démonstration :* **Existence.** Raisonnons par récurrence forte sur $\deg A$. Si $\deg A < \deg B$, le couple $(0\,;A)$ convient. Sinon, notons $m = \deg A \geqslant n = \deg B$, et a_m, b_n les coefficients dominants. Le polynôme :

$$A_1 = A - \frac{a_m}{b_n} X^{m-n} B$$

a un degré strictement inférieur à m, car le terme de degré m s'annule par construction — c'est ici que l'inversibilité de b_n, garantie par le fait que K est un corps, intervient. Par hypothèse de récurrence, $A_1 = BQ_1 + R$ avec $\deg R < n$, d'où $A = B\left(Q_1 + \frac{a_m}{b_n} X^{m-n}\right) + R$.

Unicité. Si $BQ + R = BQ' + R'$ avec $\deg R, \deg R' < n$, alors $B(Q - Q') = R' - R$. Si $Q \neq Q'$, le membre de gauche est de degré au moins n, et le membre de droite de degré strictement inférieur à n : contradiction. Donc $Q = Q'$ puis $R = R'$. □

Théorème 3.4 : $K[X]$ est principal :
Tout idéal de $K[X]$ est principal : pour tout idéal $I \neq \{0\}$, il existe un unique polynôme unitaire P_0 tel que $I = (P_0)$, et P_0 est l'élément non nul de I de plus petit degré.

∘ *Démonstration :* Soit $I \neq \{0\}$ un idéal. L'ensemble des degrés des éléments non nuls de I est une partie non vide de $\mathbb{N}$; elle admet donc un plus petit élément, atteint par un polynôme P_0 que l'on peut supposer unitaire quitte à le diviser par son coefficient dominant.

L'inclusion $(P_0) \subseteq I$ résulte de l'absorption. Réciproquement, soit $A \in I$. La division euclidienne donne $A = P_0 Q + R$ avec $\deg R < \deg P_0$. Or $R = A - P_0 Q \in I$; si R était non nul, ce serait un élément non nul de I de degré strictement inférieur à celui de P_0, ce qui contredit la minimalité. Donc $R = 0$ et $A \in (P_0)$.

L'unicité vient de ce que $(P_0) = (P_1)$ entraîne que chacun divise l'autre, donc qu'ils sont proportionnels ; étant tous deux unitaires, ils sont égaux. □

Remarque : C'est exactement la démonstration du théorème 1.1 sur les sous-groupes de $\mathbb{Z}$, avec le degré à la place de la valeur absolue. On dit que $\mathbb{Z}$ et $K[X]$ sont **principaux**, et toute l'arithmétique de l'un se transporte à l'autre : pgcd, identité de Bézout, lemme de Gauss, décomposition en facteurs irréductibles. Nous en ferons un usage constant.

Propriété 3.5 (Bézout et Gauss) : Soient $A, B \in K[X]$ non tous deux nuls. L'idéal $\{AU+BV\ ;\ U, V \in K[X]\}$ est engendré par un unique polynôme unitaire D, appelé **pgcd** de A et B. Alors :

- D divise A et B, et tout diviseur commun divise D ;
- il existe U, V tels que $AU + BV = D$ (**identité de Bézout**) ;
- si A divise BC et si $\text{pgcd}(A\,;B) = 1$, alors A divise C (**lemme de Gauss**).

∘ *Démonstration :* L'ensemble $I = \{AU + BV\}$ est visiblement un idéal, non nul, donc $I = (D)$ pour un unique D unitaire d'après le théorème 3.4. Comme $A = A \cdot 1 + B \cdot 0 \in I$, on a $D \mid A$, et de même $D \mid B$. Si $E \in K[X]$ divise A et B, il divise tout élément de la forme $AU + BV$ avec $U, V \in K[X]$, donc divise D. L'identité de Bézout traduit simplement $D \in I$.

Pour le lemme de Gauss, soit $C \in K[X]$ tel que $A \mid BC$, et supposons $\text{pgcd}(A\,;B) = 1$. L'identité de Bézout s'écrit $AU + BV = 1$ pour certains $U, V \in K[X]$; multiplions-la par C : $ACU + BCV = C$. Le polynôme A divise ACU et divise BC donc BCV : il divise leur somme C. □

Propriété 3.6 : Soit $P \in K[X]$ et $\alpha \in K$. Alors α est racine de P si et seulement si $(X - \alpha)$ divise P. Un polynôme non nul de degré n possède au plus n racines dans K.

∘ *Démonstration :* La division euclidienne de P par $X - \alpha$ donne $P = (X - \alpha)Q + R$ avec $\deg R < 1$, donc R constant ; en évaluant en α, on obtient $R = P(\alpha)$. Ainsi $P(\alpha) = 0$ équivaut à $(X - \alpha) \mid P$.

Pour la seconde assertion, raisonnons par récurrence sur n. Un polynôme de degré 0 est une constante non nulle, sans racine. Si $\deg P = n \geqslant 1$ et si P n'a pas de racine, c'est fini ; sinon, soit α une racine : $P = (X-\alpha)Q$ avec $\deg Q = n-1$. Toute racine $\beta \neq \alpha$ de P vérifie $(\beta-\alpha)Q(\beta) = 0$ avec $\beta - \alpha \neq 0$, donc $Q(\beta) = 0$ par intégrité. Les racines de P sont donc α et celles de Q, au nombre d'au plus $n-1$: total au plus n. □

Remarque : L'hypothèse d'intégrité est indispensable. Dans l'anneau $\mathbb{Z}/8\mathbb{Z}$, qui n'est pas intègre, le polynôme $X^2 - 1$ possède quatre racines : $\overline{1}, \overline{3}, \overline{5}, \overline{7}$. On mesure ici combien la structure de corps, si commode, est une hypothèse forte.

3.4 Irréductibilité

Définition : Un polynôme $P \in K[X]$ est **irréductible sur** K si $\deg P \geqslant 1$ et si toute factorisation $P = AB$ dans $K[X]$ impose que A ou B soit une constante.

Exemple : Tout polynôme de degré 1 est irréductible, sur n'importe quel corps : une factorisation en deux facteurs non constants exigerait des degrés au moins 1 chacun, donc un degré total au moins 2.

Le polynôme $X^2 - 2$ est irréductible sur $\mathbb{Q}$, faute de racine rationnelle, mais il ne l'est plus sur $\mathbb{R}$ où il vaut $\left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right)$. De même $X^2 + 1$ est irréductible sur $\mathbb{R}$ et se factorise en $(X - \mathrm{i})(X + \mathrm{i})$ sur $\mathbb{C}$. Enfin $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$, puisque $P(0) = P(1) = 1$, mais il se scinde dans le corps à quatre éléments que le paragraphe suivant va construire.

Trois polynômes, trois corps, trois réponses différentes : on ne dira jamais « P est irréductible » sans préciser sur quel corps.

Remarque : L'irréductibilité dépend du corps, et c'est le point le plus important de tout le chapitre. Le polynôme $X^2 + 1$ est irréductible sur $\mathbb{R}$ et ne l'est plus sur $\mathbb{C}$; le polynôme $X^2 - 2$ est irréductible sur $\mathbb{Q}$ et ne l'est plus sur $\mathbb{R}$. Dire qu'un polynôme est irréductible, sans préciser le corps, n'a donc aucun sens. Toute la théorie de Galois consiste précisément à mesurer comment un polynôme se décompose davantage lorsqu'on agrandit le corps.

Théorème 3.5 : factorisation :
Tout polynôme non constant de $K[X]$ s'écrit comme produit d'un scalaire et de polynômes irréductibles unitaires. Cette écriture est unique à l'ordre des facteurs près.

∘ *Démonstration :* **Existence**, par récurrence forte sur le degré. Soit P non constant, que l'on peut supposer unitaire quitte à extraire son coefficient dominant. Si P est irréductible, c'est fini. Sinon $P = AB$ avec A et B non constants, donc de degrés strictement inférieurs à celui de P ; l'hypothèse de récurrence s'applique à chacun, et l'on concatène les factorisations.

Unicité. Montrons d'abord que si $A, B, Q \in K[X]$ sont tels que Q soit irréductible et divise AB, alors Q divise A ou B. En effet, $\operatorname{pgcd}(Q\,;A)$ divise Q ; étant unitaire, il vaut 1 ou Q à une constante près. S'il vaut Q, alors $Q \mid A$. Sinon $\operatorname{pgcd}(Q\,;A) = 1$ et le lemme de Gauss donne $Q \mid B$.

Supposons maintenant $P_1 \cdots P_r = Q_1 \cdots Q_s$ avec tous les facteurs irréductibles unitaires, et raisonnons par récurrence sur r. Le polynôme P_1 divise le produit des Q_j, donc divise l'un d'eux, disons Q_1 après renumérotation. Comme Q_1 est irréductible et P_1 non constant, le quotient est une constante ; les deux étant unitaires, $P_1 = Q_1$. On simplifie par P_1, ce qui est licite dans l'anneau intègre $K[X]$, et l'hypothèse de récurrence conclut. □

Propriété 3.7 : Soit $P \in K[X]$ non constant. Alors P est irréductible si et seulement si l'idéal (P) est maximal.

∘ *Démonstration :* Les idéaux de $K[X]$ contenant (P) sont les (D) avec $D \mid P$, d'après le théorème 3.4 : en effet $(P) \subseteq (D)$ équivaut à $D \mid P$. Or P est irréductible si et seulement si ses seuls diviseurs unitaires sont 1 et P (à constante près), c'est-à-dire si et seulement si les seuls idéaux contenant (P) sont $K[X]$ et (P) — ce qui est la définition de la maximalité, l'inégalité $(P) \neq K[X]$ résultant de $\deg P \geqslant 1$. □

Propriété 3.8 (critères élémentaires) : Soit $P \in K[X]$.
- Si $\deg P = 1$, alors P est irréductible.
- Si $\deg P \in \{2\,;3\}$, alors P est irréductible sur K si et seulement si P n'a aucune racine dans K.
- Si $P = \sum a_k X^k \in \mathbb{Z}[X]$ et si $\frac{u}{v}$ est une racine rationnelle écrite sous forme irréductible, alors $u \mid a_0$ et $v \mid a_n$.

∘ *Démonstration :* Un polynôme de degré 1 ne peut se factoriser qu'en un produit de degrés 1 et 0.

Supposons $\deg P \in \{2\,;3\}$. Si $P = AB$ avec $A, B \in K[X]$ non constants, alors l'un des deux facteurs est de degré 1, donc de la forme $a(X-\alpha)$ avec $a \in K^*$ et $\alpha \in K$: P a une racine dans K. Réciproquement, une racine fournit un facteur de degré 1 et donc une factorisation non triviale. Attention : cette équivalence tombe en défaut dès le degré 4, comme le montre $X^4 + 2X^2 + 1 = \left(X^2+1\right)^2$, sans racine réelle mais réductible sur $\mathbb{R}$.

Pour le dernier point, soient $u \in \mathbb{Z}$ et $v \in \mathbb{N}^*$ premiers entre eux tels que $P\left(\frac{u}{v}\right) = 0$; en multipliant cette égalité par v^n, où $n = \deg P$, on obtient :

$$a_n u^n + a_{n-1}u^{n-1}v + \cdots + a_0 v^n = 0$$

L'entier u divise tous les termes sauf peut-être $a_0 v^n$, donc il divise $a_0 v^n$; étant premier avec v, il divise a_0. Symétriquement $v \mid a_n$. □

Théorème 3.6 : lemme de Gauss et critère d'Eisenstein :
Soit $P \in \mathbb{Z}[X]$ non constant.

- **Lemme de Gauss :** appelons **contenu** de P le pgcd de ses coefficients, et disons que P est **primitif** si son contenu vaut 1 — ce qui est notamment le cas s'il est unitaire. Si P est primitif et se factorise en produit de deux polynômes non constants de $\mathbb{Q}[X]$, alors il se factorise en produit de deux polynômes non constants de $\mathbb{Z}[X]$, de mêmes degrés.
- **Critère d'Eisenstein :** s'il existe un nombre premier q tel que q divise $a_0, \ldots, a_{n-1}$, que q ne divise pas a_n et que q^2 ne divise pas a_0, alors P est irréductible sur $\mathbb{Q}$.

∘ *Démonstration :* **Lemme de Gauss.** Notons $c(A)$ le contenu d'un polynôme non nul $A \in \mathbb{Z}[X]$. Montrons d'abord que le produit de deux polynômes primitifs est primitif. Soient $A = \sum a_i X^i$ et $B = \sum b_j X^j$ primitifs et q un premier. Comme q ne divise pas tous les a_i, soit i_0 le plus petit indice avec $q \nmid a_{i_0}$; définissons j_0 de même pour B. Le coefficient de $X^{i_0+j_0}$ dans AB vaut :

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

Les deux sommes de droite sont divisibles par q par minimalité de i_0 et j_0, tandis que $a_{i_0}b_{j_0}$ ne l'est pas, q étant premier. Donc q ne divise pas ce coefficient, et ceci pour tout q : AB est primitif.

Soient maintenant $P \in \mathbb{Z}[X]$ primitif et $P = AB$ une factorisation avec $A, B \in \mathbb{Q}[X]$ non constants. En chassant les dénominateurs puis en divisant par le contenu, il existe des rationnels $\lambda, \mu > 0$ tels que $A_1 = \lambda A$ et $B_1 = \mu B$ appartiennent à $\mathbb{Z}[X]$ et soient primitifs ; les degrés sont inchangés. Alors :

$$\lambda\mu\, P = A_1 B_1$$

Écrivons $\lambda\mu = \frac{u}{v}$ sous forme irréductible, avec $u, v \in \mathbb{N}^*$, de sorte que $u\,P = v\,A_1B_1$. Le contenu du membre de gauche vaut $u\,c(P) = u$ puisque P est primitif, et celui du membre de droite vaut $v\,c(A_1B_1) = v$ puisque A_1B_1 est primitif. Donc $u = v$, soit $\lambda\mu = 1$, et $P = A_1B_1$ est bien une factorisation dans $\mathbb{Z}[X]$ en deux facteurs non constants de mêmes degrés que A et B.

Eisenstein. Nous raisonnons *par contraposée*. Précisément, nous supposons que les deux premières hypothèses sont vérifiées — le nombre premier q divise $a_0, \ldots, a_{n-1}$ et ne divise pas a_n — et que P *n'est pas irréductible sur* $\mathbb{Q}$, et nous en déduisons que la troisième est en défaut, c'est-à-dire que q^2 divise a_0. Cela établira bien l'énoncé : si les trois hypothèses sont simultanément vraies, P est irréductible sur $\mathbb{Q}$.

Étape 1 : se ramener à une factorisation dans $\mathbb{Z}[X]$. Comme P n'est pas irréductible sur $\mathbb{Q}$ et qu'il n'est pas constant, il s'écrit $P = A'B'$ avec $A', B' \in \mathbb{Q}[X]$ non constants.

Notons c le contenu de P et écrivons $P = c\,P_1$ avec $P_1 = \sum b_k X^k$ primitif. Cet entier c divise a_n, donc q ne divise pas c. Par conséquent, les hypothèses se transmettent à P_1 : de $q \mid a_i = c\,b_i$ et $q \nmid c$ on tire $q \mid b_i$ pour $i \leqslant n-1$; de $q \nmid a_n$ on tire $q \nmid b_n$; et si q^2 divisait b_0, il diviserait $a_0 = c\,b_0$. Enfin $P_1 = \frac{1}{c}A'B'$ est encore produit de deux polynômes non constants de $\mathbb{Q}[X]$. Quitte à remplacer P par P_1, on peut donc supposer P primitif.

Le lemme de Gauss fournit alors une factorisation $P = AB$ avec $A = \sum_i \alpha_i X^i$ et $B = \sum_j \beta_j X^j$ dans $\mathbb{Z}[X]$, de degrés $r, s \geqslant 1$.

Étape 2 : réduction modulo q. Réduisons l'égalité $P = AB$ dans $\mathbb{F}_q[X]$, ce qui est licite puisque la réduction modulo q est un morphisme d'anneaux $\mathbb{Z}[X] \to \mathbb{F}_q[X]$. Comme q divise tous les coefficients de P sauf le dominant :

$$\overline{A}\,\overline{B} = \overline{P} = \overline{a_n}\,X^n \qquad \text{avec} \qquad \overline{a_n} \neq \overline{0}$$

Le polynôme X est irréductible dans $\mathbb{F}_q[X]$, et cet anneau est factoriel (théorème 3.5, valable sur tout corps). Les seuls diviseurs de $\overline{a_n}X^n$ y sont donc les λX^k : ainsi $\overline{A}$ et $\overline{B}$ sont des monômes. En particulier leurs termes constants $\overline{\alpha_0}$ et $\overline{\beta_0}$ sont nuls — car $r \geqslant 1$ et $s \geqslant 1$, donc les monômes $\overline{A}$ et $\overline{B}$ sont de degré au moins 1 —, c'est-à-dire que q divise α_0 et divise β_0.

Conclusion. Le terme constant de P vaut $a_0 = \alpha_0\beta_0$, qui est donc divisible par q^2. C'est exactement ce que nous voulions établir. □

Exemple : Le polynôme $X^3 - 2$ est irréductible sur $\mathbb{Q}$: le critère d'Eisenstein s'applique avec $q = 2$, puisque $2 \mid 2$, $2 \nmid 1$ et $4 \nmid 2$. On pouvait aussi invoquer la propriété 3.8 : les racines rationnelles éventuelles sont à chercher parmi $\pm 1, \pm 2$, et aucune ne convient. Plus généralement $X^n - p$ est irréductible sur $\mathbb{Q}$ pour tout premier p et tout $n \geqslant 1$.

Exemple : Soit p premier et $\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1$, dont les racines sont les racines p-ièmes de l'unité autres que 1. Eisenstein ne s'applique pas directement ; on effectue le changement de variable $X \mapsto X + 1$, qui ne change pas l'irréductibilité puisqu'une factorisation de l'un fournit une factorisation de l'autre. Comme $\Phi_p(X) = \frac{X^p - 1}{X - 1}$:

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

Tous les coefficients $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$ sont divisibles par p (propriété 3.3), le coefficient dominant vaut 1, et le terme constant vaut $\binom{p}{p-1} = p$, non divisible par p^2. Le critère d'Eisenstein s'applique : Φ_p est irréductible sur $\mathbb{Q}$. Pour $p = 5$, cela donne l'irréductibilité de $X^4 + X^3 + X^2 + X + 1$, dont on calculera le groupe de Galois au chapitre 6.

3.5 Le corps de rupture

Théorème 3.7 : construction d'une racine :
Soient K un corps et $P \in K[X]$ irréductible de degré n. Posons $L = K[X]/(P)$ et notons $\pi : K[X] \to L$ la projection canonique, ainsi que $\overline{A} = \pi(A)$ la classe d'un polynôme $A \in K[X]$. Alors :

- L est un corps ;
- l'application $\iota : K \to L$, $a \mapsto \overline{a}$, qui à un scalaire a associe la classe du *polynôme constant* égal à a, est un morphisme d'anneaux injectif : elle identifie K à un sous-corps de L ;
- l'élément $x = \overline{X}$, classe de l'indéterminée, est une racine de P dans L ;
- L est un K-espace vectoriel de dimension n, de base :
$$\left(1 ; x ; x^2 ; \ldots ; x^{n-1}\right)$$

∘ *Démonstration :* D'après la propriété 3.7 du paragraphe précédent, l'idéal (P) est maximal ; le théorème 3.2 en déduit que $L = K[X]/(P)$ est un corps.

Plongement de K. L'application ι est la composée de l'inclusion $K \hookrightarrow K[X]$, qui voit un scalaire comme un polynôme constant, et de la projection π : c'est donc un morphisme d'anneaux. Son noyau est un idéal de K, donc $\{0\}$ ou K tout entier puisque K est un corps ; et il ne peut valoir K, car $\iota(1) = \overline{1} \neq \overline{0}$ dans le corps L. Ainsi $\mathrm{Ker}\iota = \{0\}$ et ι est injective. On identifie désormais K à son image $\iota(K)$, ce qui revient à écrire a au lieu de $\overline{a}$.

x est racine de P. Écrivons $P = \sum a_k X^k$. La projection étant un morphisme d'anneaux :

$$P(x) = \sum \overline{a_k}\, \overline{X}^k = \overline{\sum a_k X^k} = \overline{P} = \overline{0}$$

puisque $P \in (P)$.

Base. *Génératrice :* tout élément de L s'écrit $\overline{A}$ pour un $A \in K[X]$; la division euclidienne $A = PQ + R$ avec $\deg R < n$ donne $\overline{A} = \overline{R}$, combinaison linéaire de $1, x, \ldots, x^{n-1}$. *Libre :* si $\lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1} x^{n-1} = 0$, alors le polynôme $R = \sum \lambda_k X^k$ appartient à (P) ; comme $\deg R < n = \deg P$, la seule possibilité est $R = 0$, donc tous les λ_k sont nuls. □

Remarque : Le sens de la notation $\overline{A}$ mérite d'être explicité, car tout le théorème repose sur elle. Un élément de L n'est pas un polynôme, mais une *classe* de polynômes : deux polynômes A et B ont la même classe si et seulement si leur différence est un multiple de P. La division euclidienne par P fournit dans chaque classe un représentant privilégié, l'unique polynôme de degré strictement inférieur à n ; calculer dans L, c'est calculer sur les polynômes puis remplacer systématiquement P par 0.

Ce que dit le deuxième point, c'est que ce procédé ne mélange pas les constantes entre elles : deux scalaires distincts $a \neq b$ de K restent distincts dans L, puisque $a - b$ est une constante non nulle, donc de degré $0 < n$, donc pas un multiple de P. Les classes $\overline{a}$ des polynômes constants forment ainsi une copie fidèle de K à l'intérieur de L, et c'est en ce sens que L est bien une *extension* de K.

Définition : Le corps $K[X]/(P)$ construit ci-dessus s'appelle un **corps de rupture** de P sur K : c'est un corps contenant K, engendré par une seule racine de P.

Exemple : Prenons $K = \mathbb{R}$ et $P = X^2 + 1$, irréductible sur $\mathbb{R}$ puisqu'il est de degré 2 et sans racine réelle. Posons $L = \mathbb{R}[X]/\left(X^2+1\right)$ et notons $x = \overline{X}$ la classe de l'indéterminée.

Pourquoi $x^2 = -1$. C'est la seule chose à comprendre, et elle ne repose sur aucune convention nouvelle : c'est la définition même du quotient. La projection π étant un morphisme d'anneaux, elle respecte sommes et produits, donc :

$$x^2 + 1 = \overline{X}^{\,2} + \overline{1} = \overline{X^2+1} = \overline{P} = \overline{0}$$

la dernière égalité venant de ce que P appartient à l'idéal (P) par lequel on quotiente : sa classe est nulle. En retranchant 1, il vient $x^2 = -1$.

Autrement dit, la relation $x^2 = -1$ n'est pas postulée : elle exprime seulement que l'on a décidé d'identifier à zéro tout multiple de X^2+1, et en particulier X^2+1 lui-même. C'est le mécanisme général du théorème 3.7 : quotienter par (P), c'est *forcer* P à s'annuler en x.

On reconnaît $\mathbb{C}$. Le théorème fournit la base $(1\,;x)$, donc tout élément de L s'écrit de manière unique $a+bx$ avec $a,b \in \mathbb{R}$, et la relation $x^2 = -1$ donne la règle de multiplication :

$$(a+bx)(c+dx) = ac + (ad+bc)x + bd\,x^2 = (ac-bd) + (ad+bc)x$$

C'est exactement celle des nombres complexes. La construction du théorème 3.7 *est* donc celle de $\mathbb{C}$, débarrassée de tout mystère, et le symbole i n'est rien d'autre que la classe de X modulo X^2+1.

Exemple : Prenons $K = \mathbb{F}_2$ et $P = X^2 + X + 1$. Il est irréductible sur $\mathbb{F}_2$ car il est de degré 2 et que $P(0) = P(1) = 1 \neq 0$.

Notons $\alpha = \overline{X}$ la classe de l'indéterminée modulo l'idéal (P) — c'est l'élément que le théorème 3.7 appelle x, autrement dit la racine de P que la construction fabrique. Le théorème affirme que $(1\,;\alpha)$ est une base de $\mathbb{F}_2[X]/(P)$ sur $\mathbb{F}_2$, donc que tout élément s'écrit de façon unique $a+b\alpha$ avec $a,b \in \mathbb{F}_2$: le corps $\mathbb{F}_2[X]/(P)$ a bien $2^2 = 4$ éléments, à savoir 0, 1, α et $\alpha+1$.

La seule relation à retenir est celle qui définit α, à savoir $P(\alpha) = 0$, soit $\alpha^2 + \alpha + 1 = 0$, c'est-à-dire :

$$\alpha^2 = -\alpha - 1 = \alpha + 1$$

la dernière égalité venant de ce que $-1 = 1$ en caractéristique 2. On en déduit toute la table de multiplication :

$$\alpha \times \alpha = \alpha + 1 \quad ; \quad \alpha \times (\alpha+1) = \alpha^2 + \alpha = (\alpha+1) + \alpha = 1 \quad ; \quad (\alpha+1)^2 = \alpha^2 + 1 = \alpha$$

Voici un corps à quatre éléments, qui n'est *pas* $\mathbb{Z}/4\mathbb{Z}$ — ce dernier n'est même pas intègre. On retiendra qu'il n'existe pas de corps $\mathbb{Z}/n\mathbb{Z}$ pour n non premier, mais qu'il existe bel et bien des corps de cardinal 4, 8, 9, etc.

Une notation anticipée. Nous noterons désormais $\mathbb{F}_4$ le corps $\mathbb{F}_2[X]/\left(X^2+X+1\right)$ que nous venons de construire. Cette notation appelle deux précautions, car elle anticipe sur le chapitre 5.

D'une part, elle ne prolonge *pas* la notation $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$: on a bien $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, mais $\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}$. L'indice désigne le *cardinal* du corps, et non l'entier par lequel on quotiente $\mathbb{Z}$.

D'autre part, écrire « $\mathbb{F}_4$ » comme s'il s'agissait d'un objet bien déterminé suppose que tous les corps à quatre éléments soient isomorphes entre eux — sans quoi la notation ne dirait pas *lequel* on désigne. C'est le théorème 5.3 qui le démontrera. D'ici là, $\mathbb{F}_4$ n'est qu'un nom commode pour le corps construit ci-dessus, et l'égalité $\mathbb{F}_4 = \mathbb{F}_2[X]/\left(X^2+X+1\right)$ est une définition, non un énoncé.

addition dans $\mathbb{F}_4$

+	0	1	α	α+1
0	0	1	α	α+1
1	1	0	α+1	α
α	α	α+1	0	1
α+1	α+1	α	1	0

multiplication dans $\mathbb{F}_4$

×	0	1	α	α+1
0	0	0	0	0
1	0	1	α	α+1
α	0	α	α+1	1
α+1	0	α+1	1	α

Les deux tables du corps $\mathbb{F}_4$. À gauche, l'addition : chaque élément est son propre opposé, la caractéristique valant 2. À droite, la multiplication : en retirant la ligne et la colonne du zéro, on retrouve la table d'un groupe d'ordre 3, nécessairement cyclique, engendré par α — les puissances successives de α sont α, $\alpha+1$, puis 1. Le chapitre 5 montrera que ce phénomène est général : le groupe multiplicatif d'un corps fini est toujours cyclique.

Exemple : Prenons $K = \mathbb{Q}$ et $P = X^3 - 2$, irréductible. Le corps $\mathbb{Q}[X]/\left(X^3 - 2\right)$ est de dimension 3 sur $\mathbb{Q}$, de base $\left(1\,;x\,;x^2\right)$ avec $x^3 = 2$. Il s'identifie au sous-corps $\mathbb{Q}\left(\sqrt[3]{2}\right) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4}\ ;\ a, b, c \in \mathbb{Q}\right\}$ de $\mathbb{R}$, par l'unique morphisme envoyant x sur $\sqrt[3]{2}$.

Calculons par exemple l'inverse de $x + 1$. L'identité de Bézout entre $X + 1$ et $X^3 - 2$ s'obtient en remarquant que $X^3 - 2 = (X + 1)\left(X^2 - X + 1\right) - 3$, d'où :

$$(x+1)\,\frac{x^2 - x + 1}{3} = 1 \qquad \text{soit} \qquad (x+1)^{-1} = \frac{x^2 - x + 1}{3}$$

On vérifie numériquement : $\sqrt[3]{2} \approx 1{,}2599$, donc $x + 1 \approx 2{,}2599$ et $\frac{x^2-x+1}{3} \approx \frac{1{,}5874-1{,}2599+1}{3} \approx 0{,}4425$, dont le produit avec 2,2599 vaut bien 1 à la précision affichée.

Remarque : Un corps de rupture ne contient qu'*une* racine, pas toutes. Dans $\mathbb{Q}[X]/\left(X^3 - 2\right) \simeq \mathbb{Q}\left(\sqrt[3]{2}\right) \subset \mathbb{R}$, le polynôme $X^3 - 2$ se factorise en $(X - x)\left(X^2 + xX + x^2\right)$, et le facteur du second degré n'a pas de racine, son discriminant $-3x^2$ étant strictement négatif. Les deux autres racines complexes, $\mathrm{j}\sqrt[3]{2}$ et $\mathrm{j}^2\sqrt[3]{2}$, sont absentes. Il faudra donc, au chapitre suivant, itérer la construction pour obtenir un corps où le polynôme se scinde complètement : ce sera le *corps de décomposition*, et c'est lui, et non le corps de rupture, qui portera le groupe de Galois.

Chapitre 4

Extensions de corps

Le chapitre précédent a fourni la brique élémentaire : à partir d'un polynôme irréductible sur K, on fabrique un corps plus grand où ce polynôme acquiert une racine. Il s'agit maintenant d'organiser cette construction. La notion centrale est celle de **degré** d'une extension, qui est simplement une dimension d'espace vectoriel ; sa propriété fondamentale, la multiplicativité, transforme les questions d'existence en questions d'arithmétique. On aboutit au *corps de décomposition* d'un polynôme, unique à isomorphisme près, qui sera le terrain de jeu de la théorie de Galois — et, en guise de première application, à la résolution complète de trois problèmes vieux de vingt-quatre siècles.

4.1 Degré d'une extension

Définition : Une **extension de corps** est la donnée d'un corps L et d'un sous-corps K de L ; on la note L/K. Alors L est naturellement un K-espace vectoriel, et le **degré** de l'extension est :

$$[L : K] = \dim_K L$$

L'extension est **finie** si ce degré est fini.

Remarque : La notation L/K ne désigne aucun quotient : c'est une convention typographique, malheureuse mais universelle, qui se lit « L sur K ». On rencontre aussi la notation $K \hookrightarrow L$, qui a le mérite d'indiquer le sens de l'inclusion.

Exemple : L'extension $\mathbb{C}/\mathbb{R}$ est de degré 2, une base étant $(1\,;\mathrm{i})$. L'extension $\mathbb{R}/\mathbb{Q}$ est de degré infini : si elle était finie de degré n, alors $\mathbb{R}$ serait en bijection avec $\mathbb{Q}^n$, donc dénombrable, ce qui est faux. Enfin $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ est de degré 2, de base $\left(1\,;\sqrt{2}\right)$.

Théorème 4.1 : multiplicativité des degrés :
Soient $K \subseteq L \subseteq M$ trois corps emboîtés. Alors :

$$[M : K] = [M : L] \times [L : K]$$

au sens où le membre de gauche est fini si et seulement si les deux facteurs le sont. Plus précisément, si $(e_i)_{1\leqslant i\leqslant m}$ est une base de L sur K et $(f_j)_{1\leqslant j\leqslant n}$ une base de M sur L, alors la famille $(e_i f_j)$ est une base de M sur K.

∘ *Démonstration :* Traitons le cas fini, le cas infini s'en déduisant par contraposition.

Famille génératrice. Soit $z \in M$. Comme (f_j) engendre M sur L, on écrit $z = \sum_j \lambda_j f_j$ avec $\lambda_j \in L$. Chaque λ_j se décompose à son tour sur la base (e_i) de L sur K : $\lambda_j = \sum_i \mu_{ij} e_i$ avec $\mu_{ij} \in K$. En substituant :

$$z = \sum_j \left(\sum_i \mu_{ij} e_i \right) f_j = \sum_{i,j} \mu_{ij}\, e_i f_j$$

La famille $(e_i f_j)$ engendre donc M sur K.

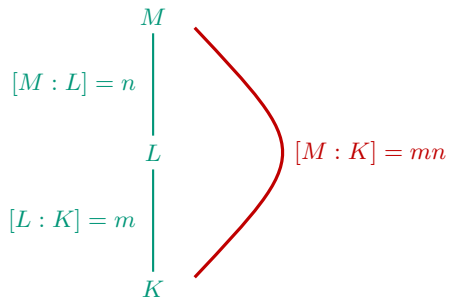
Famille libre. Supposons $\sum_{i,j} \mu_{ij} e_i f_j = 0$ avec $\mu_{ij} \in K$. Regroupons selon j :

$$\sum_j \underbrace{\left(\sum_i \mu_{ij} e_i \right)}_{\in\, L} f_j = 0$$

La famille (f_j) étant libre sur L, chaque coefficient $\sum_i \mu_{ij} e_i$ est nul ; et la famille (e_i) étant libre sur K, tous les μ_{ij} sont nuls.

La famille $(e_i f_j)$, indexée par $[\![1\,;m]\!] \times [\![1\,;n]\!]$, est donc une base de M sur K, de cardinal mn. □

Remarque : Ce théorème, d'apparence anodine, est l'outil le plus utilisé de tout le cours. Il transforme instantanément une question d'existence de corps intermédiaire en une question de divisibilité : si $[M : K] = 6$, aucun corps intermédiaire ne peut être de degré 4 sur K. C'est l'analogue exact, pour les corps, du théorème de Lagrange pour les groupes — et le chapitre 6 montrera que cette analogie est en réalité une identité.



On empile les extensions comme on empile les espaces vectoriels : les degrés se multiplient, jamais ils ne s'additionnent.

Une **tour d'extensions** et ses degrés. L'erreur la plus répandue est d'ajouter les degrés au lieu de les multiplier ; le souvenir de la dimension d'un produit d'espaces vectoriels suffit à la corriger.

4.2 Éléments algébriques et polynôme minimal

Définition : Soit L/K une extension et $\alpha \in L$. On note $K[\alpha]$ le plus petit sous-anneau de L contenant K et α, c'est-à-dire l'ensemble des $P(\alpha)$ pour $P \in K[X]$; et $K(\alpha)$ le plus petit sous-corps de L contenant K et α.

L'élément α est **algébrique sur** K s'il existe $P \in K[X]$ non nul tel que $P(\alpha) = 0$; sinon il est **transcendant sur** K.

Exemple : **Éléments algébriques sur $\mathbb{Q}$.** Tout rationnel a est algébrique, puisqu'il annule $X - a$. Le nombre $\sqrt{2}$ annule $X^2 - 2$, l'imaginaire i annule $X^2 + 1$, le nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$ annule $X^2 - X - 1$, et $\sqrt[3]{2}$ annule $X^3 - 2$. Plus généralement, $\sqrt[n]{a}$ annule $X^n - a$ pour tout rationnel $a > 0$, et la racine n-ième de l'unité $\zeta_n = \mathrm{e}^{2\mathrm{i}\pi/n}$ annule $X^n - 1$.

Le chapitre 3 en fournit une famille entière, et par construction : dans un corps de rupture $K[X]/(P)$, la classe $x = \overline{X}$ annule P, donc elle est algébrique sur K. C'est même là tout le sens de cette construction — fabriquer un élément algébrique de polynôme annulateur imposé d'avance.

Exemple : **Un élément transcendant sans mystère.** Soit K un corps et $K(T)$ le corps des fractions rationnelles en une indéterminée T. Alors T est transcendant sur K, et pour une raison tautologique : si $P = \sum a_k X^k \in K[X]$ vérifie $P(T) = 0$, cela signifie que le polynôme $\sum a_k T^k$ est nul dans $K[T]$, donc que tous les a_k sont nuls, donc que $P = 0$.

Cet exemple est le modèle de tous les autres : dire que α est transcendant sur K, c'est exactement dire que le morphisme d'évaluation $K[X] \to L$, $P \mapsto P(\alpha)$, est *injectif*, donc que $K[\alpha] \simeq K[X]$ et $K(\alpha) \simeq K(X)$. Un élément transcendant se comporte comme une indéterminée : il ne satisfait aucune relation.

Exemple : **Éléments transcendants sur $\mathbb{Q}$.** Ils existent, mais sont difficiles à exhiber. **Liouville** en construit le premier exemple explicite en 1844 :

$$\sum_{n \geqslant 1} 10^{-n!} \;=\; 0{,}11000100000000000000000001\ldots$$

les chiffres 1 occupant les rangs 1!, 2!, 3!, … Les plages de zéros, de plus en plus longues, permettent une approximation rationnelle trop bonne pour un nombre algébrique, ce qui suffit à conclure. **Hermite** démontre en 1873 que e est transcendant, et **Lindemann** en 1882 que π l'est — résultat dont le paragraphe 4.4 tirera l'impossibilité de la quadrature du cercle. Aucune de ces démonstrations n'est algébrique : toutes reposent sur des estimations analytiques.

Remarque : Comme l'irréductibilité au chapitre 3, le caractère algébrique dépend du corps de base, et il faut toujours préciser lequel. Le nombre π est transcendant sur $\mathbb{Q}$; mais il est algébrique sur $\mathbb{R}$, où il annule le polynôme $X - \pi$ de degré 1 ; et il est algébrique de degré 2 sur $\mathbb{Q}(\pi^2)$, où il annule $X^2 - \pi^2$ — ce polynôme est bien irréductible sur $\mathbb{Q}(\pi^2)$, car π n'y appartient pas, $\sqrt{T}$ n'étant pas une fraction rationnelle en T. Un même nombre peut donc être transcendant, de degré 2 ou de degré 1 selon le corps depuis lequel on le regarde.

Remarque : Un argument de dénombrabilité, dû à **Cantor** en 1874, montre que les nombres transcendants sont l'immense majorité. L'ensemble $\mathbb{Q}[X]$ est dénombrable — un polynôme est une suite finie de rationnels — et chaque polynôme non nul n'a qu'un nombre fini de racines ; l'ensemble des nombres algébriques sur $\mathbb{Q}$ est donc une réunion dénombrable d'ensembles finis, donc dénombrable. Comme $\mathbb{R}$ ne l'est pas, presque tout réel est transcendant.

Le contraste est piquant : on sait depuis un siècle et demi que presque tous les réels sont transcendants, et l'on peine encore à le démontrer pour un nombre donné. On ignore par exemple si $\pi+\mathrm{e}$ est transcendant, alors même que l'on sait que l'un au moins des deux nombres $\pi+\mathrm{e}$ et $\pi\mathrm{e}$ l'est.

Théorème 4.2 : polynôme minimal :
Soit L/K une extension et $\alpha \in L$ algébrique sur K. Il existe un unique polynôme unitaire $\mu_{\alpha,K} \in K[X]$, appelé **polynôme minimal** de α sur K, tel que :

$$\{P \in K[X]\ ;\ P(\alpha)=0\} = (\mu_{\alpha,K})$$

Ce polynôme est irréductible, c'est le polynôme unitaire non nul de plus petit degré annulant α, et si n est son degré :

$$K[\alpha] = K(\alpha) \simeq K[X]/(\mu_{\alpha,K}) \qquad \text{et} \qquad [K(\alpha):K] = n$$

∘ *Démonstration :* Considérons le morphisme d'*évaluation* $\mathrm{ev}_\alpha : K[X] \to L$, $P \mapsto P(\alpha)$. C'est un morphisme d'anneaux, d'image $K[\alpha]$. Son noyau est un idéal de $K[X]$, non nul puisque α est algébrique ; par le théorème 3.4, il est engendré par un unique polynôme unitaire μ, qui est l'élément non nul de plus petit degré du noyau.

Irréductibilité. Si $\mu = AB$ avec $\deg A, \deg B \geqslant 1$, alors $A(\alpha)B(\alpha) = 0$ dans le corps L, donc $A(\alpha) = 0$ ou $B(\alpha) = 0$; l'un des deux appartiendrait au noyau tout en étant de degré strictement inférieur à celui de μ, ce qui est exclu. Donc μ est irréductible.

Structure. Le théorème 3.1 donne $K[X]/(\mu) \simeq \mathrm{Im}(\mathrm{ev}_\alpha) = K[\alpha]$. Comme μ est irréductible, $K[X]/(\mu)$ est un corps (théorème 3.7) ; donc $K[\alpha]$ est un corps contenant K et α, et tout corps contenant K et α contient $K[\alpha]$: ainsi $K[\alpha] = K(\alpha)$. Enfin le même théorème donne la base $\left(1\,;\alpha\,;\ldots\,;\alpha^{n-1}\right)$, d'où $[K(\alpha):K] = n$. □

Remarque : L'égalité $K[\alpha] = K(\alpha)$ mérite d'être méditée : elle affirme que si α est algébrique, l'inverse de tout polynôme non nul en α est encore un polynôme en α. Rien de tel pour un élément transcendant : dans $\mathbb{Q}(\pi)$, l'inverse de π n'est pas un polynôme en π, et $\mathbb{Q}[\pi] \simeq \mathbb{Q}[X]$ n'est pas un corps.

Méthode : Pour déterminer le polynôme minimal de α sur K, on procède en deux temps :

1. On exhibe un polynôme $P \in K[X]$ unitaire annulant α, en général en isolant les radicaux et en élevant à la puissance convenable ;

2. On démontre que P est irréductible sur K (Eisenstein, absence de racine en degré 2 ou 3, réduction modulo un premier). Alors $\mu_{\alpha,K} = P$.

Sauter la seconde étape est l'erreur la plus répandue : un polynôme annulateur n'est pas le polynôme minimal.

Exemple : Sur $\mathbb{Q}$, l'élément $\sqrt{2}$ annule X^2-2, irréductible car sans racine rationnelle. Donc $\mu = X^2-2$ et $\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right] = 2$.

L'élément $\alpha = \sqrt{2}+\sqrt{3}$ demande plus de soin. De $\alpha^2 = 5+2\sqrt{6}$ on tire $\left(\alpha^2-5\right)^2 = 24$, soit $\alpha^4 - 10\alpha^2 + 1 = 0$. Le polynôme $P = X^4 - 10X^2 + 1$ n'a pas de racine rationnelle (les candidats ±1 ne conviennent pas) ; s'il se factorisait en deux facteurs de degré 2 unitaires à coefficients entiers, l'écriture $\left(X^2+aX+b\right)\left(X^2-aX+c\right)$ donnerait $b+c-a^2 = -10$, $a(c-b) = 0$ et $bc = 1$, d'où soit $a = 0$ et $b+c = -10$, $bc = 1$, système sans solution entière, soit $b = c = \pm1$ et $a^2 = 12$ ou $a^2 = 8$, sans solution entière non plus. Donc P est irréductible sur $\mathbb{Q}$ et $\left[\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right):\mathbb{Q}\right] = 4$.

Exemple : Déterminons le polynôme minimal de $\mathrm{j} = \mathrm{e}^{2\mathrm{i}\pi/3}$ sur $\mathbb{Q}$, en suivant pas à pas la méthode ci-dessus.

1. Un polynôme annulateur. Par définition, $\mathrm{j}^3 = \mathrm{e}^{2\mathrm{i}\pi} = 1$, donc $\mathrm{j}^3 - 1 = 0$. En factorisant :

$$(\mathrm{j}-1)\left(\mathrm{j}^2+\mathrm{j}+1\right) = 0$$

Or $\mathrm{j} \neq 1$, puisque $\frac{2\pi}{3}$ n'est pas un multiple de 2π ; donc $\mathrm{j}-1 \neq 0$, et comme $\mathbb{C}$ est un corps donc intègre, c'est le second facteur qui s'annule. Le polynôme unitaire $P = X^2+X+1$ annule ainsi j.

2. Il est irréductible sur $\mathbb{Q}$. Étant de degré 2, la propriété 3.8 s'applique : il est irréductible si et seulement s'il n'a aucune racine dans $\mathbb{Q}$. Or son discriminant vaut $1-4 = -3 < 0$, donc il n'a aucune racine réelle, *a fortiori* aucune racine rationnelle. On peut aussi conclure sans discriminant, par le critère des racines rationnelles : les seuls candidats sont ±1, et $P(1) = 3 \neq 0$, $P(-1) = 1 \neq 0$.

3. Conclusion. Un polynôme unitaire, annulateur et irréductible est le polynôme minimal. Donc $\mu_{\mathrm{j},\mathbb{Q}} = X^2 + X + 1$, de degré 2, et le théorème 4.2 donne :

$$[\mathbb{Q}(\mathrm{j}) : \mathbb{Q}] = 2 \qquad \text{avec} \qquad \mathbb{Q}(\mathrm{j}) = \{a + b\,\mathrm{j}\ ;\ a, b \in \mathbb{Q}\}$$

la base étant $(1\,;\mathrm{j})$ et la relation $\mathrm{j}^2 = -\mathrm{j} - 1$ permettant de multiplier deux tels éléments sans quitter cette forme. On reconnaît $\mathbb{Q}\big(\mathrm{i}\sqrt{3}\big)$, puisque $\mathrm{j} = \frac{-1+\mathrm{i}\sqrt{3}}{2}$.

Le piège. On aurait pu croire le degré égal à 3, la relation qui vient d'abord à l'esprit étant $\mathrm{j}^3 = 1$, c'est-à-dire le polynôme $X^3 - 1$. Mais celui-ci n'est *pas* le polynôme minimal : il se factorise en $(X-1)\big(X^2+X+1\big)$, donc il n'est pas irréductible. C'est exactement l'erreur contre laquelle met en garde la seconde étape de la méthode. Le degré de j est celui du plus petit polynôme qui l'annule, non du premier qui se présente.

Le corps de base compte. Sur $\mathbb{R}$, le polynôme minimal de j est encore $X^2 + X + 1$, qui reste irréductible faute de racine réelle. Mais sur $\mathbb{C}$, c'est $X - \mathrm{j}$, de degré 1, et $[\mathbb{C}(\mathrm{j}) : \mathbb{C}] = 1$ puisque j y appartient déjà. Le polynôme minimal dépend du corps de base autant que l'irréductibilité.

Propriété 4.3 : Soit L/K une extension.

- Si $[L : K]$ est fini, tout élément de L est algébrique sur K, de degré divisant $[L : K]$.
- Si α et β sont algébriques sur K, alors $[K(\alpha\,;\beta) : K]$ est fini ; en particulier $\alpha + \beta$, $\alpha\beta$ et α^{-1} (si $\alpha \neq 0$) sont algébriques sur K.

∘ *Démonstration :* Soit $n = [L : K]$ fini et $\alpha \in L$. La famille $(1\,;\alpha\,;\ldots\,;\alpha^n)$ compte $n+1$ vecteurs dans un espace de dimension n : elle est liée. Une relation de liaison non triviale fournit un polynôme non nul de degré au plus n annulant α. Enfin $K \subseteq K(\alpha) \subseteq L$ et le théorème 4.1 donnent $[K(\alpha) : K] \mid [L : K]$.

Pour le second point, notons $m = \deg \mu_{\alpha,K}$. Le polynôme $\mu_{\beta,K}$ annule β et est à coefficients dans $K \subseteq K(\alpha)$, donc β est algébrique sur $K(\alpha)$, de degré $p \leqslant \deg \mu_{\beta,K}$. Alors :

$$[K(\alpha\,;\beta) : K] = [K(\alpha)(\beta) : K(\alpha)] \times [K(\alpha) : K] = p\,m < +\infty$$

Les éléments $\alpha+\beta$, $\alpha\beta$ et α^{-1} appartiennent à $K(\alpha\,;\beta)$, qui est de degré fini sur K : le premier point s'applique. □

Remarque : Ce résultat est spectaculaire par ce qu'il évite. Montrer directement que $\sqrt{2} + \sqrt[3]{5}$ est algébrique sur $\mathbb{Q}$ demanderait d'exhiber un polynôme annulateur, calcul pénible ; la propriété 4.3 le garantit sans aucun calcul, en majorant simplement un degré par $2 \times 3 = 6$. C'est le premier bénéfice concret du point de vue « espaces vectoriels ».

4.3 Corps de décomposition

Définition : Soit $P \in K[X]$ non constant. Une extension L/K est un **corps de décomposition** de P sur K si :

- P est **scindé** dans $L[X]$, c'est-à-dire produit de facteurs de degré 1 ;
- L est engendré sur K par les racines de P, soit $L = K(\alpha_1\,;\ldots\,;\alpha_n)$.

Exemple : Le corps de décomposition de $X^2 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}\big(\sqrt{2}\big)$: le polynôme y est scindé, en $\big(X - \sqrt{2}\big)\big(X + \sqrt{2}\big)$, et les deux racines engendrent bien ce corps. Celui de $X^2 + 1$ sur $\mathbb{R}$ est $\mathbb{C}$.

Le contre-exemple est tout aussi instructif : $\mathbb{Q}\big(\sqrt[3]{2}\big)$ n'est *pas* un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$. La seconde condition y est bien vérifiée — le corps est engendré par la racine qu'il contient — mais la première ne l'est pas, le polynôme s'y factorisant en $\big(X - \sqrt[3]{2}\big)\big(X^2 + \sqrt[3]{2}X + \sqrt[3]{4}\big)$ sans que le second facteur se scinde. Il faut aller jusqu'à $\mathbb{Q}\big(\sqrt[3]{2}\,;\mathrm{j}\big)$, comme on le verra plus loin.

Théorème 4.3 : existence du corps de décomposition :
Tout polynôme non constant $P \in K[X]$ admet un corps de décomposition sur K, de degré au plus $(\deg P)!$ sur K.

∘ *Démonstration :* Récurrence forte sur $n = \deg P$. Si $n = 1$, alors P est déjà scindé et $L = K$ convient.

Soit $n \geqslant 2$. Choisissons un facteur irréductible Q de P dans $K[X]$ et posons $K_1 = K[X]/(Q)$, corps de rupture dans lequel Q, donc P, admet une racine α_1 ; on a $[K_1 : K] = \deg Q \leqslant n$. Dans $K_1[X]$, on écrit $P = (X - \alpha_1)\,P_1$ avec $\deg P_1 = n - 1$. Par hypothèse de récurrence, P_1 admet un corps de décomposition L sur K_1, avec $[L : K_1] \leqslant (n-1)!$.

Dans L, le polynôme $P = (X-\alpha_1)\,P_1$ est scindé, et L est engendré sur K par α_1 et les racines de P_1, c'est-à-dire par les racines de P. Enfin $[L:K] = [L:K_1]\,[K_1:K] \leqslant (n-1)! \times n = n!$. □

Propriété 4.4 (prolongement) : Soit $\sigma : K \to K'$ un isomorphisme de corps, prolongé en un isomorphisme $K[X] \to K'[X]$ noté encore σ. Soit $Q \in K[X]$ irréductible, α une racine de Q dans une extension de K, et α' une racine de $\sigma(Q)$ dans une extension de K'. Alors il existe un unique isomorphisme :

$$\widetilde{\sigma} : K(\alpha) \longrightarrow K'(\alpha') \qquad \text{tel que} \qquad \widetilde{\sigma}_{|K} = \sigma \quad \text{et} \quad \widetilde{\sigma}(\alpha) = \alpha'$$

∘ *Démonstration :* Le polynôme $\sigma(Q)$ est irréductible sur K', car une factorisation non triviale se transporterait par σ^{-1}. L'isomorphisme $K[X] \to K'[X]$ envoie l'idéal (Q) sur $(\sigma(Q))$, donc induit un isomorphisme des quotients :

$$K[X]/(Q) \xrightarrow{\sim} K'[X]/(\sigma(Q))$$

En composant avec les isomorphismes $K(\alpha) \simeq K[X]/(Q)$ et $K'(\alpha') \simeq K'[X]/(\sigma(Q))$ du théorème 4.2, on obtient $\widetilde{\sigma}$, qui prolonge σ et envoie α sur α'. L'unicité est claire : un tel morphisme est déterminé par ses valeurs sur K et sur α, puisque tout élément de $K(\alpha)$ est un polynôme en α à coefficients dans K. □

Théorème 4.4 : unicité du corps de décomposition :
Soit $\sigma : K \to K'$ un isomorphisme de corps, $P \in K[X]$ non constant, L un corps de décomposition de P sur K et L' un corps de décomposition de $\sigma(P)$ sur K'. Alors σ se prolonge en un isomorphisme $L \to L'$.

En particulier (cas $K = K'$ et $\sigma = \mathrm{id}$), deux corps de décomposition d'un même polynôme sur K sont isomorphes par un isomorphisme fixant K. On parle donc *du* corps de décomposition de P.

∘ *Démonstration :* Récurrence forte sur $[L:K]$. Si $[L:K] = 1$, alors $L = K$, P est scindé sur K, donc $\sigma(P)$ est scindé sur K' ; comme L' est engendré par les racines de $\sigma(P)$, qui sont dans K', on a $L' = K'$ et σ convient.

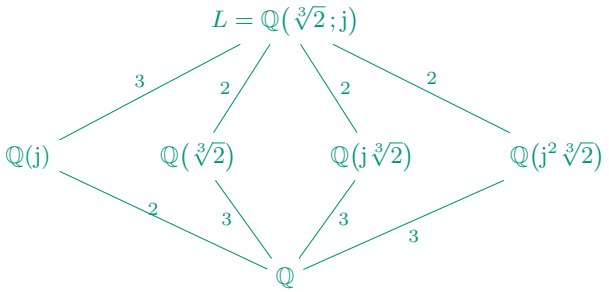
Si $[L:K] > 1$, le polynôme P possède un facteur irréductible Q dans $K[X]$ de degré $\geqslant 2$. Soit $\alpha \in L$ une racine de Q. Le polynôme $\sigma(Q)$ divise $\sigma(P)$, qui est scindé sur L' ; il admet donc une racine $\alpha' \in L'$. La propriété 4.4 fournit un isomorphisme $\widetilde{\sigma} : K(\alpha) \to K'(\alpha')$ prolongeant σ.

Or L est un corps de décomposition de P sur $K(\alpha)$, et L' en est un de $\widetilde{\sigma}(P) = \sigma(P)$ sur $K'(\alpha')$. Comme $[L:K(\alpha)] = \frac{[L:K]}{\deg Q} < [L:K]$, l'hypothèse de récurrence appliquée à $\widetilde{\sigma}$ fournit le prolongement cherché de $\widetilde{\sigma}$, donc de σ, en un isomorphisme $L \to L'$. □

Exemple : Le corps de décomposition de $X^2 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt{2})$, de degré 2 : les deux racines $\pm\sqrt{2}$ engendrent le même corps.

Celui de $(X^2-2)(X^2-3)$ est $\mathbb{Q}(\sqrt{2};\sqrt{3})$, de degré 4. En effet $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, et $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$: sinon $\sqrt{3} = a + b\sqrt{2}$ donnerait, en élevant au carré, $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, donc $ab = 0$; le cas $b = 0$ donne $\sqrt{3} \in \mathbb{Q}$, exclu, et le cas $a = 0$ donne $3 = 2b^2$, soit $\sqrt{6} = 2b \in \mathbb{Q}$, également exclu. Donc $[\mathbb{Q}(\sqrt{2};\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ et le degré total vaut 4.

Exemple : Le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est $L = \mathbb{Q}(\sqrt[3]{2};\mathrm{j})$, où $\mathrm{j} = \mathrm{e}^{2\mathrm{i}\pi/3}$, car les trois racines sont $\sqrt[3]{2}$, $\mathrm{j}\sqrt[3]{2}$ et $\mathrm{j}^2\sqrt[3]{2}$, et leurs quotients redonnent j. Son degré vaut 6 : on a $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ et $\mathrm{j} \notin \mathbb{R} \supseteq \mathbb{Q}(\sqrt[3]{2})$, donc $[L : \mathbb{Q}(\sqrt[3]{2})] = 2$. On notera que $6 = 3!$: la borne du théorème 4.3 est atteinte.



Les trois corps de rupture sont distincts mais isomorphes. Un seul est contenu dans $\mathbb{R}$.

Les corps intermédiaires entre $\mathbb{Q}$ et le corps de décomposition de $X^3 - 2$, avec les degrés portés sur les arêtes. Le produit des degrés le long de tout chemin vaut 6, conformément au théorème 4.1. On observera que ce diagramme compte exactement six sous-corps — nous verrons au chapitre 6 qu'il est la copie renversée du treillis des sous-groupes de $\mathfrak{S}_3$, qui en compte six lui aussi.

4.4 Constructions à la règle et au compas

Nous interrompons un instant le développement de la théorie pour en récolter un premier fruit, et non des moindres : la résolution de trois problèmes posés par les géomètres grecs et restés ouverts pendant vingt-quatre siècles.

Définition : On identifie le plan à $\mathbb{C}$. Partant de l'ensemble $E_0 = \{0\,;1\}$, on construit par récurrence E_{k+1} en adjoignant à E_k tous les points obtenus comme intersection de deux droites passant chacune par deux points de E_k, de deux cercles centrés en un point de E_k et de rayon la distance entre deux points de E_k, ou d'une telle droite et d'un tel cercle.

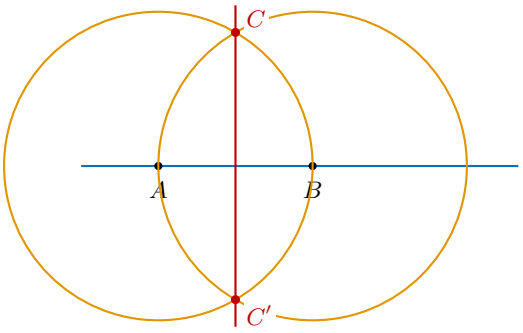
Un nombre $z \in \mathbb{C}$ est **constructible à la règle et au compas** s'il appartient à $\bigcup_{k\geqslant 0} E_k$.

Exemple : Déterminons E_1. Partant de $E_0 = \{0\,;1\}$, la seule droite disponible est l'axe réel, et les seuls cercles sont ceux de centre 0 ou 1 et de rayon 1, la seule distance entre points de E_0 valant 1. Les intersections donnent : l'axe et le cercle de centre 0 se coupent en ± 1 ; l'axe et le cercle de centre 1 se coupent en 0 et 2 ; les deux cercles se coupent en $\frac{1}{2} \pm \mathrm{i}\frac{\sqrt{3}}{2}$. Ainsi :

$$E_1 = \left\{0\,;1\,;-1\,;2\,;\tfrac{1}{2}+\mathrm{i}\tfrac{\sqrt{3}}{2}\,;\tfrac{1}{2}-\mathrm{i}\tfrac{\sqrt{3}}{2}\right\}$$

Dès la première étape apparaissent donc un nombre négatif, un entier nouveau, et surtout deux nombres non réels faisant intervenir $\sqrt{3}$: on voit poindre la racine carrée qui gouvernera tout le paragraphe.

En itérant, on obtient tous les rationnels, puis i, puis $\sqrt{2}$ comme diagonale du carré unité, et de proche en proche une infinité de nombres. La propriété 4.6 montrera en revanche que $\sqrt[3]{2}$ n'y figure jamais, quel que soit le nombre d'étapes.



L'intersection de deux cercles se calcule en soustrayant leurs équations : on obtient une droite, puis une équation du second degré.

Ici $C = \frac{6}{5} + \mathrm{i}\frac{12\sqrt{3}}{10}$, *de degré* 2 *sur* $\mathbb{Q}$.

La construction de la médiatrice de $[AB]$, avec $A = 0$ et $B = \frac{12}{5}$. Les coordonnées des points C et C' s'obtiennent en résolvant un système d'une équation linéaire et d'une équation du second degré : c'est le mécanisme général, et c'est lui qui explique pourquoi seules des racines carrées peuvent apparaître.

Théorème 4.5 : critère de Wantzel :
Si $z \in \mathbb{C}$ est constructible, alors il existe une tour d'extensions :

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r \ni z \qquad \text{avec} \qquad [K_{i+1} : K_i] = 2$$

En particulier $[\mathbb{Q}(z) : \mathbb{Q}]$ est une puissance de 2.

◦ *Démonstration :* Toute la difficulté est de suivre les *coordonnées* des points construits plutôt que les points eux-mêmes. Nous travaillons donc dans $\mathbb{R}$, et ne revenons à $\mathbb{C}$ qu'à la toute fin.

Le corps des coordonnées. Pour $k \geqslant 0$, notons F_k le sous-corps de $\mathbb{R}$ engendré sur $\mathbb{Q}$ par les abscisses et les ordonnées de tous les points de E_k. Comme $E_0 = \{0\,;1\}$, dont les coordonnées sont $(0\,;0)$ et $(1\,;0)$, on a $F_0 = \mathbb{Q}$. Nous allons montrer que l'on passe de F_k à F_{k+1} par une suite finie d'extensions de degré 1 ou 2.

Les équations sont à coefficients dans F_k. Soit F un sous-corps de $\mathbb{R}$ contenant F_k.

- La droite passant par deux points distincts $A = (x_A\,;y_A)$ et $B = (x_B\,;y_B)$ de E_k a pour équation $(y_B - y_A)(x - x_A) - (x_B - x_A)(y - y_A) = 0$, soit :
$$ax + by = c \qquad \text{avec} \qquad a = y_B - y_A, \quad b = x_A - x_B, \quad c = a\,x_A + b\,y_A$$
Ces trois nombres sont dans F, et $(a\,;b) \neq (0\,;0)$ puisque $A \neq B$.
- Le cercle de centre $\Omega = (x_0\,;y_0) \in E_k$ et de rayon ρ égal à la distance entre deux points C, D de E_k a pour équation $(x - x_0)^2 + (y - y_0)^2 = \rho^2$, soit :
$$x^2 + y^2 + \alpha x + \beta y + \gamma = 0 \qquad \text{avec} \qquad \alpha = -2x_0, \quad \beta = -2y_0, \quad \gamma = x_0^2 + y_0^2 - \rho^2$$
Ces trois nombres sont encore dans F, car $\rho^2 = (x_C - x_D)^2 + (y_C - y_D)^2$ y appartient — c'est le carré de la distance, et non la distance elle-même, qui intervient, et c'est précisément ce qui rend la construction possible.

Premier cas : deux droites sécantes. Leurs équations $ax+by=c$ et $a'x+b'y=c'$ sont à coefficients dans F, et le déterminant $\delta = ab'-a'b$ est non nul puisque les droites ne sont pas parallèles. Les formules de Cramer donnent :

$$x = \frac{cb'-c'b}{\delta} \in F \qquad \text{et} \qquad y = \frac{ac'-a'c}{\delta} \in F$$

Le point d'intersection a donc ses coordonnées dans F : l'extension $F(x\,;y)=F$ est de degré 1.

Deuxième cas : une droite et un cercle. Soient $ax+by=c$ et $x^2+y^2+\alpha x+\beta y+\gamma=0$, à coefficients dans F. Comme $(a\,;b)\neq(0\,;0)$, supposons $b\neq 0$ — sinon on échange les rôles de x et de y, ce qui est licite par symétrie. On tire alors $y=\frac{c-ax}{b}$, que l'on reporte dans l'équation du cercle ; en multipliant par b^2 pour chasser les dénominateurs :

$$\left(a^2+b^2\right)x^2+\left(b^2\alpha-2ac-ab\beta\right)x+\left(c^2+bc\beta+b^2\gamma\right)=0$$

C'est une équation du second degré à coefficients dans F, son coefficient dominant a^2+b^2 étant non nul. L'abscisse x annule donc un polynôme non nul de degré 2 de $F[X]$, d'où $[F(x):F]\leqslant 2$ par le théorème 4.2. Et l'ordonnée s'en déduit sans nouvelle extension, puisque $y=\frac{c-ax}{b}\in F(x)$. Au total :

$$[F(x\,;y):F]=[F(x):F]\in\{1\,;2\}$$

Troisième cas : deux cercles sécants. Leurs équations sont $x^2+y^2+\alpha x+\beta y+\gamma=0$ et $x^2+y^2+\alpha' x+\beta' y+\gamma'=0$. Retranchons la seconde de la première : les termes x^2+y^2 disparaissent et il reste :

$$\left(\alpha-\alpha'\right)x+\left(\beta-\beta'\right)y+\left(\gamma-\gamma'\right)=0$$

Si l'on avait $\alpha=\alpha'$ et $\beta=\beta'$, les deux cercles auraient même centre ; étant distincts, ils seraient alors concentriques de rayons différents, donc sans point commun, ce qui contredit l'hypothèse. Donc $(\alpha-\alpha'\,;\beta-\beta')\neq(0\,;0)$ et l'égalité ci-dessus est bien l'équation d'une droite à coefficients dans F, appelée **axe radical** des deux cercles. Tout point commun aux deux cercles lui appartient, et appartient au premier cercle : on est ramené au deuxième cas, et le degré vaut encore 1 ou 2.

Construction de la tour. Les points de E_{k+1} qui ne sont pas dans E_k sont en nombre fini ; notons-les $P_1,\dots,P_m$, de coordonnées $(x_j\,;y_j)$. Posons $G_0=F_k$ puis, pour $1\leqslant j\leqslant m$, $G_j=G_{j-1}(x_j\,;y_j)$. Chaque P_j est intersection de droites ou de cercles déterminés par des points de E_k, dont les coordonnées sont dans $F_k\subseteq G_{j-1}$: les trois cas s'appliquent avec $F=G_{j-1}$ et donnent $[G_j:G_{j-1}]\in\{1\,;2\}$. Comme $F_{k+1}=G_m$, on passe bien de F_k à F_{k+1} par une suite finie d'extensions de degré 1 ou 2.

Conclusion. Soit z constructible : il appartient à E_r pour un certain r, et s'écrit $z=x+\mathrm{i}y$ avec $x,y\in F_r$ par définition de F_r. En concaténant les chaînes obtenues pour $k=0,\dots,r-1$, en supprimant les étapes de degré 1 — qui ne changent pas le corps — et en ajoutant la dernière étape $F_r\subseteq F_r(\mathrm{i})$, de degré 2 puisque i annule X^2+1 sans appartenir à $F_r\subseteq\mathbb{R}$, on obtient une tour :

$$\mathbb{Q}=K_0\subseteq K_1\subseteq\cdots\subseteq K_t=F_r(\mathrm{i})\ni z \qquad \text{avec} \qquad [K_{i+1}:K_i]=2$$

Le théorème 4.1 donne alors $[K_t:\mathbb{Q}]=2^t$ par multiplicativité. Enfin $\mathbb{Q}\subseteq\mathbb{Q}(z)\subseteq K_t$, et le même théorème donne $[\mathbb{Q}(z):\mathbb{Q}]\mid 2^t$: c'est une puissance de 2. □

Remarque : La réciproque est *fausse* en général : il ne suffit pas que $[\mathbb{Q}(z):\mathbb{Q}]$ soit une puissance de 2 pour que z soit constructible. Le chapitre 7 donnera la condition exacte, qui fait intervenir le degré du corps de décomposition et non celui de z seul. Mais le sens démontré ici suffit déjà à régler les trois problèmes classiques.

Propriété 4.6 (les trois problèmes grecs) :

- La **duplication du cube** est impossible : $\sqrt[3]{2}$ n'est pas constructible.
- La **trisection de l'angle** est impossible en général : l'angle de 60° n'est pas trisectable.
- La **quadrature du cercle** est impossible : $\sqrt{\pi}$ n'est pas constructible.

∘ *Démonstration :* **Duplication.** Doubler le cube revient à construire l'arête $\sqrt[3]{2}$ d'un cube de volume 2. Or $\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=3$, qui n'est pas une puissance de 2 : le théorème 4.5 l'interdit.

Trisection. Trisecter l'angle de 60° revient à construire $\cos 20°$, l'angle de 60° étant lui-même constructible puisque $\cos 60°=\frac{1}{2}$. La formule $\cos 3\theta=4\cos^3\theta-3\cos\theta$ appliquée à $\theta=20°$ donne :

$$\tfrac{1}{2}=4\cos^3 20°-3\cos 20° \qquad \text{soit} \qquad 8x^3-6x-1=0 \quad \text{où } x=\cos 20°$$

Le polynôme $8X^3-6X-1$ est irréductible sur $\mathbb{Q}$: de degré 3, il suffit de vérifier qu'il n'a pas de racine rationnelle. Les candidats de la propriété 3.8 sont $\pm1,\pm\frac{1}{2},\pm\frac{1}{4},\pm\frac{1}{8}$, et l'on vérifie qu'aucun n'annule le polynôme — par exemple $8\left(\frac{1}{2}\right)^3-6\cdot\frac{1}{2}-1=1-3-1=-3\neq 0$. Donc $[\mathbb{Q}(\cos 20°):\mathbb{Q}]=3$, et $\cos 20°$ n'est pas constructible.

Quadrature. Construire un carré de même aire qu'un disque de rayon 1 demande de construire $\sqrt{\pi}$. Si $\sqrt{\pi}$ était constructible, π le serait aussi, donc serait algébrique sur $\mathbb{Q}$. Or π est transcendant : ce théorème, dû à **Lindemann** en 1882, est ici *admis*, sa démonstration relevant de l'analyse — elle repose sur des estimations d'intégrales et sur le théorème d'Hermite-Lindemann, et non sur les méthodes algébriques de ce cours. □

Remarque : Il vaut la peine de mesurer le renversement opéré. Les Grecs cherchaient une construction ; vingt-quatre siècles durant, on a cherché une construction. La réponse ne vient pas de la géométrie mais d'un comptage de dimensions : *trois ne divise aucune puissance de deux.* C'est le premier exemple, dans ce cours, d'un problème géométrique tranché par un invariant algébrique — et le chapitre 7 en donnera un second, plus fin, avec les polygones réguliers.

Chapitre 5

Séparabilité, normalité et corps finis

Deux pathologies peuvent empêcher une extension de se prêter à la théorie de Galois. La première est le défaut de *séparabilité* : un polynôme peut avoir des racines multiples, auquel cas il n'y a pas assez de racines pour les permuter. La seconde est le défaut de *normalité* : une extension peut contenir une racine d'un polynôme irréductible sans contenir les autres, auquel cas les permutations envisagées sortent du corps. Ce chapitre identifie ces deux obstructions, montre qu'elles disparaissent en caractéristique nulle et sur les corps finis, et démontre le théorème de l'élément primitif. Le décor sera alors planté.

5.1 Séparabilité

Définition : La **dérivée formelle** de $P = \sum_k a_k X^k \in K[X]$ est $P' = \sum_{k\geqslant 1} k\, a_k X^{k-1}$, où $k\, a_k$ désigne la somme de k copies de a_k dans K.

Un polynôme P est **séparable** s'il n'a que des racines simples dans un corps de décomposition.

Remarque : La dérivée formelle est définie sans limite ni analyse : c'est une opération purement algébrique, qui a un sens sur n'importe quel corps, y compris fini. On vérifie sans peine, par linéarité et sur les monômes, qu'elle satisfait $(PQ)' = P'Q + PQ'$.

Propriété 5.1 : Soit $P \in K[X]$ non constant et L un corps de décomposition de P. Alors P est séparable si et seulement si $\operatorname{pgcd}(P\,;P') = 1$ dans $K[X]$.

∘ *Démonstration :* Remarquons d'abord que le pgcd ne change pas lorsqu'on agrandit le corps : il est caractérisé par l'algorithme d'Euclide, qui n'utilise que des divisions euclidiennes, et celles-ci sont uniques donc identiques dans $K[X]$ et dans $L[X]$.

Supposons que P admette une racine multiple $\alpha \in L$, c'est-à-dire qu'il existe $Q \in L[X]$ tel que $P = (X-\alpha)^2 Q$. Alors :

$$P' = 2(X-\alpha)Q + (X-\alpha)^2 Q' = (X-\alpha)\left(2Q + (X-\alpha)Q'\right)$$

donc α est racine commune de P et P', et $(X-\alpha)$ divise leur pgcd, qui n'est donc pas 1.

Réciproquement, supposons toutes les racines simples : $P = c\prod_{i=1}^{n}(X-\alpha_i)$ avec les α_i deux à deux distincts. En dérivant, $P' = c\sum_i \prod_{j\neq i}(X-\alpha_j)$, donc $P'(\alpha_i) = c\prod_{j\neq i}(\alpha_i-\alpha_j) \neq 0$. Aucune racine de P n'annule P' ; comme les diviseurs communs de P et P' sont des produits de facteurs $(X-\alpha_i)$, le pgcd vaut 1. □

Exemple : **Un cas séparable.** Prenons $P = X^3 - 2$ dans $\mathbb{Q}[X]$, de dérivée $P' = 3X^2$. Appliquons l'algorithme d'Euclide, qui ne demande à aucun moment de connaître les racines :

$$X^3 - 2 = \frac{X}{3} \times 3X^2 \;-\; 2$$

Le reste vaut -2, constante non nulle. À l'étape suivante, la division de $3X^2$ par -2 tombe juste, et le dernier reste non nul est -2 : le pgcd, que l'on prend unitaire, vaut donc 1.

La propriété 5.1 conclut que P est séparable, et l'on peut le vérifier directement : ses racines $\sqrt[3]{2}$, $\mathrm{j}\sqrt[3]{2}$ et $\mathrm{j}^2\sqrt[3]{2}$ sont bien deux à deux distinctes. Mais c'est précisément l'intérêt du critère de n'avoir eu besoin ni de les calculer ni même de sortir de $\mathbb{Q}$.

Exemple : **Un cas non séparable.** Prenons $P = X^3 - 3X + 2$ dans $\mathbb{Q}[X]$, de dérivée $P' = 3X^2 - 3$. La division euclidienne donne :

$$X^3 - 3X + 2 = \frac{X}{3} \times \left(3X^2 - 3\right) \;+\; (-2X + 2)$$

car $\frac{X}{3}\left(3X^2-3\right) = X^3 - X$, et $P - \left(X^3 - X\right) = -2X + 2$. On poursuit avec $3X^2 - 3 = 3(X-1)(X+1)$ et $-2X+2 = -2(X-1)$: la division est exacte, de reste nul. Le dernier reste non nul étant $-2(X-1)$, on obtient :

$$\operatorname{pgcd}\left(P\,;P'\right) = X - 1 \;\neq\; 1$$

La propriété 5.1 conclut que P n'est pas séparable. La factorisation $P = (X-1)^2(X+2)$ le confirme : la racine 1 est double, et c'est elle que le pgcd a détectée. On retiendra ce point : le pgcd ne se contente pas de répondre par oui ou par non, il *exhibe* les racines multiples, chacune avec une multiplicité diminuée de un.

Remarque : Ces deux exemples ne montrent pas encore tout le phénomène. En caractéristique nulle, seul un polynôme *réductible* peut être inséparable, comme le second exemple — la propriété suivante le démontrera. En caractéristique p, en revanche, un irréductible peut l'être, et la cause en est toute différente : la dérivée peut s'annuler identiquement.

Le même polynôme $X^3 - 2$, vu cette fois dans $\mathbb{F}_3[X]$, l'illustre : sa dérivée $3X^2$ y est *nulle*, donc $\operatorname{pgcd}(P\,;P') = \operatorname{pgcd}(P\,;0) = P \neq 1$, et P n'est pas séparable. Le rêve du débutant le confirme : $X^3 - 2 = X^3 + 1 = (X+1)^3$ dans $\mathbb{F}_3[X]$, une unique racine de multiplicité 3. Un polynôme séparable sur $\mathbb{Q}$ peut donc cesser de l'être après réduction modulo un nombre premier.

Propriété 5.2 : Soit $P \in K[X]$ irréductible. Alors P est séparable si et seulement si $P' \neq 0$. En particulier :

- si $\operatorname{car}(K) = 0$, tout polynôme irréductible est séparable ;
- si $\operatorname{car}(K) = p$, un irréductible P est inséparable si et seulement s'il existe Q tel que $P = Q\left(X^p\right)$.

∘ *Démonstration :* Le pgcd de P et P' divise P, irréductible : à constante près, il vaut 1 ou P. S'il vaut P, alors $P \mid P'$; or $\deg P' < \deg P$, ce qui force $P' = 0$. Réciproquement, si $P' = 0$ le pgcd vaut P, de degré $\geqslant 1$, et P n'est pas séparable.

Écrivons $P = \sum_k a_k X^k$ et $n = \deg P \geqslant 1$. Si $\operatorname{car}(K) = 0$, le coefficient dominant de P' vaut $n\,a_n$, non nul puisque $a_n \neq 0$ et que $n \cdot 1_K \neq 0$ en caractéristique nulle ; donc $P' \neq 0$.

Si $\operatorname{car}(K) = p$, l'égalité $P' = 0$ signifie $k\,a_k = 0$ pour tout k, c'est-à-dire $a_k = 0$ dès que $p \nmid k$: seuls survivent les monômes d'exposant multiple de p, ce qui s'écrit $P = Q\left(X^p\right)$. □

Exemple : Sur $K = \mathbb{F}_p(T)$, corps des fractions rationnelles en une indéterminée T, considérons $P = X^p - T$. Il est irréductible : dans une extension où il admet une racine θ, on a $\theta^p = T$ et, par le rêve du débutant, $P = X^p - \theta^p = (X-\theta)^p$; un diviseur unitaire strict de P dans $K[X]$ serait donc de la forme $(X-\theta)^m$ avec $1 \leqslant m < p$, et son terme constant $\pm\theta^m$ appartiendrait à K, d'où $\theta^m \in K$; comme $\operatorname{pgcd}(m\,;p) = 1$, une relation de Bézout $um + vp = 1$ donnerait $\theta = (\theta^m)^u\,(\theta^p)^v \in K$, ce qui est faux car T n'est pas une puissance p-ième dans $\mathbb{F}_p(T)$.

Ce polynôme irréductible n'a donc *qu'une seule* racine, de multiplicité p : il est inséparable. C'est le contre-exemple standard, et il montre que la séparabilité est une hypothèse réelle et non une clause de style.

Définition : Un corps K est **parfait** si tout polynôme irréductible de $K[X]$ est séparable.

Exemple : Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont parfaits, ainsi que tout corps de caractéristique nulle : c'est la propriété 5.2. Les corps finis — les $\mathbb{F}_p$, le corps $\mathbb{F}_4$ du chapitre 3, et tous ceux que classera le théorème 5.3 — le sont également, comme la propriété suivante va l'établir.

Le corps $\mathbb{F}_p(T)$, lui, n'est *pas* parfait : l'exemple précédent y a exhibé le polynôme irréductible $X^p - T$, qui n'a qu'une racine de multiplicité p. Les corps non parfaits sont donc rares — il faut à la fois une caractéristique p et un corps infini —, mais ils existent, et c'est pour eux que toute la théorie de la séparabilité a été bâtie.

Propriété 5.3 : Tout corps de caractéristique nulle est parfait. Tout corps fini est parfait.

∘ *Démonstration :* Le premier point est la propriété 5.2. Soit maintenant K fini de caractéristique p. Le morphisme de Frobenius $\mathrm{Frob} : x \mapsto x^p$ est injectif — son noyau est un idéal du corps K ne contenant pas 1 — donc bijectif puisque K est fini. Ainsi tout élément de K est une puissance p-ième.

Soit $P \in K[X]$ irréductible et non séparable : par la propriété 5.2, il existe des scalaires $a_k \in K$ tels que $P = \sum_k a_k X^{pk}$. Le Frobenius étant surjectif, écrivons $a_k = b_k^p$ avec $b_k \in K$; alors, par le rêve du débutant appliqué à l'anneau $K[X]$:

$$P = \sum_k b_k^p \left(X^k\right)^p = \left(\sum_k b_k X^k\right)^p$$

ce qui contredit l'irréductibilité de P. Donc K est parfait. □

5.2 Plongements et degré séparable

Nous admettons ici le résultat suivant, dont la démonstration repose sur le lemme de Zorn et non sur les techniques de ce cours : *tout corps K possède une* ***clôture algébrique*** $\overline{K}$*, c'est-à-dire une extension algébrique dans laquelle tout polynôme non constant est scindé, et deux clôtures algébriques de K sont isomorphes au-dessus de K*. La difficulté contournée est purement ensembliste : il faut construire d'un coup un corps contenant les racines de *tous* les polynômes, ce qui suppose un argument de maximalité. Toutes les extensions considérées désormais sont supposées contenues dans une clôture algébrique fixée.

Définition : Soit L/K une extension finie. Un **K-plongement** de L est un morphisme de corps $\varphi : L \to \overline{K}$ tel que $\varphi_{|K} = \mathrm{id}_K$. On note $[L : K]_s$ le nombre de K-plongements de L, appelé **degré séparable**.

Un élément α algébrique sur K est **séparable sur K** si $\mu_{\alpha,K}$ est séparable ; l'extension L/K est **séparable** si tous ses éléments le sont.

Exemple : Prenons $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt[3]{2})$, de degré 3, avec $\overline{\mathbb{Q}} \subset \mathbb{C}$. Un $\mathbb{Q}$-plongement de L est déterminé par l'image de $\sqrt[3]{2}$, qui doit être une racine de $X^3 - 2$: il y en a trois, à savoir $\sqrt[3]{2}$, $\mathrm{j}\sqrt[3]{2}$ et $\mathrm{j}^2\sqrt[3]{2}$. Donc $[L : \mathbb{Q}]_s = 3 = [L : \mathbb{Q}]$, et l'extension est séparable — ce qui n'a rien d'étonnant en caractéristique nulle.

On notera que seul le premier de ces trois plongements a son image dans L : les deux autres en sortent. C'est là toute la différence entre *plongement* et *automorphisme*, et c'est elle qui, au chapitre 6, séparera la séparabilité de la normalité.

À l'opposé, avec $K = \mathbb{F}_p(S)$ et $L = K(\theta)$ où $\theta^p = S$, un K-plongement envoie θ sur une racine de $X^p - S = (X - \theta)^p$, c'est-à-dire sur θ : il n'y en a qu'un seul. Ici $[L : K]_s = 1 < p = [L : K]$, et l'extension n'est pas séparable.

Propriété 5.4 : Soit $L = K(\alpha)$ avec α algébrique de polynôme minimal μ. Alors $[L : K]_s$ est le nombre de racines *distinctes* de μ dans $\overline{K}$. En particulier $[L : K]_s \leqslant [L : K]$, avec égalité si et seulement si α est séparable sur K.

∘ *Démonstration :* Un K-plongement φ de $K(\alpha)$ est entièrement déterminé par $\varphi(\alpha)$, puisque tout élément de $K(\alpha)$ s'écrit $P(\alpha)$ avec $P \in K[X]$ et que $\varphi(P(\alpha)) = P(\varphi(\alpha))$. De plus $\mu(\varphi(\alpha)) = \varphi(\mu(\alpha)) = 0$: l'image de α est une racine de μ.

Réciproquement, pour chaque racine β de μ dans $\overline{K}$, la propriété 4.4, appliquée à $\sigma = \mathrm{id}_K$, fournit un unique K-morphisme $K(\alpha) \to K(\beta) \subseteq \overline{K}$ envoyant α sur β. La correspondance $\varphi \mapsto \varphi(\alpha)$ est donc une bijection sur l'ensemble des racines distinctes de μ. Leur nombre est au plus $\deg \mu = [L : K]$, avec égalité exactement lorsque μ est séparable. □

Théorème 5.1 : multiplicativité et critère :
Soient $K \subseteq L \subseteq M$ des extensions finies. Alors :

$$[M : K]_s = [M : L]_s \times [L : K]_s \qquad \text{et} \qquad [L : K]_s \leqslant [L : K]$$

avec égalité dans la seconde si et seulement si L/K est séparable.

∘ *Démonstration :* **Multiplicativité.** Tout K-plongement ψ de M se restreint en un K-plongement de L. Réciproquement, fixons un K-plongement φ de L ; le théorème 4.4 assure que φ se prolonge à M — on applique le prolongement successivement aux générateurs de M sur L, chaque étape relevant de la propriété 4.4 —, et le nombre de prolongements de φ ne dépend pas de φ : il vaut $[M : L]_s$, car φ transporte les polynômes minimaux sur L en polynômes ayant le même nombre de racines distinctes. En regroupant les plongements de M selon leur restriction à L, on obtient la formule.

Inégalité. Écrivons $L = K(\alpha_1 ; \dots ; \alpha_r)$ et posons $L_i = K(\alpha_1 ; \dots ; \alpha_i)$. Par la propriété 5.4, $[L_{i+1} : L_i]_s \leqslant [L_{i+1} : L_i]$ à chaque étage ; on multiplie.

Cas d'égalité. Supposons $[L : K]_s = [L : K]$ et soit $\alpha \in L$. La multiplicativité donne :

$$[L : K(\alpha)]_s \, [K(\alpha) : K]_s = [L : K(\alpha)] \, [K(\alpha) : K]$$

Chacun des deux facteurs de gauche étant inférieur au facteur correspondant à droite, l'égalité globale impose l'égalité de chacun ; donc $[K(\alpha) : K]_s = [K(\alpha) : K]$ et α est séparable par la propriété 5.4. Ainsi L/K est séparable.

Réciproquement, supposons L/K séparable et écrivons $L = K(\alpha_1 ; \dots ; \alpha_r)$. Chaque α_{i+1} est séparable sur K, donc sur L_i : en effet μ_{α_{i+1},L_i} divise $\mu_{\alpha_{i+1},K}$, qui est à racines simples. La propriété 5.4 donne alors l'égalité à chaque étage, et le produit conclut. □

Remarque : En caractéristique nulle, la propriété 5.3 rend toute extension finie séparable, et l'on a toujours $[L : K]_s = [L : K]$. Le lecteur qui ne s'intéresse qu'aux sous-corps de $\mathbb{C}$ peut donc considérer ce paragraphe comme une simple vérification ; il devient en revanche indispensable dès que l'on travaille en caractéristique p, par exemple sur les corps de fonctions.

5.3 Extensions normales

Définition : Une extension algébrique L/K est **normale** si tout polynôme irréductible de $K[X]$ possédant une racine dans L est scindé dans $L[X]$.

Théorème 5.2 : caractérisation des extensions normales :
Soit L/K une extension *finie*. Les assertions suivantes sont équivalentes :
- L/K est normale ;
- L est le corps de décomposition sur K d'un polynôme de $K[X]$;
- tout K-plongement $\varphi : L \to \overline{K}$ vérifie $\varphi(L) = L$.

∘ *Démonstration :* **Normale ⇒ corps de décomposition.** Écrivons $L = K(\alpha_1 ; \dots ; \alpha_r)$ et posons $P = \mu_{\alpha_1,K} \cdots \mu_{\alpha_r,K}$. Chaque facteur est irréductible et a une racine dans L, donc est scindé dans L par normalité ; ainsi P est scindé, et L est engendré sur K par les α_i, qui sont des racines de P. Donc L est le corps de décomposition de P.

Corps de décomposition ⇒ stabilité par plongement. Soit L le corps de décomposition de $P \in K[X]$, de racines $\beta_1, \dots, \beta_n$, et soit φ un K-plongement de L. Comme P est à coefficients dans K, on a $P(\varphi(\beta_i)) = \varphi(P(\beta_i)) = 0$: φ permute les racines de P. Or $L = K(\beta_1 ; \dots ; \beta_n)$, donc $\varphi(L) = K(\varphi(\beta_1) ; \dots) = L$.

Stabilité ⇒ normale. Soit $Q \in K[X]$ irréductible ayant une racine $\alpha \in L$, et soit $\beta \in \overline{K}$ une autre racine de Q. La propriété 4.4 fournit un K-isomorphisme $K(\alpha) \to K(\beta)$ envoyant α sur β, que le théorème 4.4 prolonge en un K-plongement φ de L dans $\overline{K}$. Par hypothèse $\varphi(L) = L$, donc $\beta = \varphi(\alpha) \in L$. Toutes les racines de Q sont dans L : il y est scindé. □

Exemple : L'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est *pas* normale : le polynôme irréductible $X^3 - 2$ y possède la racine $\sqrt[3]{2}$, mais ses deux autres racines sont complexes non réelles alors que $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$. En revanche $\mathbb{Q}(\sqrt[3]{2} ; \mathrm{j})/\mathbb{Q}$ est normale, comme corps de décomposition de $X^3 - 2$.

La normalité n'est pas non plus transitive. Les extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ et $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ sont toutes deux normales, chacune étant de degré 2 donc corps de décomposition d'un polynôme du second degré. Pourtant $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ne l'est pas : le polynôme irréductible $X^4 - 2$ y possède la racine $\sqrt[4]{2}$ mais non la racine $\mathrm{i}\sqrt[4]{2}$, qui n'est pas réelle. C'est le pendant exact de la non-transitivité de la distinction dans les groupes, signalée au chapitre 2 ; le chapitre 6 expliquera pourquoi ce n'est pas une coïncidence.

5.4 Corps finis

Théorème 5.3 : classification des corps finis :
Soit F un corps fini. Alors $|F| = p^n$ où $p = \mathrm{car}(F)$ est premier et $n = [F : \mathbb{F}_p]$. Réciproquement, pour tout premier p et tout $n \geqslant 1$, il existe un corps à p^n éléments, unique à isomorphisme près : c'est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_{p^n}$.

∘ *Démonstration :* **Cardinal.** La caractéristique de F ne peut être nulle, sinon F contiendrait $\mathbb{Q}$, infini ; elle vaut donc un premier p, et F contient $\mathbb{F}_p$. Comme F est fini, $n = [F : \mathbb{F}_p]$ est fini et $F \simeq \mathbb{F}_p^n$ comme espace vectoriel, d'où $|F| = p^n$.

Existence. Soit $q = p^n$ et L le corps de décomposition de $P = X^q - X$ sur $\mathbb{F}_p$. Posons $F = \{x \in L \, ; \, x^q = x\}$, c'est-à-dire l'ensemble des racines de P. C'est un sous-corps de L : il contient 0 et 1, il est stable par produit et inverse, et il est stable par somme grâce au rêve du débutant itéré n fois, qui donne $(x+y)^q = x^q + y^q$. Par ailleurs $P' = q\,X^{q-1} - 1 = -1$, puisque $q = p^n$ est nul dans $\mathbb{F}_p$; donc $\mathrm{pgcd}(P ; P') = 1$ et P a exactement q racines distinctes. Ainsi $|F| = q$, et $F = L$ puisque L est engendré par les racines de P.

Unicité. Soit F un corps à q éléments. Le groupe $(F^* ; \times)$ est d'ordre $q - 1$, donc $x^{q-1} = 1$ pour tout $x \neq 0$ par le théorème de Lagrange, d'où $x^q = x$ pour tout $x \in F$, y compris 0. Le polynôme $X^q - X$, de degré q, admet donc les q éléments de F pour racines : il est scindé dans F, et F est engendré par ses racines. C'est donc un corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$, et le théorème 4.4 donne l'unicité à isomorphisme près. □

Remarque : **Ce que signifie la notation $\mathbb{F}_q$.** Le théorème légitime enfin l'emploi d'un article défini : on peut parler *du* corps à q éléments, puisque tous sont isomorphes. La notation $\mathbb{F}_q$ désigne ainsi une classe d'isomorphisme plutôt qu'un ensemble précis, et une égalité comme $\mathbb{F}_4 = \mathbb{F}_2[X]/\left(X^2+X+1\right)$ doit se lire « ce quotient est *un modèle* de $\mathbb{F}_4$ ». Elle est cohérente avec la notation du chapitre 3 : pour $q = p$ premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps à p éléments, donc un modèle de $\mathbb{F}_p$. Mais pour $q = p^n$ avec $n \geqslant 2$, l'anneau $\mathbb{Z}/q\mathbb{Z}$ n'est jamais un corps, et $\mathbb{F}_q$ n'a rien à voir avec lui.

L'unicité à isomorphisme près n'est pas une banalité : des constructions différentes fournissent des corps différents *en tant qu'ensembles*. Sur $\mathbb{F}_3$, les polynômes X^2+1 et Y^2+Y+2 sont tous deux irréductibles, faute de racine dans $\mathbb{F}_3$, et fournissent deux corps à neuf éléments :

$$L_1 = \mathbb{F}_3[X]/\left(X^2+1\right) \qquad \text{et} \qquad L_2 = \mathbb{F}_3[Y]/\left(Y^2+Y+2\right)$$

Le théorème affirme qu'ils sont isomorphes, et l'on peut exhiber l'isomorphisme. Notons i la classe de X dans L_1, de sorte que $\mathrm{i}^2 = -1$; il suffit de trouver dans L_1 une racine de Y^2+Y+2. Or $1+\mathrm{i}$ convient :

$$(1+\mathrm{i})^2 + (1+\mathrm{i}) + 2 = 2\mathrm{i} + 1 + \mathrm{i} + 2 = 3 + 3\mathrm{i} = 0$$

puisque $(1+\mathrm{i})^2 = 1 + 2\mathrm{i} + \mathrm{i}^2 = 2\mathrm{i}$ et que $3 = 0$ en caractéristique 3. La propriété 4.4 fournit alors un isomorphisme $L_2 \to L_1$ envoyant la classe de Y sur $1+\mathrm{i}$. Les deux corps sont donc deux réalisations d'un même objet, $\mathbb{F}_9$.

Théorème 5.4 : cyclicité du groupe multiplicatif :
Le groupe multiplicatif F^* d'un corps fini est cyclique.

∘ *Démonstration :* Posons $m = |F^*|$ et, pour chaque diviseur d de m, notons $\psi(d)$ le nombre d'éléments de F^* d'ordre exactement d. Comme l'ordre de tout élément divise m :

$$\sum_{d|m} \psi(d) = m$$

Montrons que $\psi(d) \leqslant \varphi(d)$, où φ désigne l'indicatrice d'Euler. Si $\psi(d) = 0$, c'est acquis. Sinon, soit $x \in F^*$ d'ordre d ; le sous-groupe $\langle x\rangle$ est d'ordre d et tous ses éléments annulent $X^d - 1$. Or ce polynôme a au plus d racines dans le corps F (propriété 3.6) : *tout* élément d'ordre d est donc dans $\langle x\rangle$. Or un groupe cyclique d'ordre d possède exactement $\varphi(d)$ générateurs, c'est-à-dire $\varphi(d)$ éléments d'ordre d — les x^k avec k premier à d. Donc $\psi(d) = \varphi(d)$ dans ce cas, et $\psi(d) \leqslant \varphi(d)$ toujours.

Enfin l'identité classique $\sum_{d|m} \varphi(d) = m$, que l'on obtient en classant les entiers de $[\![1\,;m]\!]$ selon leur pgcd avec m, donne :

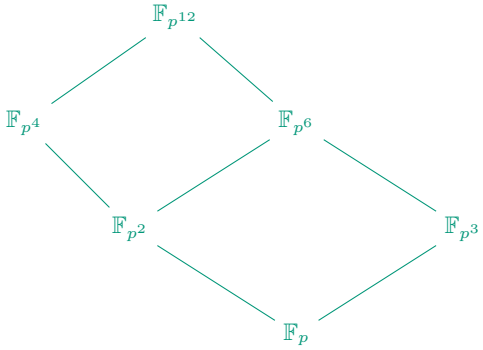
$$m = \sum_{d|m} \psi(d) \leqslant \sum_{d|m} \varphi(d) = m$$

L'inégalité est donc une égalité terme à terme, et en particulier $\psi(m) = \varphi(m) \geqslant 1$: il existe un élément d'ordre m, qui engendre F^*. □

Propriété 5.5 : Soit $q = p^n$. Les sous-corps de $\mathbb{F}_q$ sont exactement les $\mathbb{F}_{p^d}$ pour $d \mid n$, et il y en a un seul pour chaque diviseur. De plus $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^e}$ si et seulement si $d \mid e$.

∘ *Démonstration :* Si F' est un sous-corps de $\mathbb{F}_q$, il est de cardinal p^d avec $d = [F' : \mathbb{F}_p]$, et la multiplicativité des degrés donne $n = [\mathbb{F}_q : F'] \times d$, donc $d \mid n$.

Réciproquement, soit $d \mid n$. Alors $p^d - 1$ divise $p^n - 1$: en écrivant $n = dk$, on a $p^n - 1 = \left(p^d\right)^k - 1 = \left(p^d - 1\right)\left(\left(p^d\right)^{k-1} + \cdots + 1\right)$. Le groupe $\mathbb{F}_q^*$ étant cyclique d'ordre $p^n - 1$, il possède un unique sous-groupe d'ordre $p^d - 1$ (chapitre 1), constitué des solutions de $x^{p^d-1} = 1$. En lui adjoignant 0, on obtient l'ensemble $F' = \left\{x \;;\; x^{p^d} = x\right\}$, qui est un sous-corps de cardinal p^d par le même argument de Frobenius que ci-dessus, et c'est le seul possible puisque ses éléments sont déterminés comme racines de $X^{p^d} - X$. □



Le treillis des sous-corps de $\mathbb{F}_{p^{12}}$ reproduit celui des diviseurs de 12, à l'endroit cette fois : un sous-corps par diviseur, emboîtés selon la divisibilité des exposants.

On comparera cette figure au treillis des sous-groupes de $\mathbb{Z}/12\mathbb{Z}$ du chapitre 1 : les deux ont la même forme, et le chapitre 6 montrera que c'est la correspondance de Galois qui les relie, le groupe $\mathrm{Gal}\left(\mathbb{F}_{p^{12}}/\mathbb{F}_p\right)$ étant précisément cyclique d'ordre 12.

Exemple : Voici une application inattendue. Le polynôme X^4+1 est irréductible sur $\mathbb{Q}$ — c'est Φ_8, et l'on peut appliquer Eisenstein après $X \mapsto X+1$ — mais il est *réductible modulo tout nombre premier*. En effet, pour $p=2$ on a $X^4+1=(X+1)^4$. Pour p impair, l'entier $p^2-1=(p-1)(p+1)$ est produit de deux entiers pairs consécutifs, donc divisible par 8 ; le groupe cyclique $\mathbb{F}_{p^2}^*$, d'ordre p^2-1, contient donc un élément d'ordre 8, et par suite les huit racines de X^8-1. Or X^4+1 divise X^8-1 : toutes ses racines vivent dans $\mathbb{F}_{p^2}$, donc sont de degré au plus 2 sur $\mathbb{F}_p$, et sa factorisation en irréductibles sur $\mathbb{F}_p$ ne comporte que des facteurs de degré 1 ou 2.

On vérifie : modulo 3, $X^4+1=\left(X^2+X+2\right)\left(X^2+2X+2\right)$; modulo 5, $X^4+1=\left(X^2+2\right)\left(X^2+3\right)$; modulo 7, $X^4+1=\left(X^2+3X+1\right)\left(X^2+4X+1\right)$. L'irréductibilité est donc une propriété globale que nulle réduction locale ne détecte : voilà qui invite à la prudence avec le critère de réduction modulo p, qui ne fournit qu'une condition suffisante.

5.5 Le théorème de l'élément primitif

Théorème 5.5 : élément primitif :
Toute extension finie séparable L/K est **monogène** : il existe $\gamma \in L$ tel que $L=K(\gamma)$. En particulier, c'est le cas de toute extension finie en caractéristique nulle, et de toute extension de corps finis.

∘ *Démonstration :* **Cas où K est fini.** Alors L est fini, et L^* est cyclique par le théorème 5.4 ; un générateur γ de L^* engendre *a fortiori* L comme corps sur K.

Cas où K est infini. Par récurrence sur le nombre de générateurs, il suffit de traiter $L=K(\alpha\,;\beta)$ et de montrer qu'il existe $c \in K$ tel que $L=K(\gamma)$ avec $\gamma=\alpha+c\beta$.

Notons μ et ν les polynômes minimaux de α et β sur K, de racines respectives $\alpha=\alpha_1,\dots,\alpha_m$ et $\beta=\beta_1,\dots,\beta_n$ dans $\overline{K}$, toutes distinctes par séparabilité. Comme K est infini, on peut choisir $c \in K$ évitant les valeurs $\frac{\alpha_i-\alpha}{\beta-\beta_j}$ pour $j \neq 1$ — il n'y en a qu'un nombre fini. Cela garantit :

$$\alpha+c\beta \neq \alpha_i+c\beta_j \qquad \text{pour tout } i \text{ et tout } j \neq 1$$

Posons $\gamma=\alpha+c\beta$ et $M=K(\gamma)\subseteq L$. Considérons dans $M[X]$ les deux polynômes :

$$\nu(X) \qquad \text{et} \qquad R(X)=\mu(\gamma-cX)$$

Tous deux annulent β : le premier par définition, le second car $\gamma-c\beta=\alpha$ et $\mu(\alpha)=0$. Leur pgcd dans $M[X]$ est donc divisible par $X-\beta$. Réciproquement, une racine commune serait un β_j tel que $\gamma-c\beta_j$ soit un α_i, c'est-à-dire $\alpha+c\beta=\alpha_i+c\beta_j$; le choix de c interdit cela pour $j \neq 1$. Le pgcd vaut donc exactement $X-\beta$ — les racines de ν étant simples, la multiplicité ne peut excéder 1.

Or ce pgcd est calculé dans $M[X]$ par l'algorithme d'Euclide : ses coefficients sont dans M. Donc $\beta \in M$, puis $\alpha=\gamma-c\beta \in M$, et finalement $L=K(\alpha\,;\beta)\subseteq M\subseteq L$, soit $L=K(\gamma)$. □

Exemple : Reprenons $L=\mathbb{Q}\left(\sqrt{2}\,;\sqrt{3}\right)$ et posons $\gamma=\sqrt{2}+\sqrt{3}$, ce qui correspond à $c=1$. Nous avons vu que $[\mathbb{Q}(\gamma):\mathbb{Q}]=4=[L:\mathbb{Q}]$, donc $L=\mathbb{Q}(\gamma)$: la conclusion du théorème est ici vérifiable directement. On peut même exprimer les générateurs : de $\gamma^3=11\sqrt{2}+9\sqrt{3}$ et $\gamma=\sqrt{2}+\sqrt{3}$, on tire par combinaison linéaire :

$$\sqrt{2}=\frac{\gamma^3-9\gamma}{2} \qquad \text{et} \qquad \sqrt{3}=\frac{11\gamma-\gamma^3}{2}$$

On vérifie numériquement : $\gamma \approx 3{,}1463$, $\gamma^3 \approx 31{,}1448$, et $\frac{31{,}1448-9\times 3{,}1463}{2} \approx 1{,}4142$, qui est bien $\sqrt{2}$.

Remarque : Le théorème de l'élément primitif est ce qui rendra la théorie de Galois maniable : au lieu de raisonner sur un corps engendré par plusieurs racines, on pourra toujours se ramener à un seul générateur, dont le polynôme minimal porte à lui seul toute l'information. C'est exactement le *lemme II* du mémoire de Galois, qui affirmait déjà, dans le langage de 1831, l'existence d'une fonction des racines prenant des valeurs distinctes sous toutes les permutations.

Chapitre 6

La correspondance de Galois

Tout est en place. D'un côté, une extension L/K et le treillis de ses corps intermédiaires ; de l'autre, un groupe fini et le treillis de ses sous-groupes. Ce chapitre établit que, sous les hypothèses de normalité et de séparabilité, ces deux treillis sont *le même*, lu à l'endroit d'un côté et à l'envers de l'autre. C'est le théorème fondamental de la théorie de Galois. Sa démonstration repose sur un lemme d'algèbre linéaire d'apparence modeste — l'indépendance des caractères, due à **Dedekind** — et sur un théorème de **Artin** qui, en 1942, a débarrassé la théorie de tout recours aux calculs sur les racines.

6.1 Le groupe de Galois

Définition : Soit L/K une extension. Le **groupe des K-automorphismes** de L est :

$$\mathrm{Aut}(L/K) = \left\{\sigma : L \to L \text{ isomorphisme de corps } ;\ \sigma_{|K} = \mathrm{id}_K\right\}$$

muni de la composition. Plus généralement, pour un ensemble H d'automorphismes de L — en pratique un sous-groupe de $\mathrm{Aut}(L/K)$, ou un groupe quelconque d'automorphismes de L —, le **corps fixe** de H est l'ensemble des éléments de L que *tous* les éléments de H laissent inchangés :

$$L^H = \{x \in L\ ;\ \forall \sigma \in H,\ \sigma(x) = x\}$$

Remarque : Le corps fixe est bien un corps : il contient 0 et 1, que tout morphisme de corps fixe, et il est stable par les quatre opérations. En effet, si $\sigma(x) = x$ et $\sigma(y) = y$ pour tout $\sigma \in H$, alors $\sigma(x+y) = \sigma(x)+\sigma(y) = x+y$, et de même pour le produit, l'opposé et l'inverse. Lorsque $H \leqslant \mathrm{Aut}(L/K)$, le corps fixe contient de plus K, puisque les éléments de H fixent K par définition. Les deux applications $H \mapsto L^H$ et $M \mapsto \mathrm{Aut}(L/M)$ vont donc dans des sens opposés, et toute la difficulté sera de montrer qu'elles sont réciproques l'une de l'autre.

Exemple : Pour $L = \mathbb{C}$ et $K = \mathbb{R}$, un $\mathbb{R}$-automorphisme σ vérifie $\sigma(\mathrm{i})^2 = \sigma\left(\mathrm{i}^2\right) = -1$, donc $\sigma(\mathrm{i}) = \pm\mathrm{i}$: il y a au plus deux automorphismes, l'identité et la conjugaison complexe, qui en sont bien deux. Ainsi $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$, et $[\mathbb{C} : \mathbb{R}] = 2$: le compte est exact.

Exemple : Pour $L = \mathbb{Q}\left(\sqrt[3]{2}\right)$ et $K = \mathbb{Q}$, un $\mathbb{Q}$-automorphisme σ envoie $\sqrt[3]{2}$ sur une racine de $X^3 - 2$ appartenant à L ; or $L \subset \mathbb{R}$ ne contient qu'une seule de ces trois racines. Donc $\sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}$ et $\sigma = \mathrm{id}$. Ici $|\mathrm{Aut}(L/K)| = 1$ alors que $[L : K] = 3$: le compte est mauvais, et le coupable est le défaut de normalité relevé au chapitre 5.

Théorème 6.1 : indépendance des caractères, Dedekind :
Soient M un corps, G un groupe, et $\chi_1, \ldots, \chi_n$ des morphismes de groupes deux à deux distincts de G dans M^*. Alors la famille $(\chi_1, \ldots, \chi_n)$ est libre sur M dans l'espace des applications de G dans M.

∘ *Démonstration :* Raisonnons par l'absurde et considérons une relation de liaison non triviale $\sum_{i=1}^r \lambda_i\chi_i = 0$ comportant le plus petit nombre possible r de coefficients non nuls, quitte à renuméroter les caractères. On a $r \geqslant 2$: si $r = 1$, l'égalité $\lambda_1\chi_1(g) = 0$ pour tout g donnerait $\lambda_1 = 0$, puisque $\chi_1(g) \neq 0$.

Comme $\chi_1 \neq \chi_r$, il existe $h \in G$ tel que $\chi_1(h) \neq \chi_r(h)$. Écrivons, pour tout $g \in G$:

$$\sum_{i=1}^{r} \lambda_i\chi_i(hg) = \sum_{i=1}^{r} \lambda_i\chi_i(h)\chi_i(g) = 0$$

et retranchons-en $\chi_r(h)$ fois la relation initiale évaluée en g :

$$\sum_{i=1}^{r-1} \lambda_i \left(\chi_i(h) - \chi_r(h)\right) \chi_i(g) = 0$$

le terme d'indice r ayant disparu. Voilà une relation de liaison portant sur $r-1$ caractères au plus, dont le premier coefficient $\lambda_1 \left(\chi_1(h) - \chi_r(h)\right)$ est non nul. Elle contredit la minimalité de r. □

Propriété 6.2 : Soit L/K une extension finie. Alors $\mathrm{Aut}(L/K)$ est fini et :

$$|\mathrm{Aut}(L/K)| \leqslant [L : K]$$

∘ *Démonstration :* Supposons qu'il existe n automorphismes distincts $\sigma_1, \ldots, \sigma_n$ de $\mathrm{Aut}(L/K)$ avec $n > m = [L : K]$. Soit $(e_1 ; \ldots ; e_m)$ une base de L sur K. Le système linéaire de m équations à n inconnues :

$$\sum_{i=1}^{n} y_i \, \sigma_i \left(e_j\right) = 0 \qquad (1 \leqslant j \leqslant m)$$

possède, dans L, une solution non nulle $(y_1, \ldots, y_n)$, puisqu'il y a plus d'inconnues que d'équations.

Soit alors $x \in L$ quelconque, décomposé en $x = \sum_j c_j e_j$ avec $c_j \in K$. Comme chaque σ_i fixe K :

$$\sum_{i=1}^{n} y_i \, \sigma_i(x) = \sum_{i=1}^{n} y_i \sum_{j=1}^{m} c_j \sigma_i \left(e_j\right) = \sum_{j=1}^{m} c_j \underbrace{\sum_{i=1}^{n} y_i \sigma_i \left(e_j\right)}_{=\,0} = 0$$

La famille $(\sigma_1, \ldots, \sigma_n)$, vue comme famille de morphismes de L^* dans L^*, serait donc liée sur L, ce que le théorème 6.1 interdit. □

6.2 Le théorème d'Artin

Théorème 6.2 : théorème d'Artin :
Soient L un corps et G un groupe *fini* d'automorphismes de L. Posons :

$$K = L^G = \{x \in L \ ; \ \forall \sigma \in G, \ \sigma(x) = x\}$$

c'est-à-dire le corps fixe de G, formé des éléments de L que tous les automorphismes de G laissent inchangés. Alors K est un sous-corps de L et :

$$[L : K] = |G| \qquad \text{et} \qquad \mathrm{Aut}(L/K) = G$$

∘ *Démonstration :* Notons $n = |G|$ et $G = \{\sigma_1 = \mathrm{id} \, ; \sigma_2 \, ; \ldots \, ; \sigma_n\}$. Le fait que $K = L^G$ soit un sous-corps de L a été vu au paragraphe précédent ; remarquons dès maintenant que, par construction, tout élément de G fixe K point par point, de sorte que $G \subseteq \mathrm{Aut}(L/K)$. Toute la question est de savoir si cette inclusion est une égalité, et si le degré $[L : K]$ vaut exactement $|G|$.

Étape 1 : $[L : K] \leqslant n$**.** Supposons le contraire ; il existe alors $n+1$ éléments $\alpha_1, \ldots, \alpha_{n+1}$ de L linéairement indépendants sur K. Le système de n équations à $n+1$ inconnues :

$$\sum_{j=1}^{n+1} x_j \, \sigma_i \left(\alpha_j\right) = 0 \qquad (1 \leqslant i \leqslant n)$$

admet une solution non nulle dans L. Parmi toutes les solutions non nulles, choisissons-en une, notée $x = (x_j)$, ayant le plus petit nombre r de coordonnées non nulles. Quitte à renuméroter les α_j, supposons que ce sont les r premières coordonnées qui sont non nulles ; quitte à diviser x par x_1, supposons de plus $x_1 = 1$.

Si tous les x_j appartenaient à K, l'équation d'indice $i = 1$, c'est-à-dire $\sum_j x_j \alpha_j = 0$, contredirait l'indépendance des α_j sur K. Il existe donc un indice, disons 2, tel que $x_2 \notin K = L^G$: il existe $\tau \in G$ avec $\tau\left(x_2\right) \neq x_2$.

Appliquons τ à chacune des équations. Comme $\tau \circ \sigma_i$ parcourt G lorsque σ_i le parcourt, le vecteur $\tau(x)$ de coordonnées $\tau\left(x_j\right)$ est encore solution du même système. Par différence, le vecteur $x - \tau(x)$ l'est également. Or sa première coordonnée est nulle, car $x_1 = 1 \in K$; ses coordonnées d'indice supérieur à r sont nulles ; et sa deuxième coordonnée, $x_2 - \tau\left(x_2\right)$, ne l'est pas. Voilà donc une solution non nulle ayant au plus $r-1$ coordonnées non nulles : contradiction.

Étape 2 : $[L : K] \geqslant n$. Les n éléments de G sont des K-automorphismes de L, deux à deux distincts. La propriété 6.2 donne donc $n \leqslant [L : K]$ — l'extension étant finie d'après l'étape 1, la propriété s'applique.

Conclusion. On a $[L : K] = n$. Comme $G \subseteq \mathrm{Aut}(L/K)$ et que $|\mathrm{Aut}(L/K)| \leqslant [L : K] = n = |G|$, l'inclusion est une égalité. □

Remarque : Ce théorème est remarquable par son économie d'hypothèses : on ne suppose rien sur L, ni caractéristique, ni normalité, ni séparabilité. C'est le groupe G, donné d'avance, qui fabrique le corps de base et impose le degré. C'est ce renversement de perspective — partir du groupe plutôt que du polynôme — qui a permis à Artin de réécrire toute la théorie.

Exemple : **Le cas le plus simple.** Prenons $L = \mathbb{C}$ et $G = \{\mathrm{id}\,;\mathrm{conjugaison}\}$, groupe d'ordre 2. Un complexe z est fixé par la conjugaison si et seulement s'il est réel, donc $L^G = \mathbb{R}$. Le théorème d'Artin affirme alors, *sans aucun calcul*, que $[\mathbb{C} : \mathbb{R}] = 2$ et que $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = G$ — c'est-à-dire que l'identité et la conjugaison sont les seuls $\mathbb{R}$-automorphismes de $\mathbb{C}$. Nous l'avions établi à la main au paragraphe 6.1 ; le théorème le redonne gratuitement.

Exemple : **Un corps fixe que l'on ne devine pas.** Soit k un corps et $L = k(T)$ le corps des fractions rationnelles. L'application σ définie par $\sigma(F(T)) = F\left(\frac{1}{T}\right)$ est un automorphisme de L, et $\sigma^2 = \mathrm{id}$: le groupe $G = \{\mathrm{id}\,;\sigma\}$ est d'ordre 2.

Quel est son corps fixe ? On voit tout de suite que $u = T + \frac{1}{T}$ est fixé, donc $k(u) \subseteq L^G$; mais rien ne dit *a priori* qu'il n'y a pas davantage. C'est le théorème d'Artin qui tranche. D'une part, T annule le polynôme $X^2 - uX + 1 \in k(u)[X]$, puisque $T^2 - uT + 1 = T^2 - T^2 - 1 + 1 = 0$; comme $L = k(u)(T)$, on en tire $[L : k(u)] \leqslant 2$. D'autre part, le théorème d'Artin donne $\left[L : L^G\right] = |G| = 2$. La multiplicativité des degrés (théorème 4.1) appliquée à la tour $k(u) \subseteq L^G \subseteq L$ donne alors :

$$2 \geqslant [L : k(u)] = \left[L : L^G\right] \times \left[L^G : k(u)\right] = 2 \times \left[L^G : k(u)\right]$$

d'où $\left[L^G : k(u)\right] = 1$, c'est-à-dire :

$$L^G = k\left(T + \tfrac{1}{T}\right)$$

Voilà le schéma d'emploi typique du théorème d'Artin : on exhibe des éléments manifestement fixes, on majore le degré qu'ils engendrent, et le théorème, qui donne l'autre inégalité, force l'égalité. Sans lui, il faudrait démontrer directement que toute fraction rationnelle vérifiant $F(T) = F\left(\frac{1}{T}\right)$ est une fraction rationnelle en $T + \frac{1}{T}$, ce qui est bien plus pénible.

Exemple : **Les fonctions symétriques.** Voici l'exemple qui, historiquement, a tout déclenché. Soit k un corps, $L = k(T_1\,;\ldots\,;T_n)$ le corps des fractions rationnelles en n indéterminées, et $G = \mathfrak{S}_n$ agissant sur L en permutant les indéterminées : $\sigma \cdot F(T_1, \ldots, T_n) = F\left(T_{\sigma(1)}, \ldots, T_{\sigma(n)}\right)$. C'est bien un groupe d'automorphismes de L, d'ordre $n!$.

Les **polynômes symétriques élémentaires** sont fixés par G :

$$e_1 = \sum_i T_i, \qquad e_2 = \sum_{i<j} T_i T_j, \qquad \ldots, \qquad e_n = T_1 T_2 \cdots T_n$$

donc $K_0 = k(e_1\,;\ldots\,;e_n) \subseteq L^G$. Par ailleurs, les T_i sont exactement les racines du polynôme :

$$P = \prod_{i=1}^{n} (X - T_i) = X^n - e_1 X^{n-1} + e_2 X^{n-2} - \cdots + (-1)^n e_n \ \in \ K_0[X]$$

et L est engendré sur K_0 par ces racines : c'est un corps de décomposition de P sur K_0, donc $[L : K_0] \leqslant n!$ par le théorème 4.3. Le théorème d'Artin donnant $\left[L : L^G\right] = n!$, le même encadrement que ci-dessus force $L^G = K_0$, c'est-à-dire :

toute fraction rationnelle symétrique en $T_1, \ldots, T_n$ est une fraction rationnelle en $e_1, \ldots, e_n$

On obtient au passage $\mathrm{Gal}(L/K_0) = \mathfrak{S}_n$: *l'équation générale de degré n, dont les coefficients sont des indéterminées, a pour groupe de Galois le groupe symétrique tout entier.* C'est ce fait, joint à la non-résolubilité de $\mathfrak{S}_n$ pour $n \geqslant 5$ démontrée au chapitre 2, qui donnera au chapitre 7 l'impossibilité d'une formule générale par radicaux.

Remarque : L'hypothèse « G fini » ne peut pas être supprimée. Prenons $L = \mathbb{C}(T)$ et G le groupe de *tous* les automorphismes de L fixant $\mathbb{C}$: il est infini, car il contient les $T \mapsto aT + b$ pour $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$. Son corps fixe est $\mathbb{C}$, et $[L : \mathbb{C}]$ est infini : l'égalité $\left[L : L^G\right] = |G|$ n'a plus de sens. C'est bien la finitude de G qui, dans l'étape 1 de la démonstration, permet d'écrire un système de n équations.

6.3 Extensions galoisiennes

Définition : Une extension finie L/K est **galoisienne** si $L^{\mathrm{Aut}(L/K)} = K$, c'est-à-dire si les seuls éléments de L fixés par tous les K-automorphismes sont ceux de K. On note alors $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$, le **groupe de Galois** de l'extension.

Théorème 6.3 : caractérisations des extensions galoisiennes :
Soit L/K une extension finie. Les assertions suivantes sont équivalentes :

- **(i)** L/K est galoisienne, c'est-à-dire $L^{\mathrm{Aut}(L/K)} = K$;
- **(ii)** $|\mathrm{Aut}(L/K)| = [L : K]$;
- **(iii)** L/K est normale et séparable ;
- **(iv)** L est le corps de décomposition sur K d'un polynôme séparable de $K[X]$.

∘ *Démonstration :* **(i) ⇒ (ii).** Le groupe $G = \mathrm{Aut}(L/K)$ est fini par la propriété 6.2, et $L^G = K$; le théorème d'Artin donne $[L : K] = |G|$.

(ii) ⇒ (i). Posons $G = \mathrm{Aut}(L/K)$ et $M = L^G$, de sorte que $K \subseteq M \subseteq L$. Le théorème d'Artin appliqué à G agissant sur L donne $[L : M] = |G| = [L : K]$. Par multiplicativité, $[M : K] = 1$, soit $M = K$.

(i) ⇒ (iii). Soit $\alpha \in L$ et $\mathcal{O} = \{\sigma(\alpha)\ ;\ \sigma \in G\} = \{\alpha_1, \ldots, \alpha_s\}$ son orbite, formée d'éléments deux à deux distincts. Posons :

$$P = \prod_{k=1}^{s} (X - \alpha_k) \in L[X]$$

Chaque $\sigma \in G$ permute les α_k, donc laisse P invariant coefficient par coefficient : les coefficients de P sont dans $L^G = K$, et $P \in K[X]$. Comme $P(\alpha) = 0$, le polynôme minimal $\mu_{\alpha,K}$ divise P. Réciproquement, chaque $\alpha_k = \sigma(\alpha)$ vérifie $\mu_{\alpha,K}(\alpha_k) = \sigma(\mu_{\alpha,K}(\alpha)) = 0$, donc P divise $\mu_{\alpha,K}$ — les α_k étant distincts. Ainsi $\mu_{\alpha,K} = P$: il est scindé dans L et à racines simples. Ceci valant pour tout $\alpha \in L$, l'extension est normale et séparable.

(iii) ⇒ (iv). L'extension étant finie, écrivons $L = K(\alpha_1\,; \ldots\,; \alpha_r)$. Par normalité, chaque $\mu_{\alpha_i,K}$ est scindé dans L ; par séparabilité, il est à racines simples. Le produit des $\mu_{\alpha_i,K}$ *deux à deux distincts* est alors un polynôme séparable de $K[X]$ dont L est le corps de décomposition.

(iv) ⇒ (ii). Soit L le corps de décomposition d'un polynôme séparable P. Ses racines sont séparables sur K, donc L/K est séparable et $[L : K]_s = [L : K]$ par le théorème 5.1. Par ailleurs L/K est normale (théorème 5.2), donc tout K-plongement de L dans $\overline{K}$ a pour image L : les K-plongements sont exactement les K-automorphismes. D'où $|\mathrm{Aut}(L/K)| = [L : K]_s = [L : K]$. □

Remarque : La caractérisation (iv) est celle que l'on utilise en pratique : *le corps de décomposition d'un polynôme séparable est galoisien sur le corps de base.* En caractéristique nulle, la séparabilité étant automatique, il suffit de dire : *tout corps de décomposition est galoisien.* On peut donc, sans le moindre scrupule, parler du groupe de Galois d'un polynôme à coefficients rationnels.

Exemple : **Une extension qui n'est pas galoisienne.** Reprenons $L = \mathbb{Q}\big(\sqrt[3]{2}\big)$ et $K = \mathbb{Q}$, de degré 3. Nous avons vu au paragraphe 6.1 que $\mathrm{Aut}(L/K) = \{\mathrm{id}\}$. Vérifions que les quatre critères tombent tous en défaut, comme ils le doivent :

- **(i)** le corps fixe de $\{\mathrm{id}\}$ est L tout entier, et non K ;
- **(ii)** $|\mathrm{Aut}(L/K)| = 1$ alors que $[L : K] = 3$;
- **(iii)** l'extension est séparable, la caractéristique étant nulle, mais elle n'est pas normale : le polynôme irréductible $X^3 - 2$ y possède la racine $\sqrt[3]{2}$ sans y être scindé ;
- **(iv)** L n'est le corps de décomposition d'aucun polynôme de $\mathbb{Q}[X]$, précisément parce qu'il n'est pas normal.

C'est ici le défaut de *normalité* qui est en cause : il n'y a pas assez de racines dans L pour que les automorphismes aient de quoi les permuter.

Exemple : **La même équation, dans le bon corps.** Prenons maintenant $L = \mathbb{Q}\big(\sqrt[3]{2}\,; \mathrm{j}\big)$, corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$, de degré 6 (chapitre 4). Le polynôme $X^3 - 2$ est séparable, la caractéristique étant nulle : le critère **(iv)** s'applique directement, et l'extension est galoisienne. Le critère **(ii)** donne alors, sans aucun calcul d'automorphisme :

$$|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 6$$

Ainsi les six permutations des trois racines sont *toutes* réalisées par un automorphisme, ce que l'on peut comparer à l'exemple précédent où aucune ne l'était sauf l'identité. Comme $\mathrm{Gal}(L/\mathbb{Q})$ se plonge dans $\mathfrak{S}_3$, d'ordre 6 lui aussi, ce plongement est un isomorphisme :

$$\mathrm{Gal}\Big(\mathbb{Q}\Big(\sqrt[3]{2}\,; \mathrm{j}\Big)\,/\mathbb{Q}\Big) \simeq \mathfrak{S}_3$$

Exemple : **Normale mais non galoisienne : la séparabilité compte.** En caractéristique nulle, la condition **(iii)** se réduit à la normalité, et l'on pourrait croire la séparabilité superflue. Reprenons le contre-exemple du chapitre 5, avec les notations adaptées : soit p premier, $K = \mathbb{F}_p(S)$ le corps des fractions rationnelles en une indéterminée, et $L = K(\theta)$ où $\theta^p = S$ — concrètement, $L = \mathbb{F}_p(T)$ et $K = \mathbb{F}_p(T^p)$, en posant $\theta = T$ et $S = T^p$.

Le polynôme $X^p - S$ est irréductible sur K (chapitre 5) et L en est le corps de décomposition, puisque $X^p - S = (X - \theta)^p$ par le rêve du débutant. L'extension L/K est donc *normale*, de degré p. Pourtant elle n'est pas galoisienne : un K-automorphisme σ envoie θ sur une racine de $X^p - S$, c'est-à-dire sur θ lui-même, l'unique racine étant de multiplicité p ; donc $\mathrm{Aut}(L/K) = \{\mathrm{id}\}$ et $|\mathrm{Aut}(L/K)| = 1 \neq p$. Le critère **(ii)** est en défaut, et le coupable est cette fois l'inséparabilité. On mesure ici que le théorème 6.3 demande *deux* hypothèses et non une.

Définition : Soit $P \in K[X]$ séparable et L son corps de décomposition. Le **groupe de Galois de P sur K** est $\mathrm{Gal}(L/K)$.

Propriété 6.4 : Soit $P \in K[X]$ séparable de racines $\alpha_1, \ldots, \alpha_n$ dans son corps de décomposition L, et $G = \mathrm{Gal}(L/K)$. Alors l'application qui à $\sigma \in G$ associe la permutation qu'il induit sur $\{\alpha_1, \ldots, \alpha_n\}$ est un morphisme *injectif* $G \hookrightarrow \mathfrak{S}_n$. De plus, P est irréductible sur K si et seulement si G agit *transitivement* sur les racines.

∘ *Démonstration :* Chaque $\sigma \in G$ permute les racines de P, comme on l'a vu au chapitre 5, d'où un morphisme vers $\mathfrak{S}_n$; il est injectif car L est engendré par les racines, si bien qu'un automorphisme les fixant toutes est l'identité.

Supposons P irréductible et soient α_i, α_j deux racines. La propriété 4.4 fournit un K-isomorphisme $K(\alpha_i) \to K(\alpha_j)$ envoyant α_i sur α_j, que le théorème 4.4 prolonge en un automorphisme de L. L'action est donc transitive.

Réciproquement, supposons l'action transitive et soit Q le facteur irréductible de P annulant α_1. Toute racine α_j s'écrit $\sigma(\alpha_1)$, donc $Q(\alpha_j) = \sigma(Q(\alpha_1)) = 0$: le polynôme Q admet toutes les racines de P, donc $P \mid Q$ à constante près, et P est irréductible. □

Remarque : Voilà la traduction promise au chapitre 2 : l'*irréductibilité* du polynôme, notion algébrique, devient la *transitivité* de l'action, notion de théorie des groupes. On en déduit immédiatement, par le théorème orbite-stabilisateur, que n divise $|G|$ lorsque P est irréductible de degré n.

Exemple : **Le groupe de Galois de $X^4 + 1$ sur $\mathbb{Q}$.** Ce polynôme est irréductible, comme on l'a vu au chapitre 5 en appliquant Eisenstein à $(X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$ avec $q = 2$. Ses racines sont les quatre racines primitives huitièmes de l'unité $\zeta, \zeta^3, \zeta^5, \zeta^7$, où $\zeta = \mathrm{e}^{\mathrm{i}\pi/4}$; le corps de décomposition est donc $L = \mathbb{Q}(\zeta)$, de degré 4 puisque $X^4 + 1$ est le polynôme minimal de ζ.

L'extension est galoisienne par le critère **(iv)**, donc $|G| = 4$ où $G = \mathrm{Gal}(L/\mathbb{Q})$. La propriété 6.4 place G dans $\mathfrak{S}_4$ et, le polynôme étant irréductible, l'action sur les quatre racines est transitive. Un sous-groupe d'ordre 4 de $\mathfrak{S}_4$ est cyclique ou isomorphe au groupe de Klein ; pour trancher, calculons les ordres. Un automorphisme σ_k est déterminé par $\sigma_k(\zeta) = \zeta^k$ avec $k \in \{1\,;3\,;5\,;7\}$, et :

$$\sigma_k^2(\zeta) = \zeta^{k^2} = \zeta \qquad \text{car} \qquad 3^2 = 9 \equiv 1, \quad 5^2 = 25 \equiv 1, \quad 7^2 = 49 \equiv 1 \pmod 8$$

Tous les éléments de G sont donc d'ordre au plus 2 : le groupe n'est pas cyclique, et G est isomorphe au groupe de Klein $(\mathbb{Z}/2\mathbb{Z})^2$.

Ce petit calcul est instructif : l'irréductibilité, via la transitivité, a fourni la moitié de l'information — 4 divise $|G|$ — et le degré du corps de décomposition a fourni l'autre. On notera que $\zeta = \frac{1+\mathrm{i}}{\sqrt{2}}$, de sorte que $L = \mathbb{Q}\big(\mathrm{i}\,;\sqrt{2}\big)$; les trois sous-groupes d'ordre 2 du groupe de Klein correspondront, au paragraphe 6.5, aux trois sous-corps quadratiques $\mathbb{Q}(\mathrm{i})$, $\mathbb{Q}\big(\sqrt{2}\big)$ et $\mathbb{Q}\big(\mathrm{i}\sqrt{2}\big)$.

6.4 Le théorème fondamental

Théorème 6.4 : théorème fondamental de la théorie de Galois :
Soit L/K une extension galoisienne de groupe $G = \mathrm{Gal}(L/K)$. Notons $\mathscr{C}$ l'ensemble des corps intermédiaires $K \subseteq M \subseteq L$ et $\mathscr{H}$ l'ensemble des sous-groupes de G. Alors les applications :

$$\Phi : M \longmapsto \mathrm{Gal}(L/M) \qquad \text{et} \qquad \Psi : H \longmapsto L^H$$

sont des bijections réciproques l'une de l'autre, *décroissantes* pour l'inclusion. De plus :

- $[L : M] = |\mathrm{Gal}(L/M)|$ et $[M : K] = [G : \mathrm{Gal}(L/M)]$;
- M/K est galoisienne si et seulement si $\mathrm{Gal}(L/M) \trianglelefteq G$, et l'on a alors :

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

∘ *Démonstration :* **L'extension L/M est galoisienne.** Par le théorème 6.3, L est le corps de décomposition sur K d'un polynôme séparable P. Vu comme élément de $M[X]$, ce polynôme est encore séparable et L en est encore le corps de décomposition sur M : l'extension L/M est galoisienne, et $\mathrm{Gal}(L/M)$ est un sous-groupe de G — un M-automorphisme fixant $M \supseteq K$ fixe K.

$\Psi \circ \Phi = \mathrm{id}$. Comme L/M est galoisienne, $L^{\mathrm{Gal}(L/M)} = M$ par définition. Donc $\Psi(\Phi(M)) = M$.

$\Phi \circ \Psi = \mathrm{id}$. Soit $H \leqslant G$ et $M = L^H$. Le théorème d'Artin, appliqué au groupe fini H d'automorphismes de L, donne $[L : M] = |H|$ et $\mathrm{Aut}(L/M) = H$, c'est-à-dire $\mathrm{Gal}(L/M) = H$. Donc $\Phi(\Psi(H)) = H$.

Décroissance. Si $M \subseteq M'$, un M'-automorphisme fixe M : $\mathrm{Gal}(L/M') \subseteq \mathrm{Gal}(L/M)$. Symétriquement pour Ψ.

Degrés. L'égalité $[L : M] = |\mathrm{Gal}(L/M)|$ est le théorème 6.3 appliqué à L/M. Alors, par multiplicativité et par le théorème de Lagrange :

$$[M : K] = \frac{[L : K]}{[L : M]} = \frac{|G|}{|\mathrm{Gal}(L/M)|} = [G : \mathrm{Gal}(L/M)]$$

Normalité. Posons $H = \mathrm{Gal}(L/M)$. Observons d'abord que pour tout $\sigma \in G$:

$$\mathrm{Gal}\,(L/\sigma(M)) = \sigma H \sigma^{-1}$$

En effet, τ fixe $\sigma(M)$ point par point si et seulement si $\sigma^{-1}\tau\sigma$ fixe M point par point.

Supposons M/K galoisienne, donc normale. Tout $\sigma \in G$ se restreint en un K-plongement de M dans $\overline{K}$, donc $\sigma(M) = M$ par le théorème 5.2 ; la formule ci-dessus donne $\sigma H \sigma^{-1} = H$ pour tout σ, soit $H \trianglelefteq G$.

Réciproquement, supposons $H \trianglelefteq G$. Alors $\mathrm{Gal}(L/\sigma(M)) = H = \mathrm{Gal}(L/M)$ pour tout σ, et l'injectivité de Ψ donne $\sigma(M) = M$. La restriction fournit donc un morphisme de groupes :

$$\mathrm{res} : G \longrightarrow \mathrm{Aut}(M/K), \qquad \sigma \longmapsto \sigma_{|M}$$

dont le noyau est exactement H, c'est-à-dire l'ensemble des σ fixant M point par point. Par le premier théorème d'isomorphisme, $\mathrm{Im}(\mathrm{res}) \simeq G/H$, groupe d'ordre $[G : H] = [M : K]$. Comme $|\mathrm{Aut}(M/K)| \leqslant [M : K]$ par la propriété 6.2, la restriction est surjective et $|\mathrm{Aut}(M/K)| = [M : K]$: l'extension M/K est galoisienne par le théorème 6.3, de groupe $\mathrm{Gal}(M/K) \simeq G/H$. □

Remarque : Le renversement du sens des inclusions est la seule chose qui déroute au premier abord. Il s'explique très simplement : *plus le corps est grand, moins il reste d'automorphismes pour le fixer.* Au sommet, le corps L ne laisse que l'identité ; à la base, le corps K laisse tout le groupe.

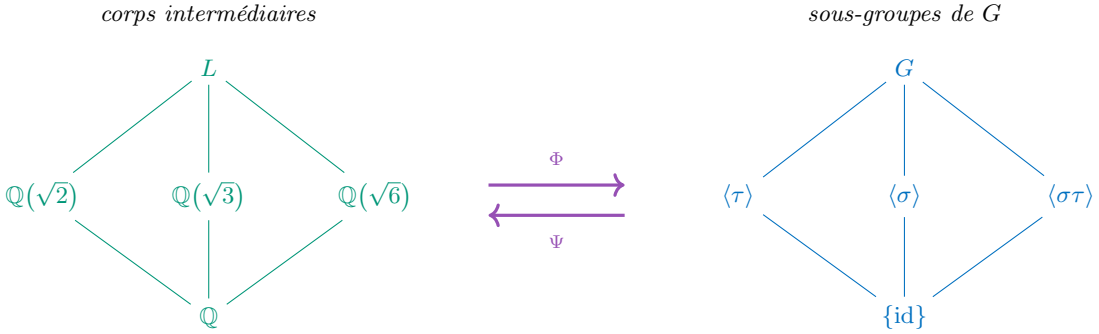
6.5 Trois exemples complets

Exemple : **L'extension $\mathbb{Q}(\sqrt{2};\sqrt{3})/\mathbb{Q}$.** Le corps $L = \mathbb{Q}(\sqrt{2};\sqrt{3})$ est le corps de décomposition de $(X^2-2)(X^2-3)$, séparable car de racines $\pm\sqrt{2}, \pm\sqrt{3}$ distinctes : l'extension est galoisienne, de degré 4, donc $|G| = 4$.

Un automorphisme est déterminé par les images de $\sqrt{2}$ et $\sqrt{3}$, chacune valant $\pm$ elle-même. Les quatre combinaisons sont réalisées, ce qui donne $G = \{\mathrm{id}\,;\sigma\,;\tau\,;\sigma\tau\}$ avec :

$$\sigma : \sqrt{2} \mapsto -\sqrt{2},\ \sqrt{3} \mapsto \sqrt{3} \qquad ; \qquad \tau : \sqrt{2} \mapsto \sqrt{2},\ \sqrt{3} \mapsto -\sqrt{3}$$

Tous les éléments non triviaux sont d'ordre 2 : G est le groupe de Klein, isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Il possède exactement cinq sous-groupes, donc il y a exactement cinq corps intermédiaires. Le corps fixe de $\langle\sigma\rangle$ est $\mathbb{Q}(\sqrt{3})$, celui de $\langle\tau\rangle$ est $\mathbb{Q}(\sqrt{2})$, et celui de $\langle\sigma\tau\rangle$ est $\mathbb{Q}(\sqrt{6})$, puisque $\sigma\tau(\sqrt{6}) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{6}$. Tous les sous-groupes d'un groupe abélien étant distingués, tous ces corps sont galoisiens sur $\mathbb{Q}$.



Les deux treillis se correspondent terme à terme, en sens inverse. Le sommet L répond au groupe trivial, la base $\mathbb{Q}$ répond à G tout entier, et $\mathbb{Q}(\sqrt{2})$ répond à $\langle\tau\rangle$, le sous-groupe qui fixe précisément $\sqrt{2}$. On lira la figure dans les deux sens : elle est le contenu même du théorème 6.4.

Exemple : **Le polynôme X^4-2 sur $\mathbb{Q}$.** Ses racines complexes sont $\pm\sqrt[4]{2}$ et $\pm\mathrm{i}\sqrt[4]{2}$; le corps de décomposition est donc $L=\mathbb{Q}(\sqrt[4]{2}\,;\mathrm{i})$. Son degré vaut 8 : on a $\left[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}\right]=4$ par Eisenstein, et $\mathrm{i}\notin\mathbb{R}$ ajoute un facteur 2.

Posons $\alpha=\sqrt[4]{2}$. Un automorphisme envoie α sur l'une des quatre racines et i sur $\pm\mathrm{i}$: au plus huit possibilités, donc exactement huit. Notons r celui qui envoie $\alpha\mapsto\mathrm{i}\alpha$ et $\mathrm{i}\mapsto\mathrm{i}$, et s la restriction de la conjugaison complexe, qui fixe α et envoie i sur $-\mathrm{i}$. On vérifie $r^4=\mathrm{id}$, $s^2=\mathrm{id}$ et $srs=r^{-1}$: le groupe est le **groupe diédral** D_4 d'ordre 8.

Il possède dix sous-groupes, donc L possède dix sous-corps. Les cinq sous-groupes d'ordre 2 donnent cinq corps de degré 4 sur $\mathbb{Q}$, et les trois sous-groupes d'ordre 4 donnent trois corps quadratiques. Le tableau ci-dessous en dresse la liste, obtenue en cherchant à chaque fois un élément fixé.

sous-groupe H	$\lvert H\rvert$	corps fixe L^H	$\left[L^H:\mathbb{Q}\right]$
$\{\mathrm{id}\}$	1	$L=\mathbb{Q}(\sqrt[4]{2}\,;\mathrm{i})$	8
$\langle s\rangle$	2	$\mathbb{Q}(\sqrt[4]{2})$	4
$\langle r^2s\rangle$	2	$\mathbb{Q}(\mathrm{i}\sqrt[4]{2})$	4
$\langle rs\rangle$	2	$\mathbb{Q}((1+\mathrm{i})\sqrt[4]{2})$	4
$\langle r^3s\rangle$	2	$\mathbb{Q}((1-\mathrm{i})\sqrt[4]{2})$	4
$\langle r^2\rangle$	2	$\mathbb{Q}(\sqrt{2}\,;\mathrm{i})$	4
$\langle r\rangle$	4	$\mathbb{Q}(\mathrm{i})$	2
$\langle r^2,s\rangle$	4	$\mathbb{Q}(\sqrt{2})$	2
$\langle r^2,rs\rangle$	4	$\mathbb{Q}(\mathrm{i}\sqrt{2})$	2
D_4	8	$\mathbb{Q}$	1

Les degrés de la dernière colonne sont bien les indices des sous-groupes correspondants. Les sous-groupes distingués de D_4 sont $\{\mathrm{id}\}$, $\langle r^2\rangle$, les trois d'ordre 4 et D_4 : les corps galoisiens sur $\mathbb{Q}$ sont donc exactement L, $\mathbb{Q}(\sqrt{2}\,;\mathrm{i})$, $\mathbb{Q}(\mathrm{i})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\mathrm{i}\sqrt{2})$ et $\mathbb{Q}$. En particulier $\mathbb{Q}(\sqrt[4]{2})$ ne l'est pas, ce que le chapitre 5 avait déjà constaté à la main — on retrouve ici, par la seule inspection du treillis des sous-groupes, un fait établi auparavant par un calcul.

Exemple : **Les corps finis.** Soit $q=p^n$. L'extension $\mathbb{F}_q/\mathbb{F}_p$ est le corps de décomposition de X^q-X, séparable ; elle est donc galoisienne de degré n. Le morphisme de Frobenius $\mathrm{Frob}:x\mapsto x^p$ est un $\mathbb{F}_p$-automorphisme, car il fixe $\mathbb{F}_p$ d'après le petit théorème de Fermat. Son ordre est exactement n : en effet $\mathrm{Frob}^k=\mathrm{id}$ signifie $x^{p^k}=x$ pour tout $x\in\mathbb{F}_q$, c'est-à-dire que $\mathbb{F}_q$ est contenu dans le corps à p^k éléments, ce qui impose $n\mid k$. Ainsi :

$$\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)=\langle\mathrm{Frob}\rangle\simeq\mathbb{Z}/n\mathbb{Z}$$

La correspondance de Galois redonne alors, sans aucun calcul supplémentaire, la propriété 5.5 : les sous-corps de $\mathbb{F}_{p^n}$ correspondent aux sous-groupes de $\mathbb{Z}/n\mathbb{Z}$, donc aux diviseurs de n. Le treillis des sous-corps de $\mathbb{F}_{p^{12}}$ et celui des sous-groupes de $\mathbb{Z}/12\mathbb{Z}$, dessinés séparément aux chapitres 5 et 1, ne sont qu'une seule et même figure.

Chapitre 7

Résolubilité par radicaux et applications

> *J'observerai d'abord que, pour résoudre une équation, il faut successivement abaisser son groupe jusqu'à ne contenir plus qu'une seule permutation.*

Évariste Galois, *Mémoire sur les conditions de résolubilité des équations par radicaux*, publié par Liouville en 1846

(*Œuvres mathématiques d'Évariste Galois*, Gauthier-Villars, 1897)

Nous disposons maintenant du dictionnaire : corps intermédiaires d'un côté, sous-groupes de l'autre. Il reste à traduire le mot *radical*. L'idée de Galois, énoncée dans la phrase ci-dessus, est que résoudre une équation consiste à abaisser son groupe par paliers jusqu'à l'identité, chaque palier correspondant à une extraction de racine. Nous allons montrer qu'un palier « extraction de racine n-ième » correspond exactement à un quotient *cyclique* — d'où l'équivalence entre résolubilité par radicaux et résolubilité du groupe.

Dans tout ce chapitre, les corps considérés sont de caractéristique nulle, ce qui rend automatiques la séparabilité et toutes les hypothèses du chapitre 6.

7.1 Extensions cyclotomiques

Définition : Soit $n \geqslant 1$. Une **racine primitive n-ième de l'unité** est un générateur du groupe cyclique μ_n des racines de $X^n - 1$. Le **polynôme cyclotomique** d'indice n est :

$$\Phi_n = \prod_{\substack{1 \leqslant k \leqslant n \\ \operatorname{pgcd}(k\,;n)=1}} \left(X - \zeta^k\right) \qquad \text{où } \zeta = \mathrm{e}^{2\mathrm{i}\pi/n}$$

Son degré est $\varphi(n)$, l'indicatrice d'Euler.

Exemple : Les premiers polynômes cyclotomiques se calculent de proche en proche :

$$\Phi_1 = X - 1, \quad \Phi_2 = X + 1, \quad \Phi_3 = X^2 + X + 1, \quad \Phi_4 = X^2 + 1, \quad \Phi_6 = X^2 - X + 1$$

Pour $n = 6$, par exemple, les racines primitives sixièmes sont $\mathrm{e}^{\pm\mathrm{i}\pi/3}$, de somme 1 et de produit 1 : d'où $\Phi_6 = X^2 - X + 1$, de degré $\varphi(6) = 2$.

On vérifie la factorisation annoncée par la propriété suivante :

$$\Phi_1\Phi_2\Phi_3\Phi_6 = (X-1)(X+1)\left(X^2+X+1\right)\left(X^2-X+1\right) = \left(X^2-1\right)\left(X^4+X^2+1\right) = X^6 - 1$$

les diviseurs de 6 étant 1, 2, 3 et 6. On notera au passage que tous ces polynômes sont à coefficients entiers, bien que leurs racines soient complexes.

Propriété 7.1 : On a $X^n - 1 = \prod_{d|n} \Phi_d$, et $\Phi_n \in \mathbb{Z}[X]$.

∘ *Démonstration :* Chaque racine n-ième de l'unité engendre un sous-groupe de μ_n, cyclique d'ordre d pour un unique diviseur d de n ; elle est alors racine primitive d-ième. En classant les n racines selon leur ordre, on obtient la factorisation annoncée, les facteurs étant deux à deux premiers entre eux.

Montrons par récurrence forte que $\Phi_n \in \mathbb{Z}[X]$. C'est vrai pour $n = 1$ où $\Phi_1 = X - 1$. Pour $n > 1$, posons $Q = \prod_{d|n,\ d<n} \Phi_d$, unitaire et à coefficients entiers par hypothèse de récurrence. La division euclidienne de $X^n - 1$ par Q dans $\mathbb{Q}[X]$ a un quotient et un reste à coefficients *entiers*, car l'algorithme de division ne divise que par le coefficient dominant de Q, qui vaut 1. Ce quotient est Φ_n, qui est donc dans $\mathbb{Z}[X]$. □

Théorème 7.1 : irréductibilité des polynômes cyclotomiques :
Pour tout $n \geqslant 1$, le polynôme Φ_n est irréductible sur $\mathbb{Q}$. Par conséquent :

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

∘ *Démonstration :* Soit ζ une racine primitive n-ième et $f = \mu_{\zeta,\mathbb{Q}}$. Comme f divise $X^n - 1$, qui est unitaire à coefficients entiers, le lemme de Gauss (chapitre 3) donne $f \in \mathbb{Z}[X]$ unitaire, et l'on écrit $X^n - 1 = f\,g$ avec $g \in \mathbb{Z}[X]$ unitaire.

Point clé : si p est premier et ne divise pas n, alors ζ^p est racine de f. Supposons le contraire. Comme ζ^p est racine de $X^n - 1$, elle est racine de g, donc ζ est racine de $g(X^p)$, donc f divise $g(X^p)$ dans $\mathbb{Q}[X]$, puis dans $\mathbb{Z}[X]$ par le lemme de Gauss. Réduisons modulo p : dans $\mathbb{F}_p[X]$, le rêve du débutant donne $\overline{g}(X^p) = \overline{g}(X)^p$, donc :

$$\overline{f} \mid \overline{g}^{\,p}$$

Tout facteur irréductible h de $\overline{f}$ divise donc $\overline{g}$, et h^2 divise $\overline{f}\,\overline{g} = X^n - \overline{1}$. Or ce dernier polynôme est séparable sur $\mathbb{F}_p$: sa dérivée nX^{n-1} est non nulle car $p \nmid n$, et le seul facteur irréductible commun possible serait X, qui ne divise pas $X^n - 1$. Contradiction.

Conclusion. Soit k premier avec n ; décomposons $k = p_1 \cdots p_s$ en facteurs premiers, tous distincts des diviseurs premiers de n. En appliquant le point clé successivement à ζ, puis à ζ^{p_1}, puis à $\zeta^{p_1 p_2}$, etc. — chacune de ces puissances étant encore une racine primitive n-ième —, on obtient que ζ^k est racine de f. Ainsi f admet pour racines les $\varphi(n)$ racines primitives, donc $\deg f \geqslant \varphi(n)$; comme f divise Φ_n, qui est de degré $\varphi(n)$, on conclut $f = \Phi_n$. □

Théorème 7.2 : groupe de Galois cyclotomique :
Soit K un corps de caractéristique nulle et ζ une racine primitive n-ième de l'unité. Alors $K(\zeta)/K$ est galoisienne et l'application :

$$\mathrm{Gal}\,(K(\zeta)/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*, \qquad \sigma \longmapsto \overline{k_\sigma} \ \text{ où } \ \sigma(\zeta) = \zeta^{k_\sigma}$$

est un morphisme *injectif* de groupes. En particulier $\mathrm{Gal}(K(\zeta)/K)$ est abélien. Lorsque $K = \mathbb{Q}$, c'est un isomorphisme.

∘ *Démonstration :* Le corps $K(\zeta)$ est le corps de décomposition de $X^n - 1$ sur K, puisque toutes les racines sont des puissances de ζ ; ce polynôme est séparable, sa dérivée nX^{n-1} étant première avec lui en caractéristique nulle. L'extension est donc galoisienne.

Tout σ envoie ζ sur une racine primitive n-ième — car σ est un automorphisme du groupe μ_n, donc conserve l'ordre —, c'est-à-dire sur ζ^{k_σ} avec $\mathrm{pgcd}\,(k_\sigma\,;n) = 1$. Si σ, τ sont deux automorphismes :

$$(\sigma\tau)(\zeta) = \sigma\left(\zeta^{k_\tau}\right) = \left(\zeta^{k_\sigma}\right)^{k_\tau} = \zeta^{k_\sigma k_\tau}$$

donc $k_{\sigma\tau} \equiv k_\sigma k_\tau$: c'est un morphisme. Il est injectif car σ est déterminé par $\sigma(\zeta)$, le corps étant engendré par ζ. Enfin, pour $K = \mathbb{Q}$, les deux groupes ont même cardinal $\varphi(n)$ d'après le théorème 7.1 : le morphisme injectif est bijectif. □

Exemple : Pour $n = 5$, on a $\mathrm{Gal}\,(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq (\mathbb{Z}/5\mathbb{Z})^* \simeq \mathbb{Z}/4\mathbb{Z}$, cyclique d'ordre 4, engendré par $\sigma : \zeta \mapsto \zeta^2$ — car 2 est d'ordre 4 modulo 5, ses puissances étant $2, 4, 3, 1$. L'unique sous-groupe d'ordre 2 est $\langle\sigma^2\rangle$ avec $\sigma^2 : \zeta \mapsto \zeta^4 = \overline{\zeta}$: son corps fixe est $\mathbb{Q}\big(\zeta + \zeta^{-1}\big) = \mathbb{Q}\big(2\cos\frac{2\pi}{5}\big)$, l'unique corps intermédiaire, de degré 2. On retrouve la valeur classique $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$, dont on vérifie numériquement qu'elle vaut 0,309017.

7.2 Extensions cycliques et extraction de racines

Théorème 7.3 : extensions cycliques et radicaux :
Soit K un corps de caractéristique nulle contenant une racine primitive n-ième de l'unité ζ.

- Pour tout $a \in K^*$ et toute racine α de $X^n - a$, l'extension $K(\alpha)/K$ est galoisienne de groupe cyclique, d'ordre divisant n.
- Réciproquement, si L/K est galoisienne de groupe cyclique d'ordre n, il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $\alpha^n \in K$.

∘ *Démonstration :* **Sens direct.** Les racines de $X^n - a$ sont $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$, deux à deux distinctes, et toutes appartiennent à $K(\alpha)$ puisque $\zeta \in K$. Donc $K(\alpha)$ est le corps de décomposition de $X^n - a$, séparable : l'extension

est galoisienne. Posons $G = \mathrm{Gal}(K(\alpha)/K)$. Pour tout $\sigma \in G$, on a $\sigma(\alpha) = \zeta^{c_\sigma}\alpha$ où c_σ est un entier bien défini modulo n. Soient alors $\sigma, \tau \in G$; il vient :

$$(\sigma\tau)(\alpha) = \sigma\left(\zeta^{c_\tau}\alpha\right) = \zeta^{c_\tau}\zeta^{c_\sigma}\alpha$$

puisque σ fixe $\zeta \in K$. L'application $\sigma \mapsto \overline{c_\sigma}$ est donc un morphisme de G dans $\mathbb{Z}/n\mathbb{Z}$, injectif car σ est déterminé par $\sigma(\alpha)$. Ainsi G est isomorphe à un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, donc cyclique d'ordre divisant n.

Sens réciproque. Soit σ un générateur de $G = \mathrm{Gal}(L/K)$, d'ordre n. Considérons la **résolvante de Lagrange** : pour $\beta \in L$,

$$\alpha(\beta) = \beta + \zeta\,\sigma(\beta) + \zeta^2\sigma^2(\beta) + \cdots + \zeta^{n-1}\sigma^{n-1}(\beta)$$

L'application $\beta \mapsto \alpha(\beta)$ est la combinaison linéaire $\sum_i \zeta^i\sigma^i$ des n automorphismes distincts $\mathrm{id}, \sigma, \ldots, \sigma^{n-1}$, à coefficients non nuls. Par le théorème d'indépendance des caractères (chapitre 6), elle n'est pas identiquement nulle : il existe β tel que $\alpha = \alpha(\beta) \neq 0$.

Appliquons σ et utilisons $\sigma(\zeta) = \zeta$ ainsi que $\sigma^n = \mathrm{id}$:

$$\sigma(\alpha) = \sigma(\beta) + \zeta\sigma^2(\beta) + \cdots + \zeta^{n-1}\beta = \zeta^{-1}\left(\zeta\sigma(\beta) + \zeta^2\sigma^2(\beta) + \cdots + \zeta^n\beta\right) = \zeta^{-1}\alpha$$

Il en résulte $\sigma\left(\alpha^n\right) = \zeta^{-n}\alpha^n = \alpha^n$, donc α^n est fixé par σ, donc par G tout entier : $\alpha^n \in K$. Par ailleurs les éléments $\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha) = \zeta^{-i}\alpha$ sont deux à deux distincts, donc α possède n conjugués : $[K(\alpha) : K] = n = [L : K]$, d'où $L = K(\alpha)$. □

Remarque : La résolvante de Lagrange n'est pas une invention de circonstance : c'est précisément l'objet introduit par **Lagrange** en 1771 dans ses *Réflexions sur la résolution algébrique des équations*, et c'est elle qui produit les formules de Cardan pour le degré 3. Avec $n = 3$, $\zeta = \mathrm{j}$ et β une racine de l'équation, la quantité $\beta + \mathrm{j}\sigma(\beta) + \mathrm{j}^2\sigma^2(\beta)$ est exactement la combinaison dont on extrait la racine cubique dans la formule classique. Le théorème 7.3 dit que ce procédé, découvert au cas par cas, est le mécanisme général.

7.3 Le critère de résolubilité

Définition : Une extension M/K est **radicale** s'il existe une tour :

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = M \qquad \text{avec} \qquad K_{i+1} = K_i(a_i) \quad \text{et} \quad a_i^{n_i} \in K_i$$

Un polynôme $P \in K[X]$ est **résoluble par radicaux** si son corps de décomposition est contenu dans une extension radicale de K.

Exemple : L'extension $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ est radicale, avec la tour à un seul étage $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}\right)$ et $\left(\sqrt{2}\right)^2 = 2 \in \mathbb{Q}$. L'extension $\mathbb{Q}\left(\sqrt{2}\,;\,\sqrt[3]{1+\sqrt{2}}\right)/\mathbb{Q}$ l'est aussi, avec cette fois deux étages :

$$\mathbb{Q} \;\subseteq\; \mathbb{Q}\left(\sqrt{2}\right) \;\subseteq\; \mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt[3]{1+\sqrt{2}}\right)$$

le cube du second générateur, $1+\sqrt{2}$, appartenant bien à l'étage précédent. C'est exactement ce qu'on écrit lorsqu'on emboîte des radicaux.

Tout polynôme du second degré est résoluble par radicaux : son corps de décomposition est $K\left(\sqrt{\Delta}\right)$, où $\Delta = b^2 - 4ac$, extension radicale à un étage. Les formules de Cardan et de Ferrari font de même pour les degrés 3 et 4. Le théorème 7.4 dira exactement jusqu'où ce procédé peut aller.

Remarque : Cette définition traduit fidèlement l'idée intuitive : les racines s'expriment à partir des coefficients au moyen des quatre opérations et d'extractions de racines n-ièmes emboîtées. Chaque étage de la tour correspond à l'écriture d'un radical, et $a_i = \sqrt[n_i]{\text{quelque chose de déjà construit}}$.

Propriété 7.4 :

- Un groupe fini G est résoluble si et seulement s'il possède une chaîne $\{e\} = G_0 \trianglelefteq \cdots \trianglelefteq G_r = G$ dont tous les quotients sont *cycliques d'ordre premier*.
- Si M/K est radicale, sa clôture galoisienne N dans $\overline{K}$ est encore radicale sur K.

∘ *Démonstration :* **Premier point.** La condition est évidemment suffisante. Réciproquement, il suffit, grâce au théorème de correspondance, de raffiner chaque quotient abélien fini $A = G_{i+1}/G_i$. Or tout groupe abélien fini $A \neq \{e\}$ possède une chaîne à quotients cycliques d'ordre premier : on choisit $x \in A$ avec $x \neq e$, puis un diviseur premier p de $o(x)$, et l'on pose $y = x^{o(x)/p}$, qui est d'ordre p ; le sous-groupe $\langle y \rangle$ est distingué puisque A est

abélien, le quotient $A/\langle y\rangle$ est abélien d'ordre strictement plus petit, et une récurrence sur $|A|$ conclut. On relève ensuite ces chaînes dans G_{i+1} par le théorème de correspondance.

Second point. Notons $\varphi_1, \dots, \varphi_s$ les K-plongements de M dans $\overline{K}$; la clôture galoisienne N est le compositum des $\varphi_j(M)$. Chaque $\varphi_j(M)$ est radicale sur K : il suffit d'appliquer φ_j à la tour de M, ce qui fournit la tour $K \subseteq \varphi_j(K_1) \subseteq \cdots$, chaque étage étant engendré par $\varphi_j(a_i)$ dont la puissance n_i-ième reste dans l'étage précédent.

Il reste à voir qu'un compositum de deux extensions radicales M_1 et M_2 de K est radical. On part de la tour de M_1, puis on la prolonge par $M_1 \subseteq M_1(b_1) \subseteq M_1(b_1; b_2) \subseteq \cdots$ où les b_i sont les générateurs successifs de la tour de M_2 : les conditions $b_i^{m_i} \in K'_{i-1} \subseteq M_1(b_1; \dots; b_{i-1})$ restent satisfaites. On itère pour un nombre fini de facteurs. □

Théorème 7.4 : critère de résolubilité de Galois :
Soit K un corps de caractéristique nulle et $P \in K[X]$ non constant, de corps de décomposition L. Alors :

$$P \text{ est résoluble par radicaux} \iff \mathrm{Gal}(L/K) \text{ est un groupe résoluble}$$

∘ *Démonstration :* **Sens direct.** Supposons $L \subseteq M$ avec M/K radicale. Quitte à remplacer M par sa clôture galoisienne, ce que la propriété 7.4 autorise, supposons M/K galoisienne. Soit $n = \mathrm{ppcm}(n_0; \dots; n_{r-1})$ des exposants de la tour, ζ une racine primitive n-ième de l'unité, et $M' = M(\zeta)$. C'est encore une extension galoisienne de K — corps de décomposition du produit du polynôme définissant M par $X^n - 1$ — et elle est encore radicale, puisque $\zeta^n = 1 \in K$.

Considérons la tour :

$$K \subseteq K(\zeta) = K'_0 \subseteq K'_1 \subseteq \cdots \subseteq K'_r = M' \qquad \text{où } K'_i = K_i(\zeta)$$

Chaque étage $K'_{i+1} = K'_i(a_i)$ vérifie $a_i^{n_i} \in K'_i$, et K'_i contient une racine primitive n_i-ième de l'unité, à savoir ζ^{n/n_i}. Le théorème 7.3 assure donc que K'_{i+1}/K'_i est galoisienne cyclique. Par ailleurs $K(\zeta)/K$ est galoisienne abélienne par le théorème 7.2.

Posons $G = \mathrm{Gal}(M'/K)$ et $H_i = \mathrm{Gal}(M'/K'_i)$, ainsi que $H_{-1} = \mathrm{Gal}(M'/K(\zeta))$. Le théorème fondamental transforme cette tour de corps en une chaîne de sous-groupes :

$$\{\mathrm{id}\} = H_r \trianglelefteq H_{r-1} \trianglelefteq \cdots \trianglelefteq H_0 = H_{-1} \trianglelefteq G$$

où chaque H_{i+1} est distingué dans H_i de quotient $\mathrm{Gal}(K'_{i+1}/K'_i)$, cyclique, et où $G/H_{-1} \simeq \mathrm{Gal}(K(\zeta)/K)$ est abélien. Tous les quotients étant abéliens, G est résoluble.

Enfin L/K est galoisienne et $L \subseteq M'$, donc $\mathrm{Gal}(L/K)$ est un quotient de G par le théorème fondamental : il est résoluble par le théorème 2.8.

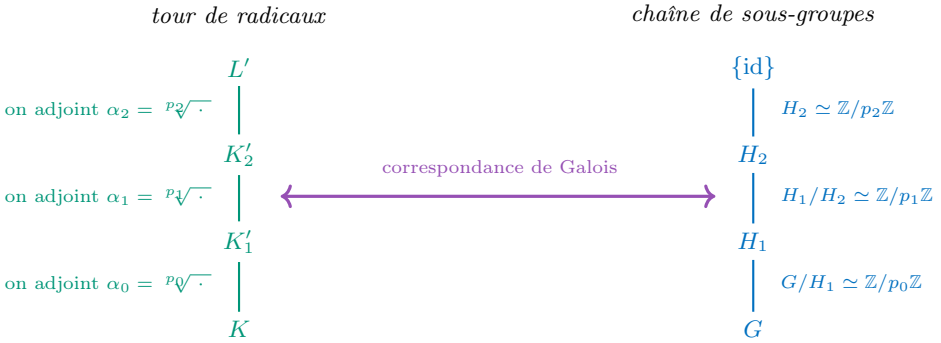
Sens réciproque. Supposons $G = \mathrm{Gal}(L/K)$ résoluble, d'ordre m. Soit ζ une racine primitive m-ième de l'unité, $K' = K(\zeta)$ et $L' = L(\zeta)$. L'extension L'/K' est galoisienne, et la restriction :

$$\mathrm{Gal}(L'/K') \longrightarrow \mathrm{Gal}(L/K), \qquad \sigma \longmapsto \sigma_{|L}$$

est bien définie — car $\sigma(L) = L$, L/K étant normale — et injective, car un automorphisme de $L' = L(\zeta)$ fixant L et ζ est l'identité. Donc $\mathrm{Gal}(L'/K')$ est isomorphe à un sous-groupe de G : il est résoluble.

Par la propriété 7.4, il existe une chaîne $\{\mathrm{id}\} = H_s \trianglelefteq \cdots \trianglelefteq H_0 = \mathrm{Gal}(L'/K')$ à quotients cycliques d'ordre premier p_i. Notons $F_i = L'^{H_i}$ les corps correspondants ; alors F_{i+1}/F_i est galoisienne cyclique de degré premier p_i, et p_i divise $|\mathrm{Gal}(L'/K')|$ qui divise m. Le corps F_i contient donc ζ^{m/p_i}, racine primitive p_i-ième de l'unité, et le théorème 7.3 donne $F_{i+1} = F_i(\alpha_i)$ avec $\alpha_i^{p_i} \in F_i$.

La tour $K \subseteq K(\zeta) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_s = L'$ est donc radicale sur K, le premier étage l'étant puisque $\zeta^m = 1$. Comme $L \subseteq L'$, le polynôme P est résoluble par radicaux. □



Le théorème 7.4 en une image : chaque extraction d'une racine p_i-ième, à gauche, correspond exactement à un quotient cyclique d'ordre p_i, à droite. Résoudre par radicaux, c'est démonter le groupe étage par étage — la phrase de Galois placée en épigraphe dit précisément cela.

7.4 Le théorème d'Abel-Ruffini

Propriété 7.5 : Soit $P \in \mathbb{Q}[X]$ irréductible de degré 5 possédant exactement trois racines réelles. Alors le groupe de Galois de P sur $\mathbb{Q}$ est isomorphe à $\mathfrak{S}_5$.

∘ *Démonstration :* Soit $L \subset \mathbb{C}$ le corps de décomposition de P et $G = \mathrm{Gal}(L/\mathbb{Q})$, vu comme sous-groupe de $\mathfrak{S}_5$ agissant sur les cinq racines (propriété 6.4).

G contient un 5-cycle. Le polynôme étant irréductible, l'action est transitive, donc l'orbite d'une racine a cinq éléments et 5 divise $|G|$ par le théorème orbite-stabilisateur. Le théorème de Cauchy fournit alors un élément d'ordre 5 dans G ; or les seuls éléments d'ordre 5 de $\mathfrak{S}_5$ sont les 5-cycles, un tel élément ayant toutes ses longueurs de cycles égales à 5.

G contient une transposition. La conjugaison complexe induit un automorphisme de L — car L est stable par conjugaison, étant engendré par les racines de P qui sont permutées par celle-ci — et il fixe $\mathbb{Q}$. Sur les racines, il fixe les trois racines réelles et échange les deux racines complexes conjuguées : c'est une transposition.

Conclusion. Notons $\tau = (a\ b)$ la transposition et c le 5-cycle. Comme $\langle c\rangle$ agit transitivement, il existe j tel que $c^j(a) = b$; et c^j est encore un 5-cycle, j n'étant pas multiple de 5. Renumérotons les racines de sorte que $c^j = (1\ 2\ 3\ 4\ 5)$ et $a = 1$, donc $b = 2$ et $\tau = (1\ 2)$. Alors, par la formule de conjugaison :

$$c^j\,(1\ 2)\,c^{-j} = (2\ 3), \qquad c^{2j}(1\ 2)c^{-2j} = (3\ 4), \qquad \text{etc.}$$

Le groupe G contient donc toutes les transpositions $(k\ \ k{+}1)$, qui engendrent $\mathfrak{S}_5$: en effet $(1\ 2)$, $(2\ 3)$, … permettent d'obtenir $(i\ j)$ quelconque par conjugaisons successives, et les transpositions engendrent $\mathfrak{S}_5$ d'après le chapitre 1. Donc $G = \mathfrak{S}_5$. □

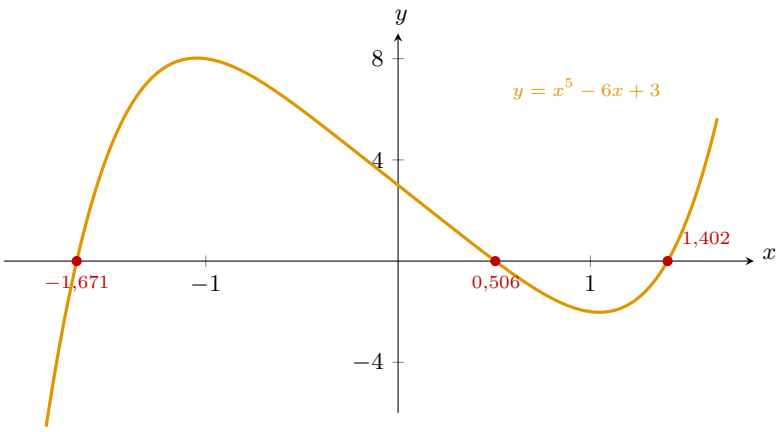
Théorème 7.5 : théorème d'Abel-Ruffini :
Le polynôme $P = X^5 - 6X + 3$ n'est pas résoluble par radicaux sur $\mathbb{Q}$. Il n'existe donc aucune formule générale, par radicaux, exprimant les racines d'une équation de degré 5 à partir de ses coefficients.

∘ *Démonstration :* **Irréductibilité.** Le critère d'Eisenstein s'applique avec $q = 3$: ce nombre divise -6 et 3, ne divise pas le coefficient dominant 1, et 9 ne divise pas 3.

Trois racines réelles. La dérivée $P' = 5X^4 - 6$ s'annule en $\pm x_0$ avec $x_0 = \left(\frac{6}{5}\right)^{1/4} \approx 1{,}0466$. La fonction P est donc croissante sur $]-\infty\,;-x_0]$, décroissante sur $[-x_0\,;x_0]$, puis croissante. On calcule $P(-x_0) \approx 8{,}03 > 0$ et $P(x_0) \approx -2{,}03 < 0$: le maximum local est positif et le minimum local négatif. Le théorème des valeurs intermédiaires donne exactement trois racines réelles, une dans chaque intervalle de monotonie, et il n'y en a pas davantage. Les deux racines restantes sont donc complexes conjuguées.

Conclusion. La propriété 7.5 donne $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathfrak{S}_5$, qui n'est pas résoluble d'après le théorème 2.10. Le critère de Galois interdit donc toute résolution par radicaux.

En particulier, une formule générale valable pour tout polynôme de degré 5 s'appliquerait à celui-ci : il n'en existe aucune. □



La courbe montre les trois racines réelles annoncées : le maximum local, atteint en $-1{,}047$, est au-dessus de l'axe, et le minimum local, en 1,047, en dessous. Ce sont ces deux inégalités, et elles seules, qui forcent la présence de deux racines non réelles, donc d'une transposition dans le groupe de Galois — et par là l'impossibilité de toute formule.

Remarque : On mesure la finesse du résultat en le comparant à un voisin : $X^5 - 2$ est également irréductible, mais son groupe de Galois est d'ordre 20, résoluble, et ses racines s'écrivent bien par radicaux, à savoir $\zeta_5^k \sqrt[5]{2}$. Ce n'est donc pas le degré 5 en lui-même qui fait obstacle, mais le groupe : une équation de degré 5 peut parfaitement être résoluble. Ce que dit le théorème, c'est qu'il n'existe pas de formule *générale* — et le critère de Galois permet, pour chaque équation particulière, de trancher.

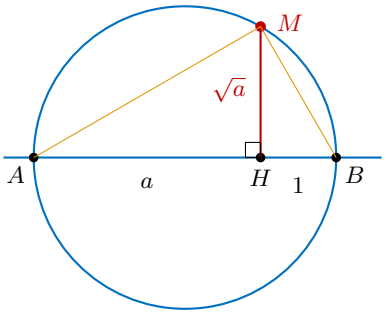
7.5 Polygones réguliers constructibles

Propriété 7.6 : L'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de $\mathbb{C}$, stable par racine carrée et par conjugaison.

∘ *Démonstration :* La stabilité par somme et par opposé se lit sur le report de longueurs au compas. Pour le produit et l'inverse de deux réels positifs, on utilise le théorème de Thalès : en plaçant 1 et a sur une demi-droite, b sur une autre, et en traçant la parallèle convenable, on obtient ab ; le même dispositif, lu à l'envers, donne $\frac{a}{b}$. Le passage aux complexes se fait en construisant séparément partie réelle et partie imaginaire, ce que permet la construction de la perpendiculaire.

Pour la racine carrée d'un réel $a > 0$: on trace le cercle de diamètre $[AB]$ avec $AB = a + 1$, on place H sur $[AB]$ avec $AH = a$ et $HB = 1$, et l'on élève la perpendiculaire en H, qui coupe le cercle en M. Le triangle AMB étant rectangle en M, la relation métrique $HM^2 = HA \times HB$ donne $HM = \sqrt{a}$. Pour un complexe, on combine avec la bissection de l'angle, qui s'obtient au compas.

Enfin la conjugaison est la symétrie par rapport à l'axe des abscisses, qui est constructible. □



La hauteur issue de l'angle droit d'un triangle rectangle vaut la moyenne géométrique des deux segments qu'elle détermine : $HM^2 = HA \times HB = a$.

La construction de $\sqrt{a}$ à la règle et au compas, ici pour $a = 3$, où $HM = \sqrt{3} \approx 1{,}732$. C'est cette figure, et elle seule, qui explique pourquoi seules les extensions de degré 2 apparaissent dans le critère de Wantzel.

Propriété 7.7 : Tout groupe d'ordre 2^k possède une chaîne de sous-groupes $\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_k = G$ avec $|H_i| = 2^i$.

∘ *Démonstration :* Récurrence sur k, le cas $k = 0$ étant trivial. Soit $|G| = 2^k$ avec $k \geqslant 1$ et écrivons l'équation aux classes du paragraphe 2.4, où $Z(G)$ désigne le centre de G :

$$2^k = |Z(G)| + \sum_{\text{orbites de cardinal}>1} |\mathcal{O}|$$

Chaque terme de la somme est une puissance de 2 supérieure à 1, donc paire ; comme 2^k est pair, $|Z(G)|$ est pair, et en particulier $Z(G) \neq \{e\}$.

Le théorème de Cauchy fournit alors $y \in Z(G)$ d'ordre 2. Le sous-groupe $\langle y \rangle$ est distingué dans G, étant central, et $G/\langle y \rangle$ est d'ordre 2^{k-1} : l'hypothèse de récurrence lui fournit une chaîne, que l'on relève par le théorème de correspondance en une chaîne de G contenant $\langle y \rangle$. En lui adjoignant $\{e\} \trianglelefteq \langle y \rangle$, on obtient la chaîne voulue. □

Théorème 7.6 : critère de constructibilité :
Soit $z \in \mathbb{C}$ algébrique sur $\mathbb{Q}$ et N le corps de décomposition de $\mu_{z,\mathbb{Q}}$. Alors :

$$z \text{ est constructible} \iff [N : \mathbb{Q}] \text{ est une puissance de 2}$$

∘ *Démonstration :* **Sens réciproque.** Supposons $[N : \mathbb{Q}] = 2^k$ et posons $G = \mathrm{Gal}(N/\mathbb{Q})$, d'ordre 2^k. La propriété 7.7 fournit une chaîne de sous-groupes d'indices successifs 2 ; par le théorème fondamental, elle correspond à une tour de corps :

$$\mathbb{Q} = M_k \subseteq M_{k-1} \subseteq \cdots \subseteq M_0 = N \qquad \text{avec} \qquad [M_{i-1} : M_i] = 2$$

Chaque étage est engendré par un élément dont le polynôme minimal est de degré 2, donc par une racine carrée d'un élément de l'étage précédent. Par récurrence, la propriété 7.6 montre que tous les éléments de N, donc z, sont constructibles.

Sens direct. Supposons z constructible. Le théorème 4.5 fournit une tour quadratique $\mathbb{Q} = K_0 \subseteq \cdots \subseteq K_r \ni z$. Notons Ω le corps de décomposition sur $\mathbb{Q}$ du produit des polynômes minimaux des générateurs successifs, et de leurs conjugués. Une récurrence sur r montre que $[\Omega : \mathbb{Q}]$ est une puissance de 2 : à chaque étage, on adjoint à un corps déjà obtenu les racines d'un polynôme du second degré et de ses conjugués, ce qui multiplie le degré par une puissance de 2, le degré de chaque adjonction valant 1 ou 2. Comme $z \in \Omega$ et que $\Omega/\mathbb{Q}$ est normale, Ω

contient toutes les racines de $\mu_{z,\mathbb{Q}}$, donc $N \subseteq \Omega$; le théorème 4.1 donne alors que $[N : \mathbb{Q}]$ divise $[\Omega : \mathbb{Q}]$, donc est une puissance de 2. □

Théorème 7.7 : théorème de Gauss-Wantzel :
Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si :

$$n = 2^a\, p_1\, p_2 \cdots p_r$$

où $a \geqslant 0$ et où les p_i sont des nombres premiers de Fermat distincts, c'est-à-dire de la forme $2^{2^m} + 1$.

∘ *Démonstration :* Le polygone régulier à n côtés est constructible si et seulement si $\zeta_n = \mathrm{e}^{2\mathrm{i}\pi/n}$ l'est. Or $\mathbb{Q}(\zeta_n)$ est déjà galoisienne sur $\mathbb{Q}$ (théorème 7.2), donc $N = \mathbb{Q}(\zeta_n)$ et le théorème 7.6 s'écrit : ζ_n est constructible si et seulement si $\varphi(n)$ est une puissance de 2.

Décomposons $n = 2^a q_1^{e_1} \cdots q_r^{e_r}$ avec les q_i premiers impairs distincts. La multiplicativité de l'indicatrice donne :

$$\varphi(n) = \varphi\left(2^a\right) \prod_{i=1}^{r} q_i^{e_i - 1}\,(q_i - 1)$$

Pour que ce nombre soit une puissance de 2, il faut et il suffit que chaque $q_i^{e_i-1}$ le soit — donc que $e_i = 1$, les q_i étant impairs — et que chaque $q_i - 1$ le soit.

Reste à voir qu'un nombre premier q tel que $q - 1 = 2^s$ est de la forme $2^{2^m} + 1$. Si s admettait un diviseur impair $d > 1$, en écrivant $s = d\,t$ on aurait, par la factorisation $Y^d + 1 = (Y+1)\left(Y^{d-1} - Y^{d-2} + \cdots + 1\right)$ appliquée à $Y = 2^t$:

$$q = 2^{dt} + 1 = \left(2^t + 1\right)\left(2^{t(d-1)} - \cdots + 1\right)$$

ce qui contredirait la primalité, le premier facteur étant strictement compris entre 1 et q. Donc s est une puissance de 2. □

m	0	1	2	3
$F_m = 2^{2^m} + 1$	3	5	17	257
premier ?	oui	oui	oui	oui

m	4
F_m	65 537
premier ?	oui

Les cinq seuls nombres de Fermat premiers connus. Fermat conjecturait qu'ils l'étaient tous ; **Euler** a montré en 1732 que $F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417$ ne l'est pas, et aucun autre nombre de Fermat premier n'a été découvert depuis.

Exemple : Les polygones constructibles à moins de vingt côtés sont ceux à 3, 4, 5, 6, 8, 10, 12, 15, 16, 17 et 20 côtés. Ne le sont pas ceux à 7, 9, 11, 13, 14, 18 et 19 côtés : par exemple $\varphi(7) = 6$ et $\varphi(9) = 6$, qui ne sont pas des puissances de 2. L'impossibilité de l'heptagone régulier est ainsi tranchée par le même argument de divisibilité que la trisection de l'angle.

Le cas $n = 17$ mérite une mention : $\varphi(17) = 16 = 2^4$, donc le polygone à dix-sept côtés *est* constructible. **Gauss** l'a découvert en 1796, à dix-neuf ans, et en a donné la valeur explicite :

$$16\cos\frac{2\pi}{17} = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

On vérifie numériquement que le membre de droite vaut 14,9196, et que $16\cos\frac{2\pi}{17} = 16 \times 0{,}932472 = 14{,}9196$. Les quatre niveaux de radicaux emboîtés correspondent exactement aux quatre étages de la chaîne de sous-groupes de $\mathbb{Z}/16\mathbb{Z}$.

7.6 Le théorème fondamental de l'algèbre

Ce dernier paragraphe utilise le théorème de Sylow, démontré au chapitre 2 : *si $|G| = 2^a m$ avec m impair, alors G possède un sous-groupe d'ordre 2^a*. C'est le seul endroit du cours où il sert, et c'est pour lui que nous l'avions établi.

Théorème 7.8 : théorème fondamental de l'algèbre :
Tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

∘ *Démonstration :* Nous n'utilisons de l'analyse que deux faits, tous deux conséquences du théorème des valeurs intermédiaires :

(a) tout polynôme réel de degré *impair* possède une racine réelle, ses limites en $\pm\infty$ étant de signes opposés ;

(b) tout nombre complexe possède une racine carrée dans $\mathbb{C}$, ce que donne l'écriture trigonométrique.

Il suffit de traiter le cas d'un polynôme $P \in \mathbb{R}[X]$: pour $P \in \mathbb{C}[X]$, on considère $P\overline{P}$, qui est à coefficients réels et dont les racines contiennent celles de P.

Soit donc $P \in \mathbb{R}[X]$ non constant, et L le corps de décomposition sur $\mathbb{R}$ de $\left(X^2+1\right)P$; il contient $\mathbb{C} = \mathbb{R}(\mathrm{i})$, et l'extension $L/\mathbb{R}$ est galoisienne. Posons $G = \mathrm{Gal}(L/\mathbb{R})$ et $|G| = 2^a m$ avec m impair.

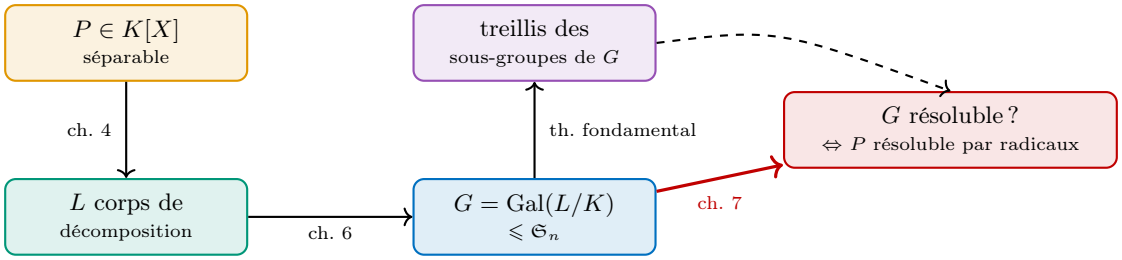
Étape 1 : $m = 1$. Soit H un sous-groupe de G d'ordre 2^a, fourni par le théorème 2.6. Le corps $M = L^H$ vérifie $[M : \mathbb{R}] = [G : H] = m$, impair. Par le théorème de l'élément primitif, $M = \mathbb{R}(\gamma)$, et $\mu_{\gamma,\mathbb{R}}$ est irréductible de degré m impair. Le fait **(a)** lui donne une racine réelle ; l'irréductibilité impose alors $m = 1$. Donc G est un groupe d'ordre 2^a.

Étape 2 : $L = \mathbb{C}$. Le groupe $G' = \mathrm{Gal}(L/\mathbb{C})$ est un sous-groupe de G, donc d'ordre 2^b. Supposons $b \geqslant 1$. La propriété 7.7 fournit un sous-groupe H' de G' d'ordre 2^{b-1}, donc d'indice 2 dans G' ; le corps $L^{H'}$ serait alors une extension de $\mathbb{C}$ de degré 2, engendrée par une racine d'un polynôme irréductible du second degré à coefficients complexes. Or un tel polynôme a toujours ses racines dans $\mathbb{C}$: la formule du discriminant s'applique, la racine carrée existant par le fait **(b)**. Contradiction. Donc $b = 0$ et $L = \mathbb{C}$.

Comme P est scindé dans $L = \mathbb{C}$, le théorème est démontré. □

Remarque : Cette démonstration, due à **Artin**, est remarquable par sa parcimonie analytique : elle n'emprunte à l'analyse que le théorème des valeurs intermédiaires, tout le reste étant de la théorie de Galois. Elle éclaire aussi l'énoncé : ce n'est pas $\mathbb{C}$ qui est miraculeux, c'est le fait que $\mathbb{R}$ n'admette pas d'extension de degré impair non triviale, et que $\mathbb{C}$ n'admette pas d'extension de degré 2.

7.7 Bilan et prolongements



Le parcours complet du cours. Partant d'un polynôme, on construit un corps, puis un groupe fini ; le théorème fondamental identifie le treillis des sous-corps à celui des sous-groupes ; et une propriété purement combinatoire de ce groupe — sa résolubilité — décide de l'existence d'une formule par radicaux.

Remarque : Quatre directions prolongent naturellement ce cours.

Le **problème inverse de Galois** demande si tout groupe fini est le groupe de Galois d'une extension de $\mathbb{Q}$. La réponse est connue pour les groupes résolubles — c'est le théorème de Šafarevič, 1954 —, pour les groupes symétriques et alternés, et pour vingt-cinq des vingt-six groupes sporadiques ; le cas général reste ouvert.

La **théorie de Galois infinie** étend la correspondance aux extensions algébriques de degré infini, comme $\overline{\mathbb{Q}}/\mathbb{Q}$. Le groupe de Galois y devient un groupe topologique compact totalement discontinu, et la correspondance ne porte plus que sur les sous-groupes *fermés* — l'ajout de la topologie de Krull restaure la bijection.

La **cohomologie galoisienne** formalise l'argument de la résolvante de Lagrange : le théorème 7.3 est un cas particulier du théorème 90 de Hilbert, qui affirme la nullité d'un premier groupe de cohomologie. Ce point de vue relie la théorie de Galois à la géométrie arithmétique et aux formes quadratiques.

Enfin la **théorie de Galois différentielle**, initiée par Picard et Vessiot, transpose toute la construction aux équations différentielles linéaires : le groupe fini y est remplacé par un groupe algébrique, et la résolubilité par radicaux par l'intégrabilité en termes de quadratures. C'est la réalisation, un siècle plus tard, de l'« application à l'analyse transcendante de la théorie de l'ambiguïté » que Galois annonçait dans la première ligne de sa lettre du 29 mai 1832.

Remarque : **Pour aller plus loin.** Les traités classiques sont ceux d'Artin (*Galois Theory*, 1942), de Lang (*Algebra*, chapitre VI) et de Escofier (*Théorie de Galois*, Dunod), ce dernier en français et très proche du présent exposé. Pour l'histoire, on lira l'édition des *Œuvres mathématiques d'Évariste Galois* (Gauthier-Villars, 1897), disponible en fac-similé, et l'analyse qu'en donne Caroline Ehrhardt dans *Évariste Galois, la fabrication d'une icône mathématique* (Éditions de l'EHESS, 2011).