Agrégation : Théorie des groupes

Cyril Demarche

21 septembre 2023

Quelques références (liste non exhaustive) :
J. Calais : Éléments de théorie des groupes
P. Garrett : Abstract Algebra (`https://www-users.cse.umn.edu/~garrett/m/algebra/Whole_with_TOC.pdf`)
X. Gourdon : Les Maths en tête, Algèbre
G. Peyré : L'algèbre discrète de la transformée de Fourier
A. Szpirglas : L3 Algèbre

Pour lectrices et lecteurs un peu plus averti·e·s, ou dans un second temps :
P. Caldero et J. Germoni : Histoires Hédonistes de groupes et de géométries (2 tomes)
D. Perrin : Cours d'algèbre

Dans ce chapitre, on suppose connues les propriétés arithmétiques élémentaires des entiers relatifs, en particulier la division euclidienne des entiers. Nous reviendrons sur ces propriétés dans un contexte plus général dans le prochain chapitre sur les anneaux euclidiens.

1 Généralités et premiers exemples

1.1 Groupes

Commençons par définir le principal objet d'étude de ce chapitre.

Définition 1.1. Un groupe est une paire $(G, \cdot)$ où G est un ensemble muni d'une loi de composition interne $G \times G \xrightarrow{\cdot} G$ vérifiant

1. pour tous $g_1, g_2, g_3 \in G$, $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.
2. il existe $e \in G$ tel que pour tout $g \in G$, $g \cdot e = e \cdot g = g$.
3. pour tout $g \in G$, il existe $h \in G$ tel que $g \cdot h = h \cdot g = e$.

Le premier axiome est appelé "associativité". L'élement e du deuxième axiome est appelé un "élément neutre". L'élément h du troisième axiome est appelé un "inverse" de g.

Exemples 1.2.
1. $(\mathbf{Z}, +)$ et $(\mathbf{R}, +)$ sont des groupes.
2. $(\mathbf{N}, +)$ n'est pas un groupe (axiome 3).
3. Si G est un singleton, il existe une unique structure de groupe sur G. On l'appelle le groupe trivial.

4. $(\mathbf{Z}, \times)$ ou $(\mathbf{R}, \times)$ ne sont pas des groupes (axiome 3).
5. $(\{\pm 1\}, \cdot)$ et $(\mathbf{R}^\times, \cdot)$ sont des groupes.
6. Si G est un ensemble de cardinal 2, le choix d'un élément e de G détermine une unique structure de groupe sur G (on pourra écrire sa table de multiplication).
7. Si $n \in \mathbf{N}$, l'ensemble $\mu_n(\mathbf{C}) := \{z \in \mathbf{C} : z^n = 1\}$ est un groupe pour la multiplication.
8. l'ensemble $\mathfrak{S}(E)$ des bijections d'un ensemble E, muni de la composition, est un groupe.
9. l'ensemble des matrices inversibles à coefficients dans un corps K, noté $\mathrm{GL}_n(K)$, muni de la multiplication des matrices, est un groupe. De même pour l'ensemble des applications linéaires inversibles $\mathrm{GL}(V)$ d'un espace vectoriel V, muni de la composition des applications.
10. L'ensemble des isométries (affines ou vectorielles) d'un plan (ou d'un espace) euclidien est un groupe pour la composition des isométries.

Proposition 1.3. *Soit $(G, \cdot)$ un groupe un ensemble muni d'une loi de composition interne assocative avec élément neutre e.*

On suppose que tout élément de G admet un inverse à droite. Alors G est un groupe.

Démonstration. Soient $g \in G$. Par hypothèse, il existe $h \in G$ tel que $g \cdot h = e$. De même, il existe $k \in G$ tel que $h \cdot k = e$.

L'associativité assure alors que

$$k = (g \cdot h) \cdot k = g \cdot (h \cdot k) = g\,,$$

donc on a l'égalité $k = g$, donc $h \cdot g = e$, ce qui assure que g admet h comme inverse à gauche et à droite. □

Proposition 1.4. *Soit $(G, \cdot)$ un groupe.*

1. *l'élement neutre de $(G, \cdot)$ est unique.*
2. *pour tout $g \in G$, l'inverse de g est unique, noté g^{-1}.*

Démonstration.

1. Soient $e, e' \in G$ deux éléments neutres. Par définition, on a $e \cdot e' = e$ et $e \cdot e' = e'$, donc $e = e'$, d'où l'unicité.
2. Soient $h, h' \in G$ deux inverses de g. L'associativité assure que $h' \cdot (g \cdot h) = (h' \cdot g) \cdot h$. Or par définition, $g \cdot h = e$ et $h' \cdot g = e$. Donc $h' \cdot e = e \cdot h$. Puisque e est neutre, on en déduit $h' = h'$, d'où l'unicité.

□

Définition 1.5. Un groupe $(G, \cdot)$ est dit commutatif, ou abélien, si pour tous $g, h \in G$, on a $g \cdot h = h \cdot g$.

Par exemple, $(\mathbf{Z}, +)$ et $(\mathbf{R}^\times, \cdot)$ sont des groupes abéliens. Le groupe $\mathfrak{S}(E)$ (resp. $\mathrm{GL}_n(K)$) est commutatif si et seulement si $|E| \leq 2$ (resp. $n \leq 1$).

1.2 Sous-groupes

Intéressons-nous maintenant à la notion de sous-objet :

Définition 1.6. Soit G un groupe. Un sous-groupe de G est une partie $P \subset G$ vérifiant

1. $P \neq \emptyset$.
2. pour tous $g, h \in P$, $g \cdot h^{-1} \in P$.

Proposition 1.7. *Une partie H de G est un sous-groupe si et seulement si $e \in H$ et H est stable par produit et par inverse, si et seulement si H est stable par la loi de G et H muni de la loi induite est un groupe.*

Démonstration. C'est une vérification immédiate. □

Exemples 1.8.

1. Pour tout groupe G, $\{e\}$ et G sont des sous-groupes de G.
2. L'ensemble $2\mathbf{Z}$ des entiers relatifs pairs est un sous-groupe de Z.
3. $\mathbf{R}^{+,\times}$ est un sous-groupe de $\mathbf{R}^{\times}$.
4. Si $F \subset E$ est une partie d'un ensemble, l'ensemble des bijections σ de $\mathfrak{S}(E)$ telle que $\sigma(F) = F$ (resp. $\sigma_{|F} = \mathrm{id}_F$) est un sous-groupe.
5. Si V est un K-espace vectoriel de dimension finie, $\mathrm{SL}(V)$ (l'ensemble des endomorphismes de déterminant 1) est un sous-groupe de $\mathrm{GL}(V)$. De même pour $\mathrm{SL}_n(K)$ qui est un sous-groupe de $\mathrm{GL}_n(K)$.
6. L'ensemble $\{A \in \mathrm{GL}_n(\mathbf{R}) : {}^tAA = A{}^tA = I_n\}$ est un sous-groupe de $\mathrm{GL}_n(\mathbf{R})$, appelé groupe orthogonal et noté $\mathbf{O}_n(\mathbf{R})$.

1.3 Morphismes

Maintenant que nous avons défini les objets (à savoir les groupes), il s'agit de définir un moyen de comparer ces objets, à savoir les morphismes entre objets.

Définition 1.9. Soient $(G, \cdot)$ et $(H, \cdot)$ deux groupes. Une application $\varphi : G \to H$ est un morphisme de groupes si et seulement si pour tous $g, g' \in G$, $\varphi(g \cdot g') = \varphi(g) \cdot \varphi(g')$.

Remarque 1.10. On notre un abus de notation classique dans cette définition : les lois de groupes sur G et sur H sont toutes les deux notée "$\cdot$", alors que l'on devrait utiliser des notations différentes (par exemple "$\cdot$" pour la première et "$\times$" pour la seconde). Notez en particulier que dans l'égalité $\varphi(g \cdot g') = \varphi(g) \cdot \varphi(g')$, la notation "$\cdot$" ne désigne pas la même loi dans le membre de gauche et dans le membre de droite.

Proposition 1.11. *Soit $\varphi : G \to H$ un morphisme de groupes. On note e (resp. e') l'élément neutre de G (resp. H).*

1. *$\varphi(e) = e'$.*
2. *pour tout $g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$.*

Démonstration.

1. On applique la définition, et plus précisément la formule $\varphi(g \cdot g') = \varphi(g) \cdot \varphi(g')$, à $g = g' = e$. On obtient $\varphi(e \cdot e) = \varphi(e) \cdot \varphi(e)$. Or $e \cdot e = e$, donc $\varphi(e) = \varphi(e) \cdot \varphi(e)$. En multipliant à gauche par l'inverse de $\varphi(e)$ dans H, on obtient $\varphi(e) = e'$.

2. On applique la formule $\varphi(g\cdot g') = \varphi(g)\cdot\varphi(g')$ à $g' = g^{-1}$. On obtient $\varphi(g\cdot g^{-1}) = \varphi(g)\cdot\varphi(g^{-1})$, donc $\varphi(e) = \varphi(g)\cdot\varphi(g^{-1})$. Or $\varphi(e) = e'$, donc $\varphi(g)\cdot\varphi(g^{-1}) = e'$. Cela assure que $\varphi(g^{-1}) = \varphi(g)^{-1}$.

□

Remarque 1.12. Si G est un groupe, la donnée d'un morphisme de groupes $\mathbf{Z} \to G$ est équivalente à la donnée d'un élément $g \in G$. Plus précisément, pour tout $g \in G$, il existe un unique morphisme $\varphi : \mathbf{Z} \to G$ tel que $\varphi(1) = g$.

Définition 1.13. On dit qu'un morphisme $\varphi : G \to H$ est un
— isomorphisme si φ est une bijection.
— endomorphisme si $H = G$.
— automorphisme si $H = G$ et φ est un isomorphisme.

Proposition 1.14. *Soit $\varphi : G \to H$ un isomorphisme. Alors $\varphi^{-1} : H \to G$ est un morphisme de groupes.*

Définissons deux sous-groupes naturellement associés à un morphisme de groupes :

Définition 1.15. Soit $\varphi : G \to H$ un morphisme de groupes.
Le noyau de φ, noté $\ker(\varphi)$, est $\varphi^{-1}(\{e'\})$. L'image de φ, notée $\mathrm{im}\,(\varphi)$, est $\varphi(G)$.

Proposition 1.16. *Soit $\varphi : G \to H$ un morphisme de groupes.*
Alors $\ker(\varphi)$ *(resp.* $\mathrm{im}\,(\varphi)$*) est un sous-groupe de G (resp. H).*

Démonstration. Puisque $\varphi(e) = e'$, on a bien $e \in \ker(\varphi)$ et $e' \in \mathrm{im}\,(\varphi)$.
Soient $g, h \in \ker(\varphi)$. Alors

$$\varphi(g \cdot h^{-1}) = \varphi(g) \cdot \varphi(h)^{-1} = e' \cdot e' = e' \,,$$

donc $g \cdot h^{-1} \in \ker(\varphi)$, ce qui assure que $\ker(\varphi)$ est un sous-groupe.
Soient $g', h' \in \mathrm{im}\,(\varphi)$. Il existe $g, h \in G$ tels que $g' = \varphi(g)$ et $h' = \varphi(h)$. Alors

$$g' \cdot h'^{-1} = \varphi(g) \cdot \varphi(h)^{-1} = \varphi(g \cdot h^{-1}) \,,$$

donc $g' \cdot h'^{-1} \in \mathrm{im}\,(\varphi)$, ce qui assure que $\mathrm{im}\,(\varphi)$ est un sous-groupe. □

Exemples 1.17.
1. Le noyau de la réduction modulo 2, à savoir $\varphi : \mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ est exactement le sous-groupe $2\mathbf{Z}$.
2. Le noyau du morphisme "signe" $\mathbf{R}^\times \to \{\pm 1\}$ est le sous-groupe $\mathbf{R}^{+,\times}$.
3. Le sous-groupe $\mathrm{SL}_n(K)$ est le noyau du morphisme déterminant $\det : \mathrm{GL}_n(K) \to K^\times$.
4. $\mu_n(\mathbf{C})$ est le noyau du morphisme $\mathbf{C}^\times \to \mathbf{C}^\times$ défini par $z \mapsto z^n$.

2 Constructions de groupes

2.1 Produit direct

Définition 2.1. Soit $(G_i)_{i\in I}$ une famille de de groupes indicée par un ensemble I. On définit le produit direct des groupes (G_i), et on note $\prod_{i\in I} G_i$, le groupe dont l'ensemble sous-jacent est le produit cartésien $\prod_{i\in I} G_i$ et dont la loi est définie par

$$(g_i)_{i\in I} \cdot (h_i)_{i\in I} := (g_i \cdot h_i)_{i\in I} \,.$$

La lectrice attentive pourra vérifier que cela définit bien une loi de groupe. On dispose de morphismes de groupes naturels $\pi_j : \prod_{i\in I} G_i \to G_j$ et $\iota_j : G_j \to \prod_{i\in I} G_i$, pour tout $j \in I$.

La propriété fondamentale du groupe produit est la suivante :

Proposition 2.2. *Soit $(G_i)_{i\in I}$ une famille de groupes. Soient $\varphi_i : G \to G_i$ des morphismes de groupes. Alors il existe un unique morphisme de groupes $\varphi : G \to \prod_{i\in I} G_i$ tel que pour tout $j \in J$, $\varphi_j = \pi_j \circ \varphi$.*

Démonstration. Pour l'unicité, on voit qu'un morphisme φ satisfaisant l'énoncé doit vérifier, pour tout $g \in G$, $\varphi(g) = (\varphi_i(g))_{i\in I}$, d'où l'unicité. Pour l'existence, on vérifie que la formule précédente définit bien un morphisme de groupes, ce qui est clair. □

2.2 Hors programme : produit semi-direct

Définition 2.3. Soit N, H deux groupes, et $\rho : H \to \mathrm{Aut}(N)$ un morphisme de groupes. On définit $G := N \rtimes_\rho H$ comme l'ensemble $N \times H$ muni de la loi de composition interne $(n, h) \cdot (n', h') := (n\rho(h)(n'), hh')$. Alors G est un groupe, le produit semi-direct de H par N.

Exemples 2.4. Le groupe diédral D_n des isométries du polygone régulier à n côtés est isomorphe à $\mathbf{Z}/n\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$. Le groupe $\mathfrak{S}_3$ est isomorphe à $\mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$.

Exemples 2.5.
— classification des groupes d'ordre ≤ 15.
— classification des groupes d'ordre pq, p^3, avec p et q premiers.
— description du groupe affine d'un espace affine.

2.3 Sous-groupe engendré

Définition 2.6. Soit G un groupe et $P \subset G$ une partie de G.

Le sous-groupe engendré par P est le plus petit sous-groupe de G contenant P. On le note $\langle P \rangle$.

L'existence et l'unicité de ce sous-groupe n'est pas complètement évidente et mérite une démonstration. On propose deux descriptions explicites de ce sous-groupe, qui démontrent cela, dans la proposition qui suit.

Lemme 2.7. *Soit G un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de G.*

Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Démonstration. L'élément neutre appartient à chacun des H_i, donc aussi à $\bigcap_{i\in I} H_i$. Pour tous $x, y \in \bigcap_{i\in I} H_i$, pour tout $i \in I$, on a $x, y \in H_i$, donc $x \cdot y^{-1} \in H_i$, donc $x \cdot y^{-1} \in \bigcap_{i\in I} H_i$. □

Proposition 2.8. *Soit G un groupe et $P \subset G$ une partie de G.*

Alors

$$\langle P \rangle = \bigcap_{\substack{H < G \\ P \subset G}} H$$

et

$$\langle P \rangle = \bigcup_{n\in\mathbf{N}} \{g_1 \dots g_n\,,\ \forall i, g_i \in P \text{ ou } g_i^{-1} \in P\}\,.$$

Démonstration. Le lemme précédent assure que la première formule définit un sous-groupe de G contenant P, et par construction, c'est le plus petit possible (il est contenu dans tout sous-groupe contenant P).

La seconde formule définit bien un sous-groupe de G (le vérifier), qui contient P. Et par définition d'un sous-groupe, tout sous-groupe contenant P doit contenir le sous-ensemble défini par cette seconde formule. □

La propriété fondamentale du sous-groupe engendré par une partie est la suivante (elle est tout à fait analogue à la propriété similaire en algèbre linéaire, affirmant qu'une application linéaire est complètement déterminée par une partie génératrice) :

Proposition 2.9. *Soit P une partie d'un groupe G, et G' un groupe.*

Un morphisme de groupes $\varphi : \langle P\rangle \to G'$ est complètement déterminé par sa restriction à P. Autrement dit, si $\varphi, \varphi' : \langle P\rangle \to G'$ sont deux morphismes de groupes, on a $\varphi = \varphi'$ si et seulement si $\varphi_{|P} = \varphi'_{|P}$.

Démonstration. Il suffit d'utiliser la seconde description de la proposition 2.8. □

Définition 2.10.
- Un groupe est dit de type fini s'il admet une partie génératrice finie.
- Un groupe est dit monogène s'il admet une partie génératrice formée d'un seul élément.
- Un groupe est dit cyclique s'il est monogène et fini.

Remarque 2.11. La première définition est l'analogue de la notion de dimension finie en algèbre linéaire. C'est une notion beaucoup plus subtile en théorie des groupes. Par exemple, les lectrices sont invitées à chercher des exemples de sous-groupes de groupe de type fini qui ne sont pas de type fini.

Exemples 2.12.
- Le groupe $\mathbf{Z}$ est monogène.
- Les groupes $\mathbf{Z}^2$ ou $(\mathbf{Z}/2\mathbf{Z})^2$ ne sont pas monogènes.
- Le groupe $\mathbf{Z}/n\mathbf{Z}$ est cyclique.
- Pour tout $n \in \mathbf{N}$, le groupe $\mathbf{Z}^n$ est de type fini.
- Tout groupe fini est de type fini.
- Les groupes $\mathbf{Q}$ et $\mathbf{R}$ ne sont pas de type fini.

Définition 2.13. Soit G un groupe et $x \in G$.

L'ordre de x dans G est le cardinal du sous-groupe $\langle x\rangle$. Si cet ordre est fini, c'est le plus petit entier $n \geq 1$ tel que $x^n = e$.

2.4 Quotients

Commençons par quelques rappels sur les quotients dans un contexte plus général.

Définition 2.14. Soit X un ensemble muni d'une relation d'équivalence $\sim$.

On définit l'ensemble quotient de X par la relation $\sim$, noté $X/\sim$, comme l'ensemble des classes d'équivalence dans X pour $\sim$.

Exemples 2.15.
- Si $\sim$ est la relation d'égalité, alors $X/\sim$ est en bijection canonique avec X.
- Si $\sim$ est la relation totale, où $x \sim y$ pour tous $x, y \in X$, alors $X/\sim$ est un ensemble à un élément, i.e. $X/\sim = \{X\}$.

— Si $X = \mathbf{Z}$ et $n \sim m$ si et seulement si $n - m$ est pair, alors $X/\sim$ est un ensemble à deux éléments (l'ensemble des nombres pairs, et l'ensemble des nombres impairs), noté $\mathbf{Z}/2\mathbf{Z}$.
— Si X est l'ensemble des étudiants de la classe, et $\sim$ est la relation "être né la même année", je vous laisse calculer l'ensemble quotient.

On dispose d'une application canonique surjective $\pi : X \to X/\sim$, appelée surjection (ou projection) canonique, ou encore application quotient. Cette application envoie un élément $x \in X$ sur sa classe d'équivalence $\pi(x) = \overline{x}$, qui est bien un élément de $X/\sim$. Réciproquement, pour tout élément $y \in X/\sim$, y est la classe d'équivalence d'un élément $x \in X$ (pas unique en général) et $\pi^{-1}(y)$ est la classe d'équivalence de x, vue comme une partie de X.

L'ensemble $X/\sim$ est plus petit, plus "simple", que l'ensemble X (au moins en cardinalité). On peut donc essayer d'étudier un ensemble X complexe à partir de l'ensemble plus simple $X/\sim$ et des fibres de l'application $\pi : X \to X/\sim$ (qui sont également plus petites que X).

Si on essaie d'adapter cette stratégie à la théorie des groupes, on peut essayer d'étudier un groupe complexe G à l'aide d'un sous-groupe plus petit H et du quotient G/H, à condition que ce dernier quotient ait un sens. Et pour rester dans le monde des groupes, on souhaiterait également que ce quotient G/H soit un groupe, et que $\pi : G \to G/H$ soit un morphisme de groupes. Nous allons voir que ce n'est pas si évident que cela.

Définition 2.16. Soit G un groupe et $H < G$ un sous-groupe.

On définit la relation binaire $\sim_H$ sur G de la façon suivante : pour tout $g, g' \in G$, on dit que $g \sim_H g'$ si et seulement si $g^{-1} \cdot g' \in H$.

Proposition 2.17. *La relation $\sim_H$ est une relation d'équivalence sur G. Pour tout $g \in G$, la classe d'équivalence de g est $gH \subset G$, appelée classe à gauche de g modulo H.*

L'ensemble quotient $G/\sim_H$ est noté G/H.

Démonstration. La relation est réflexive car $e \in H$. Elle est symétrique car H est stable par inverse, et elle est transitive car H est stable par produit. □

Remarque 2.18. On peut formuler une définition et une proposition symétrique en échangeant droite et gauche : la relation $\sim'$ définie par $g \sim' g'$ si et seulement si $g'g^{-1} \in H$ est une relation d'équivalence, les classes d'équivalence sont les classes à droite Hg, et l'ensemble quotient est noté $H\backslash G$.

On dispose alors d'une bijection canonique $G/H \xrightarrow{\sim} H\backslash G$ définie par $gH \mapsto Hg^{-1}$ (dont on laisse le soin au lecteur de vérifier qu'elle est bien définie). Cette bijection assure que le choix de convention entre droite et gauche est sans conséquence pour toute la théorie qui suit.

Remarquons que toutes les classes d'équivalence (les classes à gauche) sont en bijection : en effet, si $g, g' \in G$, alors l'application $gH \to g'H$ définie par $x \mapsto g'g^{-1}x$ est une bijection. En particulier, toutes les classes ont le même cardinal. Puisqu'elles partionnent le groupe G, on en déduit le

Théorème 2.19 (Lagrange)**.** *Soit G un groupe fini et H un sous-groupe de G.*

Alors le cardinal de H divise celui de G.

Démonstration. Les classes d'équivalence forment une partition de G, donc G est la réunion disjointe des classes à gauche gH. Or toutes ces classes sont en bijection avec H. Par conséquent,

$$|G| = |G/H| \cdot |H| \,.$$

□

Cela justifie la définition suivante, ainsi que la dernière égalité ci-dessous :

Définition 2.20. Soit G un groupe et $H < G$ un sous-groupe.

L'indice de H dans G, noté $[G : H]$, est le cardinal de l'ensemble quotient G/H.

Si G est un groupe fini, alors $[G : H] = |G/H| = \frac{|G|}{|H|}$.

Comme rappelé plus haut, on dispose d'une application surjective canonique $\pi : G \to G/H$, définie par $\pi(g) := gH$.

Afin de dévisser le groupe G en deux groupes "plus simples" H et G/H, on souhaite munir l'ensemble G/H d'une structure de groupes, de sorte que π soit un morphisme de groupes. Puisque π est surjective, une telle loi de groupe sur G/H est unique, puisqu'elle doit vérifier $\pi(g \cdot g') = \pi(g) \cdot \pi(h)$.

Proposition 2.21. *Soit G un groupe et $H < G$ un sous-groupe.*

Il existe une structure de groupes (nécessairement unique) sur G/H de sorte que $\pi : G \to G/H$ soit un morphisme de groupes si et seulement si pour tout $g \in G$, on a $gH = Hg$ si et seulement si pour tout $g \in G$, $gHg^{-1} = H$.

Démonstration.

— Unicité : soit $*$ une loi de groupe sur G/H satisfaisant les hypothèses de l'énoncé. Alors pour tous $g, g' \in G$, on a $\pi(g \cdot g') = \pi(g) * \pi(g')$. Puisque π est surjective, cette formule détermine complètement la loi $*$ à partir de la loi $\cdot$, qui est donnée, ce qui assure son unicité.

— existence : on souhaite définir une loi de composition sur G/H via la formule précédente, à savoir pour tous $\bar{g}, \bar{g}' \in G/H$,

$$\bar{g} * \bar{g}' := \pi(g \cdot g') \,,$$

où $g \in G$ (resp. $g' \in G$) désigne un antécédent de $\bar{g}$ (resp. $\bar{g}'$) par π. A priori, la loi $*$ n'est pas bien définie, puisque un élément $\bar{g} \in G/H$ a en général plusieurs antécédents par π, et la formule précédente pourrait dépendre du choix d'un tel antécédent.

La loi $*$ est bien définie si et seulement si pour tous $\bar{g}, \bar{g}' \in G/H$, l'élément $\bar{g} * \bar{g}' := \pi(g \cdot g')$ ne dépend pas du choix des représentants g et g' si et seulement si pour tous $g, g' \in G$, pour tous $h, h' \in G$, $\pi(g \cdot g') = \pi((g \cdot h) \cdot (g' \cdot h'))$ si et seulement si pour tous $g, g' \in G$, pour tout $h \in G$, $g \cdot g' \cdot g'^{-1} \cdot h^{-1} \cdot g^{-1} \in H$ si et seulement si pour tout $g \in G$, pour tout $h \in G$, $g \cdot h \cdot g^{-1} \in H$ si et seulement si pour tout $g \in G$, $gHg^{-1} \subset H$ si et seulement si pour tout $g \in G$, $gHg^{-1} = H$. Cela conclut la preuve de l'existence.

□

La proposition précédente motive la définition suivante :

Définition 2.22. Soit G un groupe et $H < G$ un sous-groupe.

On dit que H est distingué dans G, et on note $H \lhd G$, si pour tout $g \in G$, $gHg^{-1} = H$ (H est stable par conjugaison), ce qui équivaut à $gH = Hg$ (les classes à gauche coïncident avec les classes à droite).

Exemples 2.23. — les sous-groupes triviaux $\{e\}$ et G sont distingués dans G. Les quotients correspondants sont isomorphes à G et au groupe trivial.
— si G est abélien, tout sous-groupe est distingué.
— si G est un groupe, on définit son centre $Z(G)$ de la façon suivante :

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

C'est un sous-groupe commutatif de G, qui est distingué dans G.

Exemple 2.24. Soit $n \in N$, $n \geq 1$. L'ensemble $n\mathbf{Z}$ des entiers multiples de n est un sous-groupe de $\mathbf{Z}$, et le quotient $\mathbf{Z}/n\mathbf{Z}$ est un groupe cyclique (il est engendré par la classe de 1) de cardinal n.

Une notion plus forte que celle de sous-groupe distingué, qui peut-être utile dans certains contextes :

Définition 2.25. Soit G un groupe et $H < G$ un sous-groupe.

On dit que H est caractéristique dans G si pour tout automorphisme φ de G, on a $\varphi(H) \subset H$. Un tel groupe est évidemment distingué.

Proposition 2.26. *Soit $\varphi : G \to G'$ un morphisme de groupes.*

Alors $\ker(\varphi)$ *est distingué dans G.*

Plus généralement, pour tout sous-groupe $H < G$, H est distingué si et seulement s'il existe un groupe G' et un morphisme $\varphi : G \to G'$ tels que $H = \ker(\varphi)$.

Démonstration. Pour tout $g \in G$, pour tout $h \in \ker(\varphi)$, on a $\varphi(h) = e'$ et donc

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e'\,,$$

donc $ghg^{-1} \in \ker(\varphi)$.

Pour la réciproque, il suffit de remarquer qu'un sous-groupe distingué H de G est le noyau de la surjection canonique $\pi : G \to G/H$. □

Proposition 2.27. *Soit G un groupe et $H \subset G$ un sous-groupe.*

Si H est d'indice 2 dans G, alors H est distingué dans G.

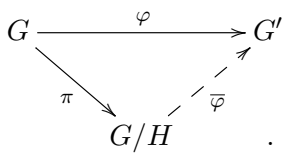
Démonstration. Soit $g \in G \setminus H$. Comme H est d'indice 2 dans G, $G/H = \{H, gH\}$. Comme G/H et $H\backslash G$ ont même cardinal, on voit que $H\backslash G = \{H, Hg\}$ (on rappelle que $g \notin H$). Enfin, G est la réunion disjointe des classes à gauche (resp. à droite), ce qui assure que $gH = Hg$. Cela suffit à assurer que $H \lhd G$. □

La propriété fondamentale du groupe quotient est la propriété universelle suivante :

Théorème 2.28. *Soit $H \lhd G$ un sous-groupe distingué et $\varphi : G \to G'$ un morphisme de groupes.*

Alors $H \subset \ker(\varphi)$ si et seulement s'il existe un unique morphisme de groupes $\overline{\varphi} : G/H \to G'$ tel que $\varphi = \overline{\varphi} \circ \pi$, où $\pi : G \to G/H$ désigne le morphisme quotient.

Autrement dit, $H \subset \ker(\varphi)$ si et seulement s'il existe un unique morphisme de groupes $\overline{\varphi} : G/H \to G'$ tel que le diagramme suivant commute :



.

Démonstration. Un sens de l'équivalence est évident : s'il existe un tel morphisme $\overline{\varphi}$, alors $\ker(\pi) \subset \ker(\varphi)$, i.e. $H \subset \ker(\varphi)$.

La réciproque est plus importante, et moins évidente. Supposons donc que $H \subset \ker(\varphi)$, et construisons $\overline{\varphi}$. Tout d'abord, l'unicité de $\overline{\varphi}$ est claire, puisqu'on doit avoir, pour tout $g \in G$, $\overline{\varphi}(\pi(g)) = \varphi(g)$, donc $\overline{\varphi}$ est complètement déterminée par les données π et φ, puisque π est surjective. Reste à montrer l'existence de $\overline{\varphi}$. Pour cela, on pose pour tout $\bar{g} \in G/H$, $\overline{\varphi}(\bar{g}) := \varphi(g)$ où $g \in G$ est un relevé quelconque de $\bar{g}$. Cette application est bien définie si et seulement si pour tout $\bar{g} \in G/H$, $\varphi(g)$ ne dépend pas du relevé $g \in G$ de $\bar{g}$ choisi, si et seulement si, pour tout $g \in G$, pour tout $h \in H$, on a $\varphi(g) = \varphi(g \cdot h)$, si et seulement si (puisque φ est un morphisme) pour tout $h \in H$, $\varphi(h) = e'$ si et seulement si $H \subset \ker(\varphi)$. On a donc bien défini l'application $\overline{\varphi}$ vérifiant $\varphi = \overline{\varphi} \circ \pi$. On vérifie pour finir que $\overline{\varphi}$ est bien un morphisme de groupes.

Cela conclut la preuve. □

On en déduit le corollaire suivant, souvent appelé premier théorème d'isomorphisme :

Corollaire 2.29. *Soit $\varphi : G \to G'$ un morphisme de groupes.*
Alors φ induit un isomorphisme de groupes

$$\overline{\varphi} : G/\ker(\varphi) \xrightarrow{\sim} \mathrm{im}\,(\varphi)\,.$$

Démonstration. Il suffit d'appliquer le théorème 2.28 à $H := \ker(\varphi)$ pour en déduire l'existence d'un morphisme $\overline{\varphi} : G/\ker(\varphi) \to G'$ tel que $\varphi = \overline{\varphi} \circ \pi$. Puisque π est surjectif, le morphisme $\overline{\varphi}$ a même image que φ, donc il induit un morphisme sujectif $\overline{\varphi} : G/\ker(\varphi) \to \mathrm{im}\,(\varphi)$. Montrons son injectivité : soit $\bar{g} \in \ker(\overline{\varphi})$. On a $\overline{\varphi}(g) = e'$, donc si $g \in G$ est un relevé de $\bar{g}$ (i.e. $\pi(g) = \bar{g}$), on a $\overline{\varphi}(\pi(g)) = e'$, i.e. $\varphi(g) = e'$, donc $g \in \ker(\varphi) = H$, donc $\bar{g} = \pi(g)$ est également à l'élément neutre $\bar{e}$ de G/H, d'où l'injectivité souhaitée. □

La conséquence suivante est un analogue du théorème du rang en algèbre linéaire :

Corollaire 2.30. *Soit G un groupe fini et $\varphi : G \to G'$ un morphisme de groupes.*
Alors $|G| = |\ker(\varphi)||\mathrm{im}\,(\varphi)|$.

Démonstration. Le corollaire 2.29 assure que $|G/\ker(\varphi| = |\mathrm{im}\,(\varphi)|$. Or le théorème de Lagrange (cf théorème 2.19 et définition 2.20) assure que $|G/\ker(\varphi)| = \frac{|G|}{|\ker(\varphi)|}$, ce qui assure le résultat. □

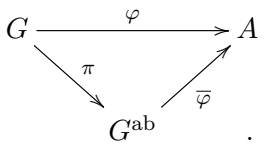
Exemple 2.31. Soit G un groupe.

Si $g, h \in G$, le commutateur de g et h est défini comme $[g, h] := ghg^{-1}h^{-1}$. De façon évidente, g et h commutent si et seulement si $[g, h] = e$.

On définit son sous-groupe dérivé $D(G)$ comme le sous-groupe de G engendré par les commutateurs. Par exemple, $D(G) = \{e\}$ si et seulement si G est abélien.

On vérifie (exercice) que $D(G)$ est distingué dans G, et on définit l'abélianisé de G comme étant le groupe quotient $G^{\mathrm{ab}} := G/D(G)$. Par définition de $D(G)$ et par propriété universelle du quotient, le groupe G^{ab} est le plus grand quotient abélien de G ; plus précisément, pour tout morphisme de groupes $\varphi : G \to A$ où A est un groupe

abélien, il existe un unique morphisme $\overline{\varphi} : G^{\mathrm{ab}} \to A$ tel que le diagramme suivant commute



Un groupe est dit parfait si $D(G) = G$, i.e. si $G^{\mathrm{ab}} = \{e\}$. C'est le cas par exemple d'un groupe simple non abélien (cf ci-dessous).

Définition 2.32. Soit G un groupe. Le groupe G est simple si G n'est pas trivial et si les seuls sous-groupes distingués de G sont $\{e\}$ et G.

Proposition 2.33. *Soit G un groupe abélien.*
Alors G est simple si et seulement si $G \simeq \mathbf{Z}/p\mathbf{Z}$ pour un nombre premier p.

Démonstration. Le théorème de Lagrange assure que si p est premier, $\mathbf{Z}/p\mathbf{Z}$ est un groupe simple. Réciproquement, soit G un groupe abélien simple. Soit $g \in G \setminus \{e\}$. Le sous-groupe $\langle g \rangle$ de G est distingué et non réduit à $\{e\}$, donc par simplicité il est égal à G. Donc G est monogène. Si G est infini, il est isomorphe à $\mathbf{Z}$, qui contient le sous-groupe (distingué) strict $2\mathbf{Z}$, et donc il n'est pas simple. Si $G = langleg\rangle$ est fini, il est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ pour un certain entier $n \geq 2$ (n est l'ordre de g). Si n n'est pas premier, il existe $d, k \geq 2$ entiers tels que $n = dk$. Alors $\langle g^k \rangle$ est un sous-groupe strict de G (d'ordre d), donc G n'est pas simple. □

3 Groupes abéliens de type fini

3.1 Groupes monogènes

L'objectif de cette sous-partie est de faire la liste de tous les groupes monogènes (à isomorphisme près).

Proposition 3.1. *Soit $H < \mathbf{Z}$ un sous-groupe.*
Alors il existe $n \in \mathbf{N}$ tel que $H = n\mathbf{Z}$.

Autrement dit, les sous-groupes de $\mathbf{Z}$ sont exactement les $n\mathbf{Z}$, avec $n \in \mathbf{N}$.

Démonstration. On suppose $H \neq \{0\}$. Puisque H est stable par inverse (i.e. par opposé pour la loi $+$), H contient un entier strictement positif. La partie $H \cap \mathbf{N}_{>0}$ de N est non vide, elle admet donc un plus petit élément noté n. Par définition, $n > 0$ et $n \in H$. Soit $a \in H$. On fait la division euclidienne de a par n : il existe $q \in \mathbf{Z}$ et $r \in \mathbf{N}$ tels que $a = nq + r$ et $0 \leq r < n$. Donc $r = a - nq$. Puisque $a, n \in H$, on voit que $r \in H$. Puisque $r < n$, on a nécessairement $r \leq 0$ par minimalité de n. donc $r = 0$ et $a = nq$. Donc $a \in n\mathbf{Z}$, donc $H \subset n\mathbf{Z}$. Comme $n \in H$ et H est un sous-groupe, H contient le sous-groupe $n\mathbf{Z}$ engendré par n. Donc $H = n\mathbf{Z}$. □

Théorème 3.2. *Soit G un groupe monogène.*
- *Si G est infini, alors G est isomorphe à $\mathbf{Z}$.*
- *Si G est fini de cardinal n, alors G est isomorphe à $\mathbf{Z}/n\mathbf{Z}$. On dit que G est cyclique (monogène fini).*

Remarque 3.3. Dans les deux cas, les isomorphismes ne sont pas canoniques : ils dépendent du choix d'un générateur. Nous étudierons les générateurs des groupes monogènes plus bas.

Démonstration. Par définition, il existe $g_0 \in G$ tel que $G = \langle g_0 \rangle$. On considère alors l'application $\varphi : \mathbf{Z} \to G$ définie par $\varphi(k) := g_0^k$. Il est clair que φ est un morphisme de groupes, et il est surjectif puisque g_0 est un générateur. Donc le corollaire 2.29 assure que φ induit un isomorphisme $\overline{\varphi} : \mathbf{Z}/\ker(\varphi) \xrightarrow{\sim} G$. En outre, la proposition 3.1 assure qu'il existe $n_0 \in \mathbf{N}$ tel que $\ker(\varphi) = n_0\mathbf{Z}$. On a alors l'alternative suivante :

— si $n_0 = 0$, alors on a un isomorphisme $\overline{\varphi} : \mathbf{Z} \xrightarrow{\sim} G$ et G est infini.
— si $n_0 > 0$, alors on a un isomorphisme $\overline{\varphi} : \mathbf{Z}/n_0\mathbf{Z} \xrightarrow{\sim} G$ et G est fini de cardinal n_0.

□

Exemple 3.4. Par exemple, le groupe $\mu_n(\mathbf{C})$ des racines n-ièmes de l'unité dans $\mathbf{C}$ est cyclique de cardinal n, engendré par $e^{\frac{2i\pi}{n}}$. On en déduit que les groupes $\mu_n(\mathbf{C})$ et $\mathbf{Z}/n\mathbf{Z}$ sont isomorphes (non canoniquement si $n \geq 3$). La donnée d'un tel isomorphisme équivaut à celle d'un générateur de $\mu_n(\mathbf{C})$, i.e. à celle d'une racine primitive n-ième de l'unité.

Proposition 3.5. *Soit p un nombre premier.*
Alors tout groupe de cardinal p est cyclique.

Démonstration. Puisque $p \geq 2$, il existe $g \in G \setminus \{e\}$. Alors le sous-groupe $\langle g \rangle$ engendré par g a un cardinal compris entre 2 et p, et par le théorème de Lagrange (cf théorème 2.19), ce cardinal divise p. Donc ce cardinal est égal à p, donc $G = \langle g \rangle$ et G est cyclique (engendré par tout élément de G distinct de e). □

Proposition 3.6. *Soit G un groupe cyclique de cardinal n.*
Tout sous-groupe et tout quotient de G est cyclique. Pour tout diviseur d de n, il existe un unique sous-groupe de G (resp. un unique quotient de G) de cardinal d.

Démonstration. Soit H un sous-groupe de $G = \langle g \rangle$ et Q un quotient de G. Puisque le morphisme quotient $\pi : G \to Q$ est surjectif, le groupe Q est engendré par $\pi(g)$ et il est fini, donc il est cyclique.

Notons n et d les cardinaux respectifs de G et H. Par le théorème 2.19 (Lagrange), d divise n. Notons alors $g' := g^{\frac{n}{d}}$. Il suffit de montrer que $H = \langle g' \rangle$. Puisque g est d'ordre n, le lecteur vérifiera que g' est d'ordre d, donc il suffit de montrer que $g' \in H$. Par définition, G/H est de cardinal $\frac{n}{d}$, donc g' a une image trivial dans G/H, donc $g' \in H$, ce qui conclut la preuve. □

Exemple 3.7. Dans le cas d'un groupe monogène infini, donc isomorphe à $\mathbf{Z}$, on voit facilement que ce groupe admet exactement deux générateurs, qui sont inverses l'un de l'autre. Dans le groupe $\mathbf{Z}$, ce sont 1 et -1.

Dans le cas de $\mathbf{Z}/n\mathbf{Z}$, l'étude des générateurs est plus intéressante. Nous y reviendrons dans le début du cours sur les anneaux.

3.2 Groupes abéliens finis

On souhaite poursuivre la classification des groupes entamée à la sous-section précédente. On s'intéresse désormais aux groupes abéliens finis, qui sont une généralisation naturelle des groupes cycliques. Peut-on lister tous les groupes abéliens finis ?

Afin de répondre à cette question, on commence par définir et étudier les caractères des groupes abéliens finis, et la dualité associée. Cette dualité fait écho à la dualité en algèbre linéaire, que nous reverrons prochainement.

Définition 3.8. Soit G un groupe. Un caractère (complexe) de G est un morphisme de groupes $\chi : G \to \mathbf{C}^\times$.

Proposition 3.9. *Soit G un groupe.*

L'ensemble des caractères de G, noté $\widehat{G}$, est naturellement un groupe abélien pour la multiplication des caractères, appelé groupe dual de G.

Démonstration. Il suffit de vérifier que si $\chi, \chi' : G \to \mathbf{C}^\times$ sont des morphismes de groupes, alors $\chi\chi' : G \to \mathbf{C}^\times$, défini par $(\chi\chi')(g) := \chi(g)\chi(g')$, est un morphisme de groupes. L'élément neutre de $\widehat{G}$ est le caractère trivial $\chi_0 : G \to \mathbf{C}^\times$ défini par $\chi_0(g) = 1$ pour tout $g \in G$. □

Exemple 3.10. Si $G = \mathbf{Z}/n\mathbf{Z}$, alors $\widehat{G}$ est canoniquement isomorphe au groupe μ_n des racines n-ièmes de l'unité dans $\mathbf{C}$, via l'isomorphisme $\psi : \widehat{G} \xrightarrow{\sim} \mu_n$ défini par $\psi(\chi) := \chi(1)$. En particulier, le choix d'une racine primitive n-ième de l'unité dans $\mathbf{C}$ induit un isomorphisme $\widehat{\mathbf{Z}/n\mathbf{Z}} \xrightarrow{\sim} \mathbf{Z}/n\mathbf{Z}$.

Remarquons qu'un morphisme de groupes $\varphi : G \to G'$ induit naturellement un morphisme de groupes $\widehat{\varphi} : \widehat{G'} \to \widehat{G}$ défini par $\widehat{\varphi}(\chi') := \chi' \circ \varphi$; cette dualité sur les morphismes de groupes respecte en outre la composition : si $G \xrightarrow{\varphi} G' \xrightarrow{\psi} G''$ sont des morphismes de groupes, alors $\widehat{\psi \circ \varphi} = \widehat{\varphi} \circ \widehat{\psi}$. La dualité agit donc à la fois sur les groupes et sur les morphismes de groupes.

Proposition 3.11. *Si $\varphi : G \to G'$ est surjectif, alors $\widehat{\varphi} : \widehat{G'} \to \widehat{G}$ est injectif.*

Démonstration. Soit $\chi' \in \ker(\widehat{\varphi})$. Alors $\chi' \circ \varphi = 1$, donc χ' est trivial sur l'image de φ. Or par hypothèse φ est surjectif, donc χ' est trivial sur tout G', donc $\chi' = 1$, d'où l'injectivité souhaitée. □

En revanche, il n'est pas vrai en général que si φ est injectif, alors $\widehat{\varphi}$ est surjectif. Par exemple, pour l'inclusion $\varphi : G = \mathbf{Z}/3\mathbf{Z} \cong \mathfrak{A}_3 \subset \mathfrak{S}_3 = G'$, le morphisme $\widehat{\varphi} : \mu_2 \cong \widehat{G'} \to \widehat{G} \cong \mu_3$ est le morphisme nul.

Cependant, dans le cas particulier des groupes abéliens finis, le résultat est vrai :

Théorème 3.12 (Prolongement des caractères)**.** *Soient G un groupe abélien fini et $H < G$ un sous-groupe.*

Alors le morphisme naturel $\widehat{G} \to \widehat{H}$ est surjectif, i.e. tout caractère de H se prolonge en un caractère de G, d'exactement $[G : H]$ façons différentes. En outre, le noyau du morphisme $\widehat{G} \to \widehat{H}$ est isomorphe à $\widehat{G/H}$.

Démonstration. Soit $\chi \in \widehat{H}$. Montrons par récurrence (forte) sur $n = [G : H]$ que χ se prolonge à G.

1. Si $n = 1$, alors $H = G$ et le résultat est évident.
2. Soit $n > 1$ et supposons le résultat montré pour tous les groupes G' et tous les sous-groupes H' de G' d'indice compris entre 1 et $n-1$. Il existe $g \in G \setminus H$, et on dispose des inclusions suivantes de sous-groupes : $H < H' := \langle H, g\rangle < G$. Si la second inclusion est stricte, alors l'hypothèse de récurrence assure que χ se prolonge de $[H' : H]$ façons différentes à H', et chacun de ces prolongements se prolonge de $[G : H']$ façons différentes à G, ce qui assure que χ se prolonge d'exactement $[G : H] = [G : H'] \cdot [H' : H]$ façons différentes à G, ce qui assure l'hérédité dans ce cas.

   Reste à traiter le cas où $G = \langle H, g\rangle$. Notons $k \geq 2$ l'entier minimal tel que $g^k \in H$ (k est l'exposant, ou l'ordre, du quotient cyclique G/H, i.e. $k = [G : H]$). Alors tout élément de G s'écrit de façon unique (exercice) sous la forme $h \cdot g^i$, avec $0 \leq i \leq k-1$. Nécessairement, si χ' est un caractère de G étendant χ, on doit avoir $\chi'(g)^k = \chi(g^k)$ et $\chi'(h \cdot g^i) := \chi(h) \cdot \chi'(g)^i$.

   Fixons donc ω une racine k-ième de $\chi(g^k)$ dans $\mathbf{C}$, et définissons une application $\chi' : G \to \mathbf{C}^\times$ prolongeant $\chi : H \to \mathbf{C}^\times$, de la façon suivante :

$$\chi'(h \cdot g^i) := \chi(h) \cdot \omega^i \,,$$

   pour tout $h \in H$ et $0 \leq i \leq k-1$. Il est clair que χ' est bien définie (car l'écriture d'un élément de G un produit $h \cdot g^i$ est unique) et que $\chi'_{|H} = \chi$. Montrons maintenant que χ' est un caractère : d'abord $\chi'(e) = \chi(e) = 1$. Soient $h, h \in H$ et $\leq i, j \leq k-1$ et notons $f = h \cdot g^i$ et $f' := h' \cdot g^j$. Alors $(h \cdot g^i) \cdot (h' \cdot g^j) = (h \cdot h') \cdot g^{i+j}$. Distinguons deux cas :

   — si $i + j < k$, alors par définition

$$\chi'(f \cdot f') = \chi'((h \cdot h') \cdot g^{i+j}) = \chi(h \cdot h')\omega^{i+j} = \chi(h)\omega^i \chi(h')\omega^j = \chi'(h \cdot g^i)\chi'(h' \cdot h^j) = \chi'(f)\chi'(f') \,.$$

   — sinon, on a $k \leq i + j < 2k$, donc $0 \leq i + j - k < k$ et donc par définition (on rappelle que $g^k \in H$)

$$\chi'(f \cdot f') = \chi'((h \cdot h') \cdot g^{i+j}) = \chi'((h \cdot h' \cdot g^k) \cdot g^{i+j-k}) = \chi(h \cdot h' \cdot g^k)\omega^{i+j-k} = \chi(h)\chi(h')\chi(g^k)\omega^{i+j-k} \,.$$

   Or par construction $\chi(g^k) = \omega^k$, donc finalement

$$\chi'(f \cdot f') = \chi(h)\chi(h')\omega^k \omega^{i+j-k} = \chi(h)\omega^i \chi(h')\omega^j = \chi'(hg^i)\chi'(h'g^j) = \chi'(f)\chi'(f') \,.$$

   Finalement, on a bien vérifié que χ' était un caractère de G prolongenant χ.

   On a montré que dans le cas où $G = \langle H, g\rangle$, l'ensemble des caractères de G prolongeant χ était en bijection avec l'ensemble des racines k-ièmes de $\chi(g^k)$, donc de cardinal $k = [G : H]$, ce qui conclut la preuve.

Il reste à montrer la dernière assertion de l'énoncé : nous avons montré que le morphisme $\widehat{G} \to \widehat{H}$ était surjectif, et que ses fibres (donc en particulier son noyau) étaient de cardinal $[G : H]$. Or le morphisme surjectif $\pi : G \to G/H$ induit un morphisme injectif $\widehat{\pi} : \widehat{G/H} \to \widehat{G}$ (cf proposition 3.11), et la composée de ce morphisme avec le morphisme naturel $\widehat{G} \to \widehat{H}$ est triviale (exercice), donc l'image de $\widehat{\pi}$ est contenue dans le noyau de $\widehat{G} \to \widehat{H}$. Enfin, le résultat déjà démontré, appliqué au sous-groupe $\{e\} \subset G/H$ assure que $[G : H] = |\widehat{G/H}|$, ce qui assure le résultat. □

Corollaire 3.13. *Soit G un groupe abélien fini.*
Alors $|\widehat{G}| = |G|$.

Démonstration. Il suffit d'appliquer le théorème 3.12 à $H = \{e\} < G$. □

Remarque 3.14. Le groupe $\widehat{G}$ est défini même si G n'est pas commutatif. En revanche, pour un groupe fini G, la condition $|\widehat{G}| = |G|$ équivaut au fait que G est abélien. Plus précisément, on a un isomorphisme canonique $\widehat{G^{\mathrm{ab}}} \xrightarrow{\sim} \widehat{G}$, et par le corollaire précédent, on en déduit que $|\widehat{G}| = |G^{\mathrm{ab}}|$.

Corollaire 3.15. *Soient G, H deux groupes abéliens finis. Alors on a un isomorphisme canonique*

$$\widehat{G \times H} \cong \widehat{G} \times \widehat{H}\,.$$

Démonstration. □

Avant de démontrer le théorème principal ci-dessous, commençons par un lemme très utile pour les groupes abéliens.

Définition 3.16. Soit G un groupe de torsion. L'exposant du groupe G est le plus petit entier $n \geq 1$, s'il existe, tel que $g^n = e$ pour tout $g \in G$. Par définition, l'exposant de G est le ppcm des ordres des éléments de G.

Lemme 3.17. *Soit G un groupe abélien d'exposant fini.*
Alors il existe dans G un élément d'ordre égal à l'exposant de G.

Démonstration. On note $n = e(G) = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition en facteur premiers de l'exposant de G, avec p_i des nombres premiers deux-à-deux distincts et $\alpha_i \geq 1$.

L'exposant $e(G)$ étant le ppcm des ordres des éléments de G, pour tout $1 \leq i \leq r$, il existe $g_i \in G$ tel que l'ordre de g_i soit multiple de $p_i^{\alpha_i}$, i.e. de la forme $p_i^{\alpha_i} n_i$. Alors $h_i := g_i^{n_i}$ est d'ordre $p_i^{\alpha_i}$.

Notons alors $h = h_1 \cdot \dots \cdot h_r \in G$, et montrons que g est d'ordre $e(G)$. Cet ordre est naturellement un diviseur de $e(G)$, et pour tout $1 \leq i \leq r$, on a

$$h^{\frac{e(G)}{p_i}} = h_i^{\frac{e(G)}{p_i}} \neq e\,,$$

puisque $p_i^{\alpha_i}$ ne divise pas $\frac{e(G)}{p_i}$. Donc l'ordre de h est un diviseur de $e(G)$ qui ne divise aucun des $\frac{e(G)}{p_i}$, c'est donc $e(G)$ lui-même. □

Remarque 3.18. On retrouvera une preuve analogue en algèbre linéaire, quand nous étudierons le polynôme minimal d'un endomorphisme (analogue de l'exposant d'un groupe) et le polynôme minimal ponctuel en un vecteur (analogue de l'ordre d'un élément).

Théorème 3.19. *Soit G un groupe abélien fini. Alors il existe des entiers $d_1, \dots, d_r \geq 2$ tels que pour tout i, $d_i | d_{i+1}$, et*

$$G \cong \mathbf{Z}/d_1\mathbf{Z} \times \dots \times \mathbf{Z}/d_r\mathbf{Z}\,.$$

En outre, les d_i sont uniques.

Démonstration. — Existence : on raisonne par récurrence (forte) sur le cardinal de G (l'initialisation étant évidente pour le groupe trivial). On suppose $|G| \geq 2$. Le lemme 3.17 assure qu'il existe un élément $g \in G$ d'ordre égal à l'exposant n de G. On considère $\langle g \rangle < G$. Fixons ζ une racine primitive n-ième de l'unité dans $\mathbf{C}$. L'élément g étant d'ordre n, considérons la caractère $\chi : \langle g \rangle \to \mathbf{C}^\times$ défini par $\chi(g^k) := \zeta^k$ (induisant un isomorphisme de groupes cycliques $\langle g \rangle \cong \mu_n$). Le théorème 3.12 assure qu'il existe un prolongement $\chi' : G \to \mathbf{C}^\times$ de χ. Puisque G est d'exposant n, χ' est à valeur dans μ_n, i.e. $\chi' : G \to \mu_n$ est surjectif. Notons $H := \ker(\chi')$, et considérons le morphisme $\varphi : H \times \langle g \rangle \to G$ défini par $\varphi(h, g^k) := h \cdot g^k$. C'est clairement un morphisme de groupes, montrons que c'est un isomorphisme. Puisque les deux groupes ont même cardinal, il suffit de montrer qu'il est injectif. Soit $(h, g^k) \in \ker(\varphi)$. Alors $h \cdot g^k = e$, donc en appliquant χ', on obtient $\chi'(h)\chi(g)^k = 1$, i.e. $\zeta^k = 1$, donc k est multiple de n, donc $g^k = e$, donc $h = e$, donc $\ker(\varphi) = \{(e, e)\}$, donc φ est injective, donc un isomorphisme $\varphi : H \times \langle g \rangle \xrightarrow{\sim} G$. Puisque G est cyclique d'ordre n, on a un isomorphisme (donné par g) $\langle g \rangle \cong \mathbf{Z}/n\mathbf{Z}$. Finalement, on a construit un isomorphisme

$$G \cong H \times \mathbf{Z}/n\mathbf{Z}\,,$$

avec n égal à l'exposant de G.
Par hypothèse de récurrence, il existe $d_1, \ldots, d_{r-1} \geq 2$ tels que $d_1 | \ldots | d_{r-1}$ et un isommorphisme $H \cong \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_{r-1}\mathbf{Z}$. Donc on a un isomorphisme $G \cong \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_{r-1}\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$. Enfin, il existe un élément d'ordre d_{r-1} dans G, puisque $(0, \ldots, 0, 1, 0)$ est d'ordre d_{r-1} dans $Z/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_{r-1}\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$, donc d_{r-1} divise $d_r := n$ qui est l'exposant de G. D'où le résultat.

— Unicité : soient deux familles $(d_1, \ldots, d_r)$ et $(b_1, \ldots, b_s)$ d'entiers vérifiant les hypothèses de l'énoncés. Ce sont des entiers ≥ 2 se divisant successivement les uns les autres, tels que

$$G \cong \mathbf{Z}/b_1\mathbf{Z} \times \cdots \times \mathbf{Z}/b_s\mathbf{Z} \cong \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z}\,.$$

Pour tout $n \in \mathbf{N}$, on calcule de deux façons différentes le cardinal de G/nG : on voit que $nG = \prod_{i=1}^{r} (d_i, n)\mathbf{Z}/d_i\mathbf{Z}$, d'où

$$|G/nG| = \prod_{i=1}^{r} (n, d_i) = \prod_{j=1}^{s} (n, b_j)\,.$$

Montrons par récurrence sur r, que cette égalité pour tout $n \in \mathbf{N}$ implique $r = s$ et pour tout i, $d_i = b_i$.
Pour $n = d_1$, on obtient $d_1^r = \prod_{j=1}^{s} (d_1, b_j)$, ce qui implique $r \leq s$, donc par symétrie, $r = s$, puis $d_1 | b_1$, donc $d_1 = b_1$ par symétrie. On peut donc réécrire la condition numérique précédente dans le facteur d_1, et par récurrence, $d_i = b_i$ pour tout i. D'où l'unicité.

□

Remarque 3.20. Une démonstration alternative de l'unicité repose sur la propriété merveilleuse suivante (simplification des groupes finis) : si G, H, K sont trois groupes finis, munis d'un isomorphisme $G \times H \cong G \times K$, alors il existe un isomorphisme $H \cong K$ (on peut simplifier par G). Cette propriété est fausse pour des groupes infinis.

Corollaire 3.21. *Si G est un groupe abélien fini, alors G est isomorphe à $\widehat{G}$, non canoniquement en général.*

Démonstration. On utilise le théorème de classification précédent et le fait que $\widehat{G \times H} \cong \widehat{G} \times \widehat{H}$ pour se ramener au cas d'un groupe cyclique, pour lequel c'est évident. □

Donnons quelques applications du théorème de classification.

Proposition 3.22. *Soit p un nombre premier. Pour tout $n \geq 1$, le nombre de groupes abéliens de cardinal p^n est exactement le nombre de partitions de l'entier n, i.e. le nombre de façons d'écrire n comme une somme croissante d'entiers strictement positifs.*

Démonstration. □

Poursuivons avec quelques propriétés supplémentaires de la dualité. Les formules d'orthogonalité des caractères sont les suivantes :

Proposition 3.23. *Soit G un groupe fini.*

1. *Pour tout $\chi \in \widehat{G}$,*
$$\sum_{g \in G} \chi(g) = \begin{cases} 0 \text{ si } \chi \neq 1 \\ |G| \text{ si } \chi = 1 \end{cases}.$$
2. *Si G est abélien, pour tout $g \in G$,*
$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} 0 \text{ si } g \neq e \\ |\widehat{G}| = |G| \text{ si } g = e \end{cases}.$$

Démonstration.

1. Si $\chi = 1$, c'est évident car $\chi(g) = 1$ pour tout $g \in G$. Supposons $\chi \neq 1$. Alors il existe $g_0 \in G$ tel que $\chi(g_0) \neq 1$. On calcule alors
$$\chi(g_0) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g_0)\chi(g) = \sum_{g \in G} \chi(g_0 \cdot g)\,.$$
Or l'application $G \to G$ définie par $g \mapsto g_0 \cdot g$ est bijective, donc on peut réindicer la somme précédente pour obtenir :
$$\chi(g_0) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g)\,,$$
donc $(1-\chi(g_0)) \sum_{g \in G} \chi(g) = 0$. Or $\chi(g_0) \neq 1$, donc cela implique (**C** est intègre) que $\sum_{g \in G} \chi(g) = 0$.
2. Si $g = e$, c'est évident. Supposons donc $g \neq e$. Le théorème 3.12 assure qu'il existe $\chi_0 \in \widehat{G}$ tel que $\chi_0(g) \neq 1$. On écrit alors
$$\chi_0(g) \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} (\chi_0\chi)(g) = \sum_{\chi \in \widehat{G}} \chi(g)\,.$$
Or $\chi_0(g) \neq 1$, donc cela assure que $\sum_{\chi \in \widehat{G}} \chi(g) = 0$.

□

Un outil utile est le morphisme de bidualité :

Définition 3.24. Soit G un groupe. On dispose du morphisme canonique de bidualité $G \to \widehat{\widehat{G}}$, défini par $g \mapsto (\chi \mapsto \chi(g))$.

Proposition 3.25. *Si G est un groupe abélien fini, alors le morphisme de bidualité $G \to \widehat{\widehat{G}}$ est un isomorphisme de groupes.*

Démonstration. Montrons que ce morphisme est injectif : si g est dans le noyau de ce morphisme, alors $\chi(g) = 1$ pour tout $\chi \in \widehat{G}$, donc la proposition 3.23 assure que $g = e$, d'où l'injectivité.

On en déduit que c'est un isomorphisme puisque G et $\widehat{G}$ (et donc $\widehat{\widehat{G}}$) ont même cardinal (cf corollaire 3.13). □

Intéressons désormais à une incarnation algébrique de la transformée de Fourier, à savoir la transformée de Fourier sur les groupes abéliens finis.

Définition 3.26. Soit G un groupe abélien fini. On définit l'algèbre de groupes de G, notée $\mathbf{C}[G]$ ou $\mathbf{C}^G$, comme étant l'algèbre $(\mathbf{C}^G, +, *, \cdot)$ des applications $G \to \mathbf{C}$, munie des opérations $+$ et $\cdot$ naturelles, et du produit $*$ de convolution des fonctions, défini pour $\varphi, \psi \in \mathbf{C}^G$ par

$$(\varphi * \psi) : g \mapsto \frac{1}{|G|} \sum_{h \cdot k = g} \varphi(h)\psi(k)\,.$$

Remarquons que $\mathbf{C}[G]$ est une $\mathbf{C}$-algèbre de dimension finie $|G|$, dont une base canonique est donnée par les fonctions indicatrices $(\delta_g)_{g \in G}$ définies par $\delta_g(x) = 0$ si $x \neq g$ et $\delta_g(g) = 1$.

Notons que $\mathbf{C}[G]$ est muni d'un produit hermitien canonique, défini par

$$\langle f, f' \rangle := \frac{1}{|G|} \sum_{g \in G} \overline{f(g)} f'(g)\,,$$

pour tous $f, f' \in \mathbf{C}[G]$. Alors la base $(\delta_g)_{g \in G}$ est une base orthonogonale de $\mathbf{C}[G]$.

Proposition 3.27. *Si on munit $\mathbf{C}[G]$ du produit hermitien défini par*

$$\langle f, f' \rangle := \frac{1}{|G|} \sum_{g \in G} \overline{f(g)} f'(g)\,,$$

alors $\widehat{G}$ est une base orthonormée de $\mathbf{C}[G]$.

Démonstration. C'est exactement le contenu de la proposition 3.23, avec le calcul de la dimension de $\mathbf{C}[G]$. □

Définissons maintenant la transformée de Fourier sur le groupe G :

Définition 3.28. Pour tout $f \in \mathbf{C}[G]$, on définit $\widehat{f} \in \mathbf{C}[\widehat{G}]$ par

$$\widehat{f}(\chi) := \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} f(g) = \langle \chi, f \rangle\,,$$

pour tout $\chi \in \widehat{G}$.

Comme en analyse, on dispose des résultats fondamentaux de la théorie de Fourier, à savoir la formule d'inversion, la formule de Plancherel, le lien avec le produit de convolution, la formule de Parseval et la formule de Poisson.

Commençons par l'inversion de Fourier : on identifie canoniquement $\widehat{\widehat{G}}$ à G, et on définit pour tout $\varphi \in \mathbf{C}[\widehat{G}]$, une application $\widehat{\varphi} \in \mathbf{C}[G]$ par

$$\widehat{\varphi}(g) := \sum_{\chi \in \widehat{G}} \chi(g)\varphi(\chi)\,,$$

pour tous $g \in G$.

On dispose ainsi de deux applications linéaires

$$\mathbf{C}[G] \underset{\mathcal{F}^{-1}}{\overset{\mathcal{F}}{\rightleftarrows}} \mathbf{C}[\widehat{G}]\,.$$

Proposition 3.29 (Inversion de Fourier)**.** *Pour tout $f \in \mathbf{C}[G]$, on a $\widehat{\widehat{f}} = f$, i.e. $\mathcal{F}^{-1} \circ \mathcal{F} = \mathrm{id}$. De même, $\mathcal{F} \circ \mathcal{F}^{-1} = \mathrm{id}$.*

Démonstration. Puisque ce sont des applications linéaires entre $\mathbf{C}$-espaces vectoriels de dimension finie, il suffit de montrer l'une des égalités. Montrons la première. Soit $g \in \mathbf{C}[G]$.

Alors, pour tout $g \in G$,

$$\widehat{\widehat{f}}(g) = \sum_{\chi \in \widehat{G}} \chi(g)\widehat{f}(\chi) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(g) \sum_{h \in G} \overline{\chi(h)} f(h) = \frac{1}{|G|} \sum_{h \in G} f(h) \sum_{\chi \in \widehat{G}} \chi(gh^{-1})\,.$$

Or la proposition 3.23 assure que pour tout $h \in G$,

$$\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(gh^{-1}) = \delta_{g,h}\,,$$

donc

$$\widehat{\widehat{f}}(g) = f(g)\,,$$

ce qui conclut la preuve. □

Munissons $\mathbf{C}[\widehat{G}]$ du produit hermitien

$$\langle \varphi, \varphi' \rangle := \sum_{\chi \in \widehat{G}} \overline{\varphi(\chi)} \varphi'(\chi)\,,$$

et poursuivons avec la formule de Parseval-Plancherel :

Proposition 3.30 (Parseval-Plancherel)**.** *Pour tout $f, f' \in \mathbf{C}[G]$, on a*

$$\langle f, f' \rangle = \langle \widehat{f}, \widehat{f'} \rangle\,,$$

et en particulier

$$\frac{1}{|G|} \sum_{g \in G} |f(g)|^2 = \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|^2\,.$$

Autrement dit, $\mathcal{F}$ est une isométrie de $\mathbf{C}[G]$ vers $\mathbf{C}[\widehat{G}]$.

Démonstration. Soient $f, f' \in \mathbf{C}[G]$.

Calculons $\langle \widehat{f}, \widehat{f'} \rangle$:

$$\langle \widehat{f}, \widehat{f'} \rangle = \sum_{\chi \in \widehat{G}} \overline{\widehat{f}(\chi)} \widehat{f'}(\chi) = \frac{1}{|G|^2} \sum_{\chi \in \widehat{G}} \sum_{g,h \in G} \chi(g) \overline{f(g)\chi(h)} f'(h) = \frac{1}{|G|} \sum_{g,h \in G} \overline{f(g)} f'(h) \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(gh^{-1}) \,.$$

Or la proposition 3.23 assure que pour tout $g, h \in G$, on a

$$\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(gh^{-1}) = \delta_{g,h} \,,$$

donc

$$\langle \widehat{f}, \widehat{f'} \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{f(g)} f'(g) = \langle f, f' \rangle \,.$$

□

Étudions maintenant le lien entre transformée de Fourier et produit de convolution :

Proposition 3.31 (convolution)**.** *L'application* $\mathcal{F} : (\mathbf{C}[G], +, *, .) \to (\mathbf{C}[\widehat{G}], +, \cdot, .)$ *est un isomorphisme de* $\mathbf{C}$*-algèbres. En particulier, pour tous* $f, f' \in \mathbf{C}[G]$*,*

$$\widehat{f * f'} = \widehat{f}\widehat{f'} \,.$$

Démonstration. Calculons $\widehat{f * f'}$: pour tout $\chi \in \widehat{G}$, on a

$$\widehat{f * f'}(\chi) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} (f * f')(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \frac{1}{|G|} \sum_{\substack{h,\, k \,\in\, G \,:\\ h \,\cdot\, k \,=\, g}} f(h) f'(k) \,,$$

donc

$$\widehat{f * f'}(\chi) = \frac{1}{|G|^2} \sum_{h,k \in G} \overline{\chi(h \cdot k)} f(h) f'(k) = \frac{1}{|G|^2} \sum_{h,k \in G} \overline{\chi(h)} f(h) \overline{\chi(k)} f'(k) = \widehat{f}(g) \widehat{f'}(g) \,.$$

□

Quelques applications possibles de la dualité et de la transformée de Fourier :

1. principe d'incertitude : $f \in \mathbf{C}[G]$ non nulle, alors $|\mathrm{supp}(f)||\mathrm{supp}(\widehat{f})| \geq |G|$.
2. sommes de Gauss et application à la loi de réciprocité quadratique (voir le chapitre d'arithméique).
3. transformée de Fourier discrète (TFD).
4. algorithme de transformée de Fourier rapide (TFR ou FFT) dans le cas $G = \mathbf{Z}/n\mathbf{Z}$.
5. multiplication rapide de grands entiers ou polynômes via la FFT (algorithmes de Cooley-Tuckey et Schönhage-Strassen).
6. fonctions L de Dirichlet associées à des caractères et application au théorème de la progression arithmétique de Dirichlet.

3.3 Quelques groupes abéliens infinis

Proposition 3.32. *Soit G un sous-groupe de $(\mathbf{R}, +)$.*
Alors soit G est dense, soit il existe $x \in G$ tel que $G = \mathbf{Z}x$.

Démonstration. Notons $G_+ := G \cap \mathbf{R}^{+,\times}$.

Si $G_+ = \emptyset$, alors $G = \{0\} = \mathbf{Z}0$. Supposons maintenant $G_+ \neq \emptyset$. Alors G_+ est une partie non vide de $\mathbf{R}$ minorée par 0. Elle admet une borne inférieure, notée $x \in \mathbf{R}^+$. On a alors l'alternative suivante :

— soit $x > 0$. Montrons qu'alors $x \in G$ et $G = \mathbf{Z}x$. Supposons $x \notin G$. Alors il existe $g_1 \in G$ tel que $x < g_1 < 2x$. De même, il existe $g_2 \in G$ tel que $x < g_2 < g_1$. Puisque G est un sous-groupe de $\mathbf{R}$, il est stable par somme et par opposé, donc $g_1 - g_2 \in G$. Or par construction $0 < g_1 - g_2 < x$, donc $g_1 - g_2 \in G_+$ et l'inégalité $g_1 - g_2 < x$ est contradictoire. Donc $x \in G$.
Soit alors $g \in G \setminus \{0\}$. Quitte à remplacer g par $-g$, on peut supposer $g \in G_+$. Puisque $\mathbf{R}$ est archimédien, il existe $n \in \mathbf{N}$ tel que $nx \leq g < (n+1)x$. Alors par stabilité de G, $g - nx \in G$ et $0 \leq g - nx < x$, donc par définition de x, $g - nx = 0$, donc $g = nx$, donc $g \in \mathbf{Z}x$. D'où l'égalité $G = \mathbf{Z}x$.

— soit $x = 0$. Montrons qu'alors G est dense dans $\mathbf{R}$. Soit U un ouvert non vide de $\mathbf{R}$. Il existe $x \in U \setminus \{0\}$ et $\varepsilon > 0$ tels que $]x - \varepsilon, x + \varepsilon[\subset U$. Puisque $\inf G_+ = 0$, il existe $g \in G_+$ tel que $0 < g < \varepsilon$. Comme $\mathbf{R}$ est archimédien, il existe $n \in \mathbf{Z}$ tel que $ng \in]x - \varepsilon, x + \varepsilon[$ (prendre n égal à la partie entière de $\frac{x}{n}$), donc $ng \in U$, donc $G \cap U \neq \emptyset$, donc G est dense dans $\mathbf{R}$.

□

Une variante de cet énoncé :

Proposition 3.33. *Notons $\mathbf{U}$ le groupe des nombres complexes de module 1, et soit G un sous-groupe de $\mathbf{U}$.*
Alors soit G est dense, soit il est cyclique et égal à un certain $\mu_n(\mathbf{C})$.
En outre, pour tout $\theta \in \mathbf{R}$, le sous-groupe de $\mathbf{U}$ engendré par $e^{i\theta}$ est dense si $\frac{\theta}{2\pi} \notin \mathbf{Q}$ et il est cyclique si $\frac{\theta}{2\pi} \in \mathbf{Q}$.

Démonstration. On dispose du morphisme naturel $\varphi : \mathbf{R} \to \mathbf{U}$ défini par $\varphi(x) := e^{ix}$. Ce morphisme de groupes est surjectif, de noyau $2\pi\mathbf{Z}$. Alors $\varphi^{-1}(G)$ est un sous-groupe de $\mathbf{R}$ tel que $G = \varphi(\varphi^{-1}(G))$. Par la proposition précédente, on a l'alternative suivante :

— soit $\varphi^{-1}(G)$ est dense dans $\mathbf{R}$, auquel cas G est dense dans $\mathbf{R}$.

— soit $\varphi^{-1}(G)$ est de la forme $\mathbf{Z}\theta$ pour un $\theta \in \mathbf{R}$. Alors G est monogène, engendré par $e^{i\theta}$. Or $\varphi^{-1}(G)$ contient $\ker \varphi = 2\pi\mathbf{Z}$, donc $2\pi \in \mathbf{Z}\theta$, donc en particulier $\frac{\theta}{2\pi} \in \mathbf{Q}$, ce qui assure que que G est cyclique (de cardinal égal au dénominateur d'un fraction irréductible représentant θ).

□

4 Actions de groupes

Définition 4.1. Soit G un groupe et X un ensemble. Une action ou opération (à gauche) de G sur X est la donnée d'une application $\begin{array}{c} G \times X \to X \\ (g, x) \mapsto g \cdot x \end{array}$ vérifiant les conditions suivantes :

1. Pour tout $g, g' \in G$ et tout $x \in X$, on a $(g \cdot g') \cdot x = g \cdot (g' \cdot x)$.
2. Pour tout $x \in X$, $e \cdot x = x$.

Remarque 4.2. De façon équivalente, une action de groupe (à gauche) est la donnée d'un morphisme de groupes $\varphi : G \to \mathfrak{S}(X)$. En effet, à partir de la définition précédente, on définit l'application φ via $\varphi(g) : x \mapsto g \cdot x$ et les deux axiomes assurent que c'est un morphisme. Réciproquement, si $\varphi : G \to \mathfrak{S}(X)$ est un morphisme, alors l'application $(g, x) \mapsto g \cdot x := \varphi(g)(x)$ vérifie bien les deux axiomes de la définition.

Exemples 4.3.
- Si $X = G$, on dispose de plusieurs action naturelles de G sur lui-même : l'action par translation à gauche (resp. à droite) définie par $g \cdot g' := gg'$ (resp.$g \cdot g' := g'g^{-1}$) ; l'action par conjugaison définie par $g \cdot g' := gg'g^{-1}$.
- Si X est un ensemble, le groupe $G := \mathfrak{S}(X)$ agit naturellement sur X via $\sigma \cdot x := \sigma(x)$.
- Si V est un espace vectoriel sur un corps K, alors le groupe $\mathrm{GL}(V)$ des endomorphismes inversibles agit sur l'espace V, via $u \cdot x := u(x)$ (et aussi sur l'espace projectif associé $\mathbb{P}(V)$, formé des droites vectorielles dans V).
- Si E est un espace euclidien, le groupe des isométries de E agit naturellement sur l'espace E.
- Le groupe $\mathrm{GL}_n(K)$ agit par translation à gauche sur $\mathrm{Mat}_{n,p}(K)$.
- Le groupe $\mathrm{GL}_n(K) \times \mathrm{GL}_p(K)$ agit naturellement sur $\mathrm{Mat}_{n,p}(K)$ via la formule $(P, Q) \cdot M := PMQ^{-1}$.
- Si G est un groupe, $H < G$ un sous-groupe et $X = G/H$, alors G agit naturellement sur X par translation à gauche, via $g \cdot (g'H) := (gg')H$.

Proposition 4.4 (Théorème de Cayley)**.** *Soit G un groupe fini de cardinal n. Alors l'action de G sur lui-même par translation à gauche définit un morphisme de groupes injectif*

$$G \hookrightarrow \mathfrak{S}(G) \cong \mathfrak{S}_n \,.$$

Démonstration. Il suffit de vérifier que le morphisme induit par cette action est injectif. Soit $g \in G$ dans le noyau de ce morphisme. Alors pour tout $h \in G$, $g \cdot h = h$, donc $g = e$, d'où l'injectivité. □

Corollaire 4.5. *Soit G un groupe fini de cardinal n.*
Pour tout corps K, il existe n tel que G soit un sous-groupe de $\mathrm{GL}_n(K)$.

Démonstration. En utilisant la proposition précédente, il suffit de construire un morphisme de groupes injectif $p : \mathfrak{S}_n \to \mathrm{GL}_n(K)$ et de le composer avec le morphisme précédent. Pour cela, on définit pour tout $\sigma \in \mathfrak{S}_n$, $p(\sigma) = P_\sigma \in \mathrm{GL}_n(K)$ comme la matrice de permutation associée à σ. Plus précisément, $(P_\sigma)_{i,j} := \delta_{i,\sigma(j)}$, i.e. le coefficient d'indice (i, j) de P_σ vaut 1 si $i = \sigma(j)$ et 0 sinon. Alors un calcul simple assure que p est un morphisme de groupes ($P_{\sigma\circ\tau} = P_\sigma P_\tau$ et $P_{\mathrm{id}} = I_n$) et par construction p est injectif, ce qui conclut la preuve. □

Remarque 4.6. Plus canoniquement, on a des morphismes injectifs canoniques

$$G \hookrightarrow \mathfrak{S}(G) \hookrightarrow \mathrm{GL}(K^G) \,.$$

Définition 4.7. Soit G un groupe agissant sur un ensemble X. Pour tout $x \in X$, on définit l'orbite de x dans X comme l'ensemble

$$\mathcal{O}_x := \{g \cdot x, g \in G\} \subset X \,.$$

Notons que l'action de G sur X se restreint naturellement en une action de G sur $\mathcal{O}_x$.

Remarquons que la relation $\sim_G$ sur X définie $x \sim_G y$ si et seulement s'il existe $g \in G$ tel que $y = g \cdot x$ est une relation d'équivalence. On peut la reformuler en remarquant que $x \sim_G y$ si et seulement si $\mathcal{O}_x = \mathcal{O}_y$. Les orbites sont exactement les classes d'équivalence pour $\sim_G$, et par conséquent elles partitionnent X. On note $G\backslash X$ l'ensemble quotient, à savoir l'ensemble des classes d'équivalence, ou encore l'ensemble des orbites pour cette action. Au passage, si $H < G$ est un sous-groupe, alors H agit sur G par translation à gauche via $h \cdot g := hg$, et les orbites sont exactement les classes à droite Hg, pour $g \in G$, et l'ensemble quotient $H\backslash G$ coïncide avec celui défini à la remarque 2.18.

Définition 4.8. Soit G un groupe agissant sur un ensemble X. Pour tout $x \in X$, on définit le stabilisateur de x dans G comme l'ensemble $\mathrm{Stab}_G(x) := \{g \in G : g \cdot x = x\} \subset G$. C'est un sous-groupe de G.

Poursuivons avec le vocabulaire des actions de groupes :

Définition 4.9. Soit G un groupe agissant sur un ensemble X. Pour tout $g \in G$, on définit le fixateur de g dans X comme

$$\mathrm{Fix}_X(g) := \{x \in X : g \cdot x = x\}.$$

L'ensemble des points fixes de G dans X est

$$X^G := \{x \in X : \forall g \in G, g \cdot x = x\} = \bigcap_{g \in G} \mathrm{Fix}_X(g).$$

Exemples 4.10.
- On considère l'action naturelle de $\mathfrak{S}_n$ sur $\{1, \ldots, n\}$. Alors le stabilisateur de n est naturellement isomorphe à $\mathfrak{S}_{n-1}$. L'orbite d'un point est égale à $\{1, \ldots, n\}$ et l'ensemble des points fixes est vide, sauf si $n = 1$.
- Si G agit sur lui-même par conjugaison, le stabilisateur d'un élément g de G est l'ensemble des éléments de G commutant avec g, et l'ensemble des points fixes est le centre de G.
- Si G est le groupe orthogonal $\mathcal{O}_2(\mathbf{R})$ des isométries vectorielles (rotations de centre 0 et symétries orthogonales par rapport à des droites vectorielles) du plan euclidien $\mathbf{R}^2$, alors l'orbite d'un vecteur de norme r est le cercle de centre 0 et de rayon r ; le stabilisateur d'un vecteur non nul v est le sous-groupe à deux éléments formé de l'identité et de la symétrie d'axe $\mathbf{R}v$, alors que le stabilisateur du vecteur nul est $\mathcal{O}_2(\mathbf{R})$ tout entier ; le fixateur de l'identité est $\mathbf{R}^2$, celui d'un rotation non triviale est $\{0\}$ et celui d'un symétrie est exactement l'axe de cette symétrie ; l'ensemble des points fixes est réduit à $\{0\}$.

Définition 4.11. Soit G un groupe agissant sur un ensemble X. On dit que l'action est
- fidèle si le morphisme $\varphi : G \to \mathfrak{S}(X)$ est injectif. De façon équivalente, cela signifie que $\bigcap_{x \in X} \mathrm{Stab}_G(x) = \{e\}$.
- libre si pour tout $x \in X$, $\mathrm{Stab}_G(x) = \{e\}$. En particulier, une action libre est fidèle.
- transitive si pour tous $x, y \in X$, il existe $g \in G$ tel que $g \cdot x = y$, ce qui équivaut à dire que l'action a une seule orbite.

— simplement transitive si elle est libre et transitive, i.e. si pour tous $x, y \in X$, il existe un unique $g \in G$ tel que $g \cdot x = y$.

On peut préciser légèrement la notion de transitivité :

Définition 4.12. Soit G un groupe agissant sur un ensemble X et $n \geq 1$.

On dit que l'action est n-transitive si pour tout $(x_1, \dots x_n, y_1, \dots, y_n) \in X^{2n}$ tels que $x_i \neq x_j$ et $y_i \neq y_j$ pour tout $i \neq j$, il existe $g \in G$ tel que $g \cdot x_i = y_i$ pour tout i.

Exemples 4.13.
— l'action par translation de G sur lui-même est libre, donc fidèle, et elle est transitive.
— l'action par conjugaison de G sur lui-même est fidèle ssi le centre de G est trivial. Cette action est libre (resp. transitive) ssi $G = \{1\}$. Les orbites sont les classes de conjugaison.
— l'action de $\mathfrak{S}(X)$ sur X est fidèle et transitive.
— l'action de $\mathrm{GL}(V)$ sur V est fidèle. Elle est transitive si et seulement si $V = \{0\}$. Sinon, cette action a exactement deux orbites : $\{0\}$ et $V \setminus \{0\}$.
— l'action de $\mathrm{PGL}_2(K)$ sur l'ensemble $\mathbf{P}^1(K)$ des droites vectorielles de K^2 (la droite projective) est 3-transitive, mais pas 4-transitive. On peut en déduire une définition du birapport.

Lemme 4.14. *Soit G un groupe agissant sur un ensemble X. Pour tout $x \in X$ et $g \in G$, on a* $\mathrm{Stab}_G(g \cdot x) = g\mathrm{Stab}_G(x)g^{-1}$.

Cela signifie en particulier que deux points dans la même orbite ont des stabilisateurs conjugués, donc isomorphes.

Démonstration. Pour tout $h \in G$, on a $h \in \mathrm{Stab}_G(x)$ si et seulement si $h \cdot x = x$ si et seulement si $(hg^{-1}g) \cdot x = x$ si et seulement si $(ghg^{-1})(g \cdot x) = g \cdot x$ si et seulement si $ghg^{-1} \in \mathrm{Stab}_G(g \cdot x)$. D'où l'égalité souhaitée. □

La proposition suivante est cruciale, elle permet de relier l'orbite d'un point à son stabilisateur :

Proposition 4.15. *Soit G un groupe agissant sur un ensemble X. Pour tout $x \in X$, on dispose d'une bijection canonique*

$$G/\mathrm{Stab}_G(x) \xrightarrow{\sim} \mathcal{O}_x\,,$$

induite par $g \mapsto g \cdot x$.

En outre, cette bijection est compatible aux actions naturelles (à gauche) de G sur $G/\mathrm{Stab}_G(x)$ et sur $\mathcal{O}_x$.

On dit que c'est une bijection G-equivariante.

Démonstration. On considère l'application naturelle $\varphi_x : G \to \mathcal{O}_x$ définie par $\varphi_x(g) := g \cdot x$. Par définition, cette application est surjective. En outre, pour tout $g \in G$ et $h \in \mathrm{Stab}_G(x)$, on a $\varphi_x(gh) = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = \varphi_x(g)$, autrement dit l'application φ_x est constante sur chaque classe à gauche de $H := \mathrm{Stab}_G(x)$ dans G. Par conséquent, φ_x se factorise en une application surjective $\pi_x : G/\mathrm{Stab}_G(x) \to \mathcal{O}_x$. Montrons que cette application est injective : soient $g, g' \in G$ tels que $\pi_x(gH) = \pi_x(g'H)$, i.e. $g \cdot x = g' \cdot x$. Alors $(g^{-1}g') \cdot x = x$, donc $g^{-1}g' \in H$, donc $gH = g'H$, d'où l'injectivité de π_x.

Pour finir, montrons que π_x (ou φ_x) est G-équivariante pour l'action de G par multiplication à gauche sur G/H (ou sur G lui-même) : soient $g, g' \in G$, alors

$$\pi_x(g \cdot (g'H)) = \pi_x((gg')H) = (gg') \cdot x = g \cdot (g' \cdot x) = g \cdot \pi_x(gH)\,,$$

ce qui est exactement la propriété souhaitée. □

Corollaire 4.16 (Équation aux classes)**.** *Soit G un groupe fini agissant sur un ensemble fini X.*

Alors on a

$$|X| = \sum_{x \in G\backslash X} |\mathcal{O}_x| = \sum_{x \in G\backslash X} \frac{|G|}{|\mathrm{Stab}_G(x)|}\,.$$

Démonstration. La relation "être dans la même orbite" est une relation d'équivalence, et les orbites sont les classes d'équivalence. Donc X est la réunion disjointe des orbites. Par conséquent,

$$|X| = \sum_{x \in G\backslash X} |\mathcal{O}_x|\,.$$

Il suffit enfin d'appliquer la proposition 4.15 pour avoir la seconde égalité. □

Une autre formule très utile pour l'étude des actions de groupes est la suivante :

Proposition 4.17 (Formule de Burnside)**.** *Soit X un ensemble fini muni d'une action d'un groupe fini G.*

$$|G\backslash X| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_X(g)|\,.$$

Démonstration. On considère l'ensemble

$$E := \{(g, x) \in G \times X : g \cdot x = x\}\,.$$

On va calculer le cardinal de E de deux façons différentes. On peut considérer E comme une réunion disjointe, de deux façons différentes :

$$E = \coprod_{g \in G} \{x \in X : g \cdot x = x\} = \coprod_{g \in G} \mathrm{Fix}_X(g)$$

et

$$E = \coprod_{x \in X} \{g \in G : g \cdot x = x\} = \coprod_{x \in X} \mathrm{Stab}_G(x)\,.$$

On a donc les deux expressions suivantes pour le cardinal de E :

$$\sum_{g \in G} |\mathrm{Fix}_X(g)| = \sum_{x \in X} |\mathrm{Stab}_G(x)|\,.$$

Or, pour tout $x \in X$, pour tout $y \in \mathcal{O}_x$, □

Remarque 4.18. Cette formule dit que le nombre moyen de points fixes d'un élément de G est le nombre d'orbites. Par exemple, une permutation aléatoire de $\mathfrak{S}_n$ a en moyenne un point fixe.

Exemple 4.19. Si G agit sur lui-même par conjugaison, on obtient les relations suivantes :

— $|G| = |Z(G)| + \sum_{g \in C_G \setminus Z(G)} \frac{|G|}{|Z_G(g)|}$, où $C_G \subset G$ est un ensemble de représentants des classes de conjugaison, $Z_G(g)$ est le centralisateur de g et $Z(G)$ est le centre de G.

— $|C_G| = \frac{1}{|G|} \sum_{g \in G} |Z_G(g)|$.

L'équation aux classes a de nombreuses applications en théorie des groupes et en combinatoire. En voici quelques unes.

Lemme 4.20. *Soit G un groupe de cardinal p^n (un p-groupe), où p est un nombre premier, agissant sur un ensemble fini X. Alors $|X^G| \equiv |X| \pmod{p}$.*

Démonstration. On écrit l'équation aux classes :

$$|X| = |X^G| + \sum_{x \in G \setminus X, x \notin X^G} \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

Or, pour tout $x \notin X^G$, le stabilisateur $\mathrm{Stab}_G(x)$ est un sous-groupe strict de G, donc par Lagrange son cardinal est de la forme p^r, avec $0 \leq r < n$. Donc pour tout $x \notin X^G$, $\frac{|G|}{|\mathrm{Stab}_G(x)|} = p^{n-r}$ est multiple de p. Donc l'équation aux classes précédente assure que $|X| \equiv |X^G| \pmod{p}$. □

On rappelle que si p est un nombre premier, un p-groupe est un groupe fini de cardinal p^r, avec $r \in \mathbf{N}$.

Proposition 4.21. *Soit G un p-groupe non trivial.*
Alors le centre $Z(G)$ de G est non trivial.

Démonstration. On considère l'action de G sur $X = G$ par conjugaison. Par définition, $X^G = Z(G)$ et le lemme 4.20 assure que $|Z(G)| \equiv |G| \pmod{p}$. Donc en particulier p divise le cardinal de $Z(G)$. Enfin, $Z(G)$ contient l'élément neutre et $p \geq 2$, donc $Z(G) \neq \{e\}$. □

Remarque 4.22. Puisque le centre est lui-même un p-groupe, on peut lui appliquer la proposition, et par récurrence prouver que tout p-groupe est nilpotent (notion hors-programme).

Corollaire 4.23. *Soit p un nombre premier.*
Tout groupe d'ordre p^2 est abélien.

Démonstration. Soit G un groupe d'ordre p^2.

La proposition 4.21 assure que $Z(G)$ est non trivial, donc $|Z(G)| = p$ ou p^2. Dans le second cas, $Z(G) = G$, ce qui assure que G est commutatif. Supposons donc maintenant $|Z(G)| = p$. Alors le quotient $G/Z(G)$ est un groupe d'ordre p, il est donc cyclique. On conclut maintenant grâce au lemme suivant :

Lemme 4.24. *Soit G un groupe.*
Si $G/Z(G)$ est monogène, alors G est abélien.

Démonstration. On note $\pi : G \to G/Z(G)$ la surjection canonique. Par hypothèse, il existe $\bar{g} \in G/Z(G)$ tel que $G/Z(G) = \langle \bar{g} \rangle$. Puisque π est surjective, il existe $g \in G$ tel que $\pi(g) = \bar{g}$.

Soient $g_1, g_2 \in G$. Il existe $k_1, k_2 \in \mathbf{Z}$ tels que $\pi(g_i) = \bar{g}^{k_i} = \pi(g^{k_i})$. Donc il existe $z_1, z_2 \in Z(G)$ tels que $g_i = z_i g^{k_i}$.

Alors on a

$$g_1 g_2 = (z_1 g^{k_1})(z_2 g^{k_2}) = (z_1 z_2) g^{k_1+k_2} \,,$$

puisque $z_i \in Z(G)$. De même,

$$g_2 g_1 = (z_2 g^{k_2})(z_1 g^{k_1}) = (z_2 z_1) g^{k_2+k_1} = (z_1 z_2) g^{k_1+k_2} \,,$$

donc $g_1 g_2 = g_2 g_1$, ce qui conclut la preuve. □

□

Remarque 4.25. En revanche, pour tout nombre premier p, il existe un groupe d'ordre p^3 non commutatif. La lectrice est invitée à trouver de tels exemples.

Théorème 4.26 (Cauchy)**.** *Soit G un groupe fini et p un nombre premier divisant $|G|$.*
Alors G admet un élément d'ordre p.

Démonstration. On considère l'ensemble $X := \{(g_1, \dots, g_p) \in G^p : g_1 \dots g_p = e\}$ et l'action du groupe $G = \mathbf{Z}/p\mathbf{Z}$ par permutation circulaire sur X. Plus précisément, pour tout $\bar{k} \in \mathbf{Z}/p\mathbf{Z}$ (avec $k \in \mathbf{Z}$), et tout $(g_1, \dots, g_p) \in X$, on pose $\bar{k} \cdot (g_1, \dots, g_p) := (g_{k+1}, \dots, g_{k+p})$, où les indices sont calculés modulo p. On vérifie facilement que $\bar{k} \cdot (g_1, \dots, g_p) \in X$ et que la formule définit une action de G sur X.

Clairement, X^G est exactement l'ensemble $\{(g, \dots, g) \in G^p : g^p = e\}$, qui est en bijection avec l'ensemble des éléments d'ordre divisant p dans G. Il suffit donc de montrer que X^G n'est pas réduit à l'élément évident $(e, \dots, e)$.

Pour cela, calculons le cardinal de X : on dispose d'une application naturelle

$$\psi : G^{p-1} \to X$$

définie par $\psi(g_1, \dots, g_{p-1}) := (g_1, \dots, g_{p-1}, (g_1 \dots g_{p-1})^{-1})$ (vérifier qu'elle est bien définie). On voit facilement que ψ est bijective. Cela assure que $|X|$ est multiple de p (car $|G|$ l'est). Alors le lemme 4.20 assure que p divise $|X^G|$. Or $p \geq 2$, donc $|X^G| \geq 2$, donc il existe $g \in G \setminus \{e\}$ tel que $(g, \dots, g) \in X^G$, i.e. tel que $g^p = e$. □

Proposition 4.27. *Soit G un groupe fini et p le plus petit nombre premier divisant $|G|$. Alors tout sous-groupe de G d'indice p est distingué.*

Démonstration. Soit H un sous-groupe de G d'indice p. On considère l'action naturelle de G sur $X = G/H$, définie par $g \cdot (g'H) := (gg')H$. Cette action induit un morphisme de groupes

$$\varphi : G \to \mathfrak{S}(G/H) \,,$$

que l'on peut restreindre à H pour obtenir un morphisme

$$\varphi : H \to \mathfrak{S}(G/H) \,,$$

défini par, pour tout $h \in H$ et $g \in G$, $\varphi(h)(gH) = (hg)H$.

Observons que pour tout $h \in H$, $\varphi(h)(H) = hH = H$, donc $\varphi(h)$ envoie H sur lui-même. Par conséquent, pour tout $h \in H$, $\varphi(h)$ induit par restriction une bijection de $Y := (G/H) \setminus \{H\}$. D'où finalement un morphisme

$$\psi : H \to \mathfrak{S}(Y)$$

avec $|Y| = p - 1$ et $\psi(h)(gH) = (hg)H$.

Or $|H|$ est par définition produit de nombres premiers supérieurs ou égaux à p, alors que $|\mathfrak{S}(Y)| = (p-1)!$ est produit de nombres premiers strictement inférieurs à p. Or l'image de ψ a un cardinal qui divise à la fois le cardinal de H et celui de $\mathfrak{S}(Y)$. Donc $\mathrm{im}\,(\psi)$ est de cardinal 1, donc ψ est le morphisme trivial. Cela signifie que pour tout $h \in H$, pour tout $g \in G$, $h(gH) = gH$, i.e. $g^{-1}hg \in H$, donc H est distingué dans G. □

La preuve de l'énoncé ci-dessous sera présentée plus tard, une fois introduits les polynômes cyclotomiques :

Théorème 4.28 (Wedderburn)**.** *"Tout corps fini est commutatif". Plus précisément, tout anneau intègre fini (pas commutatif a priori) est un corps (commutatif).*

Démonstration. Soit K un tel anneau intègre fini.

Remarquons d'abord que tout élément x non nul de K est inversible, puisque l'application $K \setminus \{0\} \to K \setminus \{0\}$ définie par $y \mapsto xy$ est injective (car K est intègre), donc bijective par égalité des cardinaux, ce qui assure que x admet un inverse à droite. Par symétrie, x admet un inverse à gauche, et cela assure que x est inversible.

Notons $k := \{t \in K : tx = xt\,,\ \forall x \in K\}$ le centre de K. Alors k est un corps (commutatif, fini) dont on note $q \geq 2$ le cardinal.

L'application $k \times K \to K$ définie par $(t, x) \mapsto tx$ munit K d'une structure de k-espace vectoriel. Puisque K est fini, K est un k-espace vectoriel de dimension finie. Notons d sa dimension, alors $K \cong k^d$, donc $|K| = |k|^d$.

Considérons alors le groupe $G := K^\times = K \setminus \{0\}$ (non commutatif a priori) et faisons le agir sur lui-même par conjugaison, i.e. $x \cdot y := xyx^{-1}$.

Écrivons l'équation aux classes pour cette action :

$$|K^\times| = |(K^\times)^G| + \sum_{x \in G \setminus K^\times, x \notin K^G} \frac{K^\times}{\mathrm{Stab}_{K^\times}(x)}\,.$$

Or $K^G = k$ par définition, et pour tout $x \in K \setminus k$, l'ensemble des $y \in K$ tels que $xy = yx$ est un sous-k-espace vectoriel de K, non trivial, donc cet ensemble est de cardinal q^r, avec $1 \leq r < d$. En particulier, pour tout $x \in K \setminus k$, $|\mathrm{Stab}_{K^\times}(x)| = q^r - 1$ pour un tel $1 \leq r < d$. En outre, $q^r - 1$ divise $q^d - 1$, ce qui implique que r divise d. On obtient donc un ensemble fini d'entiers $1 \leq r_1, \ldots, r_a < d$ (où a est le nombre d'orbites non réduites à un singleton) tels que r_i divise d pour tout i et l'équation aux classes s'écrive

$$q^d - 1 = q - 1 + \sum_{i=1}^{a} \frac{q^d - 1}{q^{r_i} - 1}\,. \tag{1}$$

Introduisons maintenant les polynômes cyclotomiques $\phi_n(X) := \prod_{\zeta \in \mu_n^*}(X - \zeta)$, où $\mu_n^* \subset \mu_n(\mathbf{C})$ désigne l'ensemble des racines primitives n-ièmes de l'unité dans $\mathbf{C}$. Le théorème de Lagrange et la description des racines n-ièmes de l'unité dans $\mathbf{C}$ assurent

que $X^n - 1 = \prod_{d|n} \phi_d(X)$. Puisque les $\phi_d(X)$ sont unitaires, une récurrence simple assure que $\phi_n(X) \in \mathbf{Z}[X]$ pour tout n.

Revenons à l'égalité (1) : puisque dans $\mathbf{Z}[X]$, $\phi_d(X)$ divise $X^d - 1$, et aussi $\frac{X^d-1}{X^{r_i}-1}$, on en déduit que $\phi_d(q)$ divise $q - 1$ dans $\mathbf{Z}$. Or

$$|\phi_d(q)| = \prod_{\zeta \in \mu_d^*} |q - \zeta| \,,$$

et pour tout $\zeta \neq 1$, $|q - \zeta| > q - 1$ (faire un dessin).

Finalement, si $d > 1$, on voit que $\phi_d(q) > q - 1$, ce qui contredit le fait que $\phi_d(q)$ divise $q - 1$. On en déduit donc que $d = 1$, ce qui signifie que $K = k$, donc K est commutatif. □

Une application classique des actions de groupes en combinatoire :

Exemple 4.29. Les colliers de perles.

On cherche à dénombrer les colliers à 9 perles dont 4 bleues, 3 blanches et 2 rouges. En utilisant une action du groupe diédral D_9, on trouve qu'il y a exactement 76 tels colliers.

5 Hors programme : Théorèmes de Sylow

Théorème 5.1. *Soit G un groupe fini de cardinal $n = p^\alpha m$, avec $(m, p) = 1$.*

1. *Il existe un sous-groupe de G de cardinal p^α, appelé un p-sous-groupe de Sylow de G.*
2. *Tout p-sous-groupe de G est contenu dans un p-Sylow de G.*
3. *Si S et T sont deux p-Sylow de G, alors il existe $g \in G$ tel que $T = gSg^{-1}$.*
4. *Si n_p désigne le nombre de p-Sylow de G, alors n_p divise m et $n_p \equiv 1 \pmod p$.*

Exemples 5.2.
— Un groupe d'ordre < 60 n'est pas simple.
— $\mathfrak{A}_5$ est l'unique groupe simple d'ordre 60.
— Un groupe d'ordre $60 < . < 168$ n'est pas simple.
— $\mathrm{SL}_3(\mathbb{F}_2) \cong \mathrm{PSL}_2(\mathbb{F}_7)$ est l'unique groupe simple d'ordre 168.

6 Groupes de permutations

6.1 Généralités sur le groupe symétrique

Définition 6.1. Soit X un ensemble. On note $\mathfrak{S}(X)$ l'ensemble des bijections de X dans X.

Proposition 6.2. *L'ensemble $\mathfrak{S}(X)$ muni de la composition est un groupe, appelé groupe des permutations de X.*

Exemple 6.3. Si $X = \{1, \ldots, n\}$, alors $\mathfrak{S}(X)$ est noté $\mathfrak{S}_n$.

Notations : on peut représenter une permutation σ de $\mathfrak{S}_n$ par un tableau à deux lignes et n colonnes. Sur la colonne supérieure on place les entiers de 1 à n, et en-dessous de chaque entier $1 \leq k \leq n$, on place l'entier $\sigma(k)$.

Proposition 6.4. $|\mathfrak{S}_n| = n!$.

Définition 6.5. Soit $\sigma \in \mathfrak{S}_n$ et $1 \leq k \leq n$.

On dit que k est un point fixe de σ si $\sigma(k) = k$. L'ensemble des points fixes de σ est noté $\mathrm{Fix}(\sigma)$.

Le support de σ est $\mathrm{Supp}(\sigma) := \{1 \leq k \leq n : \sigma(x) \neq x\}$.

Le groupe $\mathfrak{S}(X)$ est muni de son action naturelle sur l'ensemble X.

Proposition 6.6. *L'action de $\mathfrak{S}_n$ sur $\{1, \ldots, n\}$ est transitive. Elle est même n-transitive.*

En particulier, la formule de Burnside assure que le nombre moyen de points fixes d'une permutation de $\mathfrak{S}_n$ est 1.

6.2 Structure du groupe symétrique

Définition 6.7. Soient $2 \leq k \leq n$ et $a_1, \ldots, a_k \in \{1, \ldots, n\}$ des éléments deux-à-deux distincts.

Le k-cycle σ défini par la suite $(a_1, \ldots, a_k)$ est la permutation définie par $\sigma(a_i) = a_{i+1}$ pour tout i (avec la convention $a_{k+1} = a_1$) et $\sigma(x) = x$ si $x \notin \{a_1, \ldots, a_k\}$. On le note $\sigma = (a_1 \ \ldots \ a_k)$.

L'entier k est appelé longueur du cycle $(a_1 \ \ldots \ a_k)$. un cycle de longueur 2 (ou 2-cycle) est appelé une transposition.

Lemme 6.8. *Soit $\sigma \in \mathfrak{S}_n$ et $(a_1 \ \ldots \ a_k)$ un cycle.*

Alors $\sigma \circ (a_1 \ \ldots \ a_k) \circ \sigma^{-1} = (\sigma(a_1) \ \ldots \ \sigma(a_k))$.

Démonstration: Il s'agit de calculer les images des éléments $\sigma(a_i)$ pour tout i, puis des éléments $\notin \{\sigma(a_1), \ldots, \sigma(a_k)\}$. □

Corollaire 6.9. *Pour tout $n \neq 2$, $Z(\mathfrak{S}_n) = \{\mathrm{id}\}$.*

Démonstration: Soit $n \geq 3$ et $\sigma \in Z(\mathfrak{S}_n)$. Soit $1 \leq i \leq n$. Alors pour tout $1 \leq i \neq j \leq n$, $\sigma \circ (i\,j) \circ \sigma^{-1} = (i\,j)$. Donc par le lemme 6.8, $(\sigma(i)\,\sigma(j)) = (i\,j)$. Donc $\sigma(i) \in \{i, j\}$ pour tout $j \neq i$, donc (comme $n \geq 3$), $\sigma(i) = i$. Donc $\sigma = \mathrm{id}$. □

Le résultat suivant est fondamental :

Théorème 6.10. *Soit $\sigma \in \mathfrak{S}_n$.*

Alors il existe des cycles c_1, …, c_k à supports disjoints, tels que $\sigma = c_1 \circ \cdots \circ c_k$. De plus, cette décomposition est unique, à l'ordre près des facteurs.

Démonstration:

— On considère l'action du sous-groupe $\langle\sigma\rangle < \mathfrak{S}_n$ sur $X_n = \{1, \ldots, n\}$. Alors X_n est partionné par les orbites sous cette action, i.e. $X_n = \bigcup_{i=1}^{k} \omega_i$ (union disjointe), où les ω_i sont les orbites. Alors par construction, pour tout $1 \leq i \leq k$, $\omega_i \subset X_n$ est stable par σ, et si $|\omega_i| > 1$, la restriction de σ à ω_i est un cycle noté c_i (en l'occurence, si $j \in \omega_i$ et $|\omega_i| = l_i$, alors la restriction est le l_i-cycle $(j\,\sigma(j) \ \ldots \ \sigma^{l_i-1}(j))$). Par construction, les supports des c_i sont disjoints. Enfin, on a $\sigma = c_1 \circ \cdots \circ c_k$ (en enlevant les orbites réduites à un point), puisque c'est vrai en restriction à chaque orbite ω_i.

— Unicité : soient $d_1, \ldots, d_r$ des cycles à supports disjoints tels que $\sigma = d_1 \circ \cdots \circ d_r$. Alors les orbites ω_i non réduites à un point sont exactement les supports des d_j. Autrement dit, $r = k$ et il existe une bijection $i \mapsto j_i$ de $\{1, \ldots, r\}$ telle que pour tout i, $\mathrm{supp}(d_{j_i}) = \omega_i = \mathrm{supp}(c_i)$. Alors la restriction de σ à ω_i est égale à d_{j_i} puisque les autres d_l ont un support disjoint de ω_i, et cette restriction est égale à c_i par la première partie de la preuve. Donc pour tout i, $c_i = d_{j_i}$.

□

Corollaire 6.11. *Soient $\sigma, \sigma' \in \mathfrak{S}_n$. Pour tout $1 \leq k \leq n$, on note n_k (resp. n'_k) le nombre de cycles de longueur k dans la décomposition de σ (resp. σ') en produit de cycles à supports disjoints.*

Alors σ et σ' sont conjugués dans $\mathfrak{S}_n$ si et seulement si pour tout $1 \leq k \leq n$, $n_k = n'_k$.

Démonstration: C'est la conséquence du lemme 6.8 et du théorème 6.10. □

En particulier, le nombre de classes de conjugaison dans $\mathfrak{S}_n$ est égal au nombre $p(n)$ de partitions de l'entier n, i.e. le nombre de façon d'écrire n comme une somme d'entiers croissants ≥ 1.

Lemme 6.12. *Soit $c = (a_1 \ \ldots \ a_k)$.*
Alors $c = (a_1\, a_2) \circ \cdots \circ (a_{k-1}\, a_k)$.

Proposition 6.13. *Tout élément de $\mathfrak{S}_n$ est produit de transpositions.*

Démonstration: C'est la conjonction du théorème 6.10 et du lemme 6.12. □

Remarque 6.14. En revanche, cette décomposition n'est pas unique : $\mathrm{id} = (1\,2) \circ (1\,2)$.

Une application géométrique :

Théorème 6.15. *On se place dans un espace affine euclidien de dimension 3.*

1. *Le groupe des isométries d'un tétraèdre régulier est isomorphe à $\mathfrak{S}_4$.*
2. *Le groupe des isométries directes d'un cube ou d'un octaèdre est isomorphe à $\mathfrak{S}_4$.*

Une application en théorie des groupes :

Théorème 6.16. *Pour tout $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur.*

Démonstration: Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$.

Pour toute transposition τ, $\varphi(\tau)$ est d'ordre 2, donc produit de $k \geq 1$ transpositions à supports disjoints. Or les transpositions forment une classe de conjugaison dans $\mathfrak{S}_n$, donc φ envoie l'ensemble des transpositions bijectivement sur l'ensemble des produits de k transpositions à supports dijoints (en utilisant le corollaire 6.11. Par conséquent, le nombre de transpositions est égal au nombre de tels produits. Or le nombre de transpositions vaut exactement $\binom{n}{2}$, alors que le nombre de produits k transpositions à supports disjoints vaut

$$\frac{\binom{n}{2} \cdot \binom{n-2}{2} \cdot \cdots \cdot \binom{n-2(k-1)}{2}}{k!} = \frac{n!}{2^k k!(n-2k)!}\,.$$

Or ces deux nombres sont égaux si et seulement si $(n-2)! = 2^{k-1} \cdot k!(n-2k)!$ si et seulement si $\binom{n-k}{k}(n-2)\dots(n-k+1) = 2^{k-1}$ si et seulement si $k=1$ ou ($k=2$ et $(n-2)(n-3)=4$) ou ($k \geq 3$ et $n-2 = n-k+1 \leq 2$) si et seulement si $k=1$ ou ($k=3$ et $n=6$).

Comme $n \neq 6$, on a $k=1$ et φ envoie les transpositions sur des transpositions. Notons $\tau_i := (1\,i)$. Alors pour tout i, $\varphi(\tau_i)$ est une transposition, et si $i \neq j$, $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne commutent pas (car τ_i et τ_j ne commutent pas), donc leurs supports ont une intersection de cardinal 1. Notons $a_{i,j}$ l'unique élément dans cette intersection. Si i,j,k,l sont deux-à-deux distincts (donc $n \geq 5$), on voit que σ_i, σ_j, σ_k et σ_l ont un élément commun dans leurs supports, donc $a_{i,j}$ ne dépend pas de i et j. La même conclusion vaut si $n=3$. On le note a_1, et alors pour tout i, il existe un unique $a_i \neq a_1$ tel que $\varphi(\tau_i) = (a_1\,a_i)$. On vérifie alors facilement que $\sigma : i \mapsto a_i$ est dans $\mathfrak{S}_n$, et $\sigma \circ \tau_i \circ \sigma^{-1} = \varphi(\tau_i)$ pour tout i. Comme les transpositions σ_i engendrent $\mathfrak{S}_n$, on en déduit que φ est intérieur, c'est la conjugaison par σ.

Si $n = 1$, 2 le résultat est évident. Reste le cas $n = 4$: □

Résumé sur les générateurs de $\mathfrak{S}_n$:

Théorème 6.17. ⋆ *Le groupe $\mathfrak{S}_n$ est engendré par les cycles ; par les transpositions ; par les transpositions $(1\ i)$, $2 \leq i \leq n$; par les transpositions $(i\ i+1)$, $1 \leq i \leq n-1$; par la transposition $(1\ 2)$ et le cycle $(1\ 2\ \dots\ n)$.*

Une application : l'algorithme de tri à bulles (bubble sort) permet de trier une liste de n éléments en faisant uniquement des comparaisons d'élements voisins et des échanges d'élements voisins.

Proposition 6.18. *Soit $P \subset \mathfrak{S}_n$ une partie formée de transpositions. Si $\langle P \rangle = \mathfrak{S}_n$, alors $|P| \geq n-1$.*

6.3 Signature, groupe alterné

Définition 6.19. Pour tout $\sigma \in \mathfrak{S}_n$, on pose

$$\varepsilon(\sigma) := \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j} \in \{\pm 1\},$$

appelée signature de σ.

Remarque 6.20. On peut en fait indicer ce produit par l'ensemble des paires d'entiers distincts entre 1 et n.

Proposition 6.21. *L'application $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un morphisme de groupes.*

Démonstration:

$$\begin{aligned} \varepsilon(\sigma\circ\tau) &= \textstyle\prod_{i<j} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{i-j} = \prod_{i<j} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} \cdot \frac{\tau(i)-\tau(j)}{i-j} \\ &= \varepsilon(\tau) \cdot \textstyle\prod_{i<j} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)}. \end{aligned}$$

En faisant un changement d'indices, on voit que $\prod_{i<j} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} = \prod_{k<l} \frac{\sigma(k)-\sigma(l)}{k-l} = \varepsilon(\sigma)$, d'où le résultat. □

Exemples 6.22. — Si τ est une transposition, alors $\varepsilon(\tau) = -1$. En particulier, ε est l'unique morphisme de groupes $\mathfrak{S}_n \to \mathbf{C}^\times$ tel que $\varepsilon(\tau) = -1$ pour toute transposition τ.

— Si c est un k-cycle, alors $\varepsilon(c) = (-1)^{k-1}$. De nouveau, cette propriété caractérise la signature.

Définition 6.23. Le groupe alterné $\mathfrak{A}_n$ est le noyau du morphisme ε. C'est un sous-groupe distingué d'indice 2 dans $\mathfrak{S}_n$.

En particulier, $|\mathfrak{A}_n| = \frac{n!}{2}$.

Proposition 6.24. *Pour tout $n \geq 2$, pour tout groupe abélien A et tout morphisme de groupe $\varphi : \mathfrak{S}_n \to A$, il existe un unique morphisme de groupes $\overline{\varphi} : \{\pm 1\} \to A$ tel que $\varphi = \overline{\varphi} \circ \varepsilon$.*

Démonstration: Soit $\varphi : G \to A$ comme dans l'énoncé.

Le corollaire 6.11 assurent que les transpositions sont toutes conjuguées. Comme A est abélien, cela assure que toutes les transpositions ont même image $a \in A$ par φ. En outre, a vérifie $a^2 = 1$. Si $a = 1$, alors toutes les transpositions sont dans le noyau de φ, et la proposition 6.13 assure que φ est le morphisme trivial, auquel cas $\overline{\varphi}$ est le morphisme trivial. Supposons maintenant que $a \neq 1$. Il existe un unique morphisme de groupes $\overline{\varphi} : \{\pm 1\} \to A$ tel que $\varphi(-1) = a$. Alors $\varphi(\tau) = \overline{\varphi} \circ \varepsilon(\tau)$ pour toute tranposition τ. Par la proposition 6.13, on a bien $\varphi = \overline{\varphi} \circ \varepsilon$. L'unicité de $\overline{\varphi}$ est évident et résulte de la surjectivité de ε. □

En particulier, $\mathfrak{A}_n$ est le seul sous-groupe d'indice 2 dans $\mathfrak{S}_n$

La description des classes de conjugaison dans $\mathfrak{A}_n$ est un peu plus subtile que dans $\mathfrak{S}_n$. On remarque d'abord que puisque $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$, la classe de conjugaison dans $\mathfrak{S}_n$ d'un élément de $\mathfrak{A}_n$ est contenue dans $\mathfrak{A}_n$. Comme $\mathfrak{A}_n$ est d'indice 2 dans $\mathfrak{S}_n$, pour tout $\sigma \in \mathfrak{A}_n$, la classe de conjugaison de σ dans $\mathfrak{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathfrak{A}_n$, soit réunion de deux classes de conjugaison dans $\mathfrak{A}_n$ (celle de σ et une autre). Montrons alors que l'on est dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition.

En effet, si σ admet un cycle c de longueur paire, pour tout $\tau \in \mathfrak{S}_n$, on a $\tau \circ \sigma \circ \tau^{-1} = (\tau \circ c) \circ \sigma \circ (\tau \circ c)^{-1}$, ce qui assure que les classes de conjugaison dans $\mathfrak{A}_n$ et $\mathfrak{S}_n$ coïncident. Si σ admet deux cycles $c = (a_1, \ldots, a_{2k+1})$ et $c' = (a'_0, \ldots, a'_{2k+1})$ de même longueur impaire, alors si on note $d := (a_1\, a'_1) \circ \cdots \circ (a_{2k+1}\, a'_{2k+1})$ (permutation impaire), on a pour tout $\tau \in \mathfrak{S}_n$, $\tau \circ \sigma \circ \tau^{-1} = (\tau \circ d) \circ \sigma \circ (\tau \circ d)^{-1}$, ce qui assure que les classes de conjugaison dans $\mathfrak{A}_n$ et $\mathfrak{S}_n$ coïncident.

Réciproquement, si σ n'a que des cycles de longueurs impaires deux-à-deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ, et on voit facilement que $(i\, j) \circ \sigma \circ (i\, j)$ n'est pas conjuguée à σ dans $\mathfrak{A}_n$, alors qu'elle l'est dans $\mathfrak{S}_n$.

Corollaire 6.25. *Pour tout $n \geq 1$, $D(\mathfrak{S}_n) = \mathfrak{A}_n$.*

Théorème 6.26. *Pour tout $n \geq 1$,*

1. *le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles.*
2. *si $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.*

Démonstration:

1. La proposition 6.13 assure que tout élément $\sigma \in \mathfrak{A}_n$ est produit d'un nombre pair de transpositions. Il suffit donc de montrer que tout produit de deux transpositions est un produit de 3-cycles.

   Soient $\tau = (i\,j)$ et $\tau' = (k\,l)$ deux transpositions.
   — Si les supports de τ et τ' ne sont pas disjoints, alors $\tau \circ \tau' = \mathrm{id}$ ou $\tau \circ \tau'$ est un 3-cycle (en effet, si i, j et k sont deux-à-deux distincts, alors $(i\,j) \circ (i\,k) = (i\,k\,j)$).
   — Si les supports de τ et τ' sont disjoints, alors

   $$\tau \circ \tau' = (i\,j) \circ (k\,l) = (i\,j) \circ (j\,k) \circ (j\,k) \circ (k\,l) = (i\,j\,k) \circ (j\,k\,l)\,.$$

   Dans tous les cas, $\tau \circ \tau'$ est bien un produit de 3-cycles.

2. Soient $\sigma = (a\,b\,c)$ et $\sigma' = (a'\,b'\,c')$ deux 3-cycles. Il existe $\tau \in \mathfrak{S}_n$ par $\tau(a) = a'$, $\tau(b) = b'$ et $\tau(c) = c'$. Alors $\tau \circ \sigma \circ \tau^{-1} = \sigma'$. Si $\tau \notin \mathfrak{A}_n$, alors il existe $d \neq e \in \{1, \ldots, n\} \setminus \{a, b, c\}$ car $n \geq 5$. Alors $\tau' := \tau \circ (d\,e) \in \mathfrak{A}_n$ et $\tau' \circ \sigma \circ \tau'^{-1} = \sigma'$, ce qui conclut la preuve.

□

Corollaire 6.27. *Si $n \geq 5$, $D(\mathfrak{A}_n) = \mathfrak{A}_n$.*

Démonstration: En utilisant le théorème 6.26, il suffit de montrer que tout 3-cycle est dans $D(\mathfrak{A}_n)$. Soit $\tau = (a\,b\,c)$ un 3-cycle. Alors on vérifie par exemple que, pour tout $d \neq e \in \{1, \ldots, n\} \setminus \{a, b, c\}$,

$$(a\,b\,c) = (a\,b\,d) \circ (a\,c\,e) \circ (a\,b\,d)^{-1} \circ (a\,c\,e)^{-1} = [(a\,b\,d), (a\,c\,e)]\,,$$

donc $\tau \in D(\mathfrak{A}_n)$. □

Une application : le groupe $\mathfrak{S}_5$ n'est pas un groupe résoluble. La théorie de Galois (hors programme) permet d'en déduire que l'équation générale de degré 5 n'est pas résoluble par radicaux ; autement dit, il n'existe pas de formule utilisant uniquement des sommes, des produits, et des racines k-ièmes des coefficients, permettant de calculer les solutions de toutes les équations polynômiales de degré 5. En revanche, ces formules existent en degré $n \leq 4$, car le groupe $\mathfrak{S}_n$ est alors résoluble.

Corollaire 6.28. *Pour tout $n \geq 3$, $n \neq 4$, le groupe $\mathfrak{A}_n$ est simple.*

Démonstration: On suppose $n \geq 5$. Soit $N \subset \mathfrak{A}_n$ un sous-groupe distingué distinct de $\{\mathrm{id}\}$.

1. On suppose $n = 5$. Par le théorème 6.26, les 3-cycles sont conjugués dans $\mathfrak{A}_5$. Montrons que toutes les bitranspositions sont également conjuguées : soient $\sigma = \tau_1 \circ \tau_2$ et $\sigma' = \tau_1' \circ \tau_2'$ deux bitranspositions. Par le corollaire 6.11, il existe $\mu \in \mathfrak{A}_5$ tel que $\mu \circ \sigma \circ \mu^{-1} = \sigma'$. Si $\mu \notin \mathfrak{A}_5$, alors on remplace μ par $\mu \circ \tau_1 \in \mathfrak{A}_5$. Enfin, il existe exactement deux classes de conjugaison de 5-cycles dans $\mathfrak{A}_5$: celle de $(1\,2\,3\,4\,5)$ et celle de $(1\,2\,3\,5\,4)$. Par conséquent, les classes de conjugaison dans $\mathfrak{A}_5$ (qui est de cardinal 60) sont de cardinal respectif 1 (identité), 20 (3-cycles),

15 (bitranspositions), 12 et 12 (5-cycles). Or N étant distingué, il est réunion (disjointe) de classes de conjugaison. Son cardinal est donc parmi

$$\{1+20, 1+15, 1+12, 1+20+15, 1+20+12, 1+15+12, 1+12+12,$$
$$1+20+15+12, 1+20+12+12, 1+15+12+12, 1+20+15+12+12\}$$
$$= \{21, 16, 13, 36, 33, 28, 25, 48, 45, 40, 60\}$$

Or le cardinal de N divise 60, donc la seule possibilité est 60, donc $N = \mathfrak{A}_5$, donc $\mathfrak{A}_5$ est simple.

2. Soit $n \geq 5$ et $\{\mathrm{id}\} \neq N < \mathfrak{A}_n$ un sous-groupe distingué. Pour montrer que $N = \mathfrak{A}_n$ (et donc que $\mathfrak{A}_n$ est simple), il suffit de montrer que N contient un 3-cycle. Pour cela, on va se ramener au cas de $\mathfrak{A}_5$ traité plus haut, en construisant $\sigma \neq \mathrm{id}$ dans N tel que $|\mathrm{supp}(\sigma)| \leq 5$. On commence par choisir $\mathrm{id} \neq \tau \in N$, et $a \in \{1, \ldots, n\}$ tel que $b := \tau(a) \neq a$. Puis on choisit $c \in \{1, \ldots, n\} \setminus \{a, b, \tau(b)\}$ (c'est possible car $n \geq 4$).
Considérons alors $\sigma := [(a\,b\,c); \tau] = (a\,b\,c) \circ \tau \circ (a\,c\,b) \circ \tau^{-1}$. Comme N est distingué, on voit que $\sigma \in N$. En outre, $\sigma = (a\,b\,c) \circ (b\,\tau(c)\,\tau(b))$ grâce au lemme 6.8. Donc le support de σ est contenu dans $X := \{a, b, c, \tau(b), \tau(c)\}$, qui est de cardinal au plus 5. Quitte à ajouter un ou deux autre éléments de $\{1, \ldots, n\}$ à X, on peut supposer $|X| = 5$ et $\sigma(i) = i$ pour tout $i \notin X$. En particulier, la restriction de σ à X défini un élément $\sigma_X \in \mathfrak{S}(X) \xrightarrow{\sim} \mathfrak{S}_5$. Notons que l'on peut voir naturellement $\mathfrak{S}$ comme un sous-groupe de $\mathfrak{S}_n$. En outre, on voit que $N' := N \cap \mathfrak{S}(X)$ est un sous-groupe distingué de $\mathfrak{S}(X) \cap \mathfrak{A}_n \xrightarrow{\sim} \mathfrak{A}_5$. Or $\sigma \neq \mathrm{id}$ car $\sigma(\tau(b)) = c$ et $c \neq \tau(b)$ par construction. Donc $N' \neq \{\mathrm{id}\}$. Comme $\mathfrak{A}_5$ est simple, $N' = \mathfrak{A}_5$, donc N' contient un 3-cycle. Alors ce 3-cycle est aussi dans N, ce qui conclut la preuve.

□

Remarque 6.29. On peut aussi montrer que $\mathfrak{A}_5$ est le seul groupe simple d'ordre 60, et que c'est le plus petit groupe simple non abélien (cela utilise les théorèmes de Sylow a priori).

Corollaire 6.30. *Pour tout $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Corollaire 6.31. *Pour $n \geq 5$, tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.*

Démonstration: Soit H un sous-groupe d'indice n de $G = \mathfrak{S}_n$. On dispose de l'action naturelle de G sur $X = G/H$, définie par $g \cdot (g'H) := (gg')H$. Cette action définit un morphisme $\varphi : G \to \mathfrak{S}(X)$. Considérons la restriction de φ au sous-groupe H, i.e. $\psi : H \to \mathfrak{S}(X)$. On constate que H agit trivialement sur l'élément $H \in X$, donc en posant $Y := X \setminus \{H\}$, ψ induit $\psi' : H \to \mathfrak{S}(X') \cong \mathfrak{S}_{n-1}$. Notons $N = \ker(\psi') < H$. Alors N est contenu dans $\ker(\varphi)$. Montrons que φ est injective : $\ker(\varphi)$ est un sous-groupe distingué de $\mathfrak{S}_n$. Par le corollaire précédent, $\ker(\varphi)$ est égal à $\{\mathrm{id}\}$, $\mathfrak{A}_n$ ou $\mathfrak{S}_n$. Or l'action de $\mathfrak{S}_n$ sur X est transitive, et $|X| = n$, donc $\ker(\varphi) \neq \mathfrak{X}_n$, et $\ker(\varphi) \neq \mathfrak{A}_n$ (sinon $|X| \leq 2$). Donc $\ker(\varphi) = \{\mathrm{id}\}$, donc $N = \{\mathrm{id}\}$, donc ψ' est injective. Or $|H| = |\mathfrak{S}_{n-1}|$, donc $\psi' : H \xrightarrow{\sim} \mathfrak{S}_{n-1}$ est un isomorphisme. □

6.4 Quelques applications du groupe symétrique

6.4.1 Groupes d'isométries de polyèdres

Exemple 6.32. Soit Δ un triangle équilatéral, de sommets A, B et C, dans un plan euclidien. Notons $\mathrm{Is}(\Delta)$ le sous-groupe des isométries du plan préservant Δ. Alors on dispose d'un morphisme naturel

$$\mathrm{Is}(\Delta) \to \mathfrak{S}(\{A, B, C\})$$

défini par $u \mapsto u_{|\{A,B,C\}}$ (vérifier que cela est bien défini). On montre facilement que c'est un isomorphisme de groupes. Donc $\mathrm{Is}(\Delta) \cong \mathfrak{S}_3$.

Théorème 6.33. *Soit Δ (resp. $\square$) un tétraèdre régulier (resp. un cube) dans un espace euclidien de dimension 3. Alors on dispose d'isomorphismes de groupes*

$$\mathrm{Is}(\Delta) \cong \mathfrak{S}_4$$

et

$$\mathrm{Is}(\square) \cong \mathfrak{S}_4 \times \mathbf{Z}/2\mathbf{Z}\,.$$

Démonstration. Il s'agit de faire agir le groupe d'isométries sur l'ensemble des quatre sommets du tétraèdre (resp. sur l'ensemble des quatre grands diagonales du cube) et de vérifier que cela induit les isomorphismes annoncés. □

Remarque 6.34. On peut montrer de même que le groupe des isométries d'un dodécaèdre (ou d'un icosaèdre) régulier est isomorphe à $\mathfrak{A}_5 \times \mathbf{Z}/2\mathbf{Z}$.

6.4.2 Quelques isomorphismes exceptionnels

Si k est un corps, on rappelle que $\mathrm{PGL}_n(k)$ est le quotient de $\mathrm{GL}_n(k)$ par le sous-groupe central $k^\times I_n$ formé des homothéties, et $\mathrm{PSL}_n(k)$ est le quotient de $\mathrm{SL}_n(k)$ par le sous-groupe formé des homothèties de déterminant 1, i.e. $\mu_n(k)I_n$.

Théorème 6.35. *On dispose d'isomorphismes de groupes :*
- $\mathrm{SL}_2(\mathbf{F}_2) = \mathrm{GL}_2(\mathbf{F}_2) = \mathrm{PGL}_2(F_2) = \mathrm{PSL}_2(\mathbf{F}_2) \cong \mathfrak{S}_3$.
- $\mathrm{PGL}_2(\mathbf{F}_3) \cong \mathfrak{S}_4$ *et* $\mathrm{PSL}_2(\mathbf{F}_3) \cong \mathfrak{A}_4$.
- $\mathrm{PSL}_2(\mathbf{F}_4) = \mathrm{PGL}_2(\mathbf{F}_4) \cong \mathfrak{A}_5$.
- $\mathrm{PGL}_2(\mathbf{F}_5) \cong \mathfrak{S}_5$ *et* $\mathrm{PSL}_2(\mathbf{F}_5) \cong \mathfrak{A}_5$.

Démonstration. On considère l'action naturelle de $\mathrm{GL}_2(\mathbf{F}_q)$ sur l'ensemble, noté $\mathbf{P}^1(\mathbf{F}_q)$, des droites (vectorielles) dans $\mathbf{F}_q^2$. Cette action induit un morphisme de groupes

$$\varphi_q : \mathrm{GL}_2(\mathbf{F}_q) \to \mathfrak{S}(\mathbf{P}^1(\mathbf{F}_q))\,.$$

Calculons le noyau de φ. Soit $A \in \mathrm{GL}_2(\mathbf{F}_q)$. On a $A \in \ker(\varphi_q)$ si et seulement si pour toute droite Δ de $\mathbf{F}_q^2$, $A \cdot \Delta = \Delta$ si et seulement si tout droite de $\mathbf{F}_q^2$ est une droite propre pour A si et seulement si tout vecteur non nul de $\mathbf{F}_q^2$ est vecteur propre de A si et seulement si A est une homothétie, i.e. dans $\mathbf{F}_q^\times I_2$ (exercice classique). Donc $\ker(\varphi_q) = \mathbf{F}_q^\times I_2$. Par la propriété universelle du quotient, φ induit un morphisme injectif de groupes

$$\overline{\varphi}_q : \mathrm{PGL}_2(\mathbf{F}_q) := \mathrm{GL}_2(\mathbf{F}_q)/(\mathbf{F}_q^\times I_2) \hookrightarrow \mathfrak{S}(\mathbf{P}^1(\mathbf{F}_q))\,.$$

Or $|\mathbf{P}^1(\mathbf{F}_q)| = q+1$, donc une numérotation des droites induit un morphisme injectif

$$\overline{\varphi}_q : \mathrm{PGL}_2(\mathbf{F}_q) \hookrightarrow \mathfrak{S}_{q+1}\,.$$

Or les cardinaux des deux groupes en question sont :

$$|\mathrm{PGL}_2(\mathbf{F}_q)| = \frac{(q^2-1)(q^2-q)}{q-1} = (q-1)q(q+1)\,,$$

et

$$|\mathfrak{S}_{q+1}| = (q+1)!\,.$$

Pour $q = 2, 3, 4, 5$, calculons explicitement ces valeurs :

q	$\lvert\mathrm{PGL}_2(\mathbf{F}_q)\rvert$	$\lvert\mathfrak{S}_{q+1}\rvert$
2	6	6
3	24	24
4	60	120
5	120	720

On voit donc immédiatemment que $\varphi_2 : \mathrm{PGL}_2(\mathbf{F}_2) \xrightarrow{\sim} \mathfrak{S}_3$ et $\varphi_3 : \mathrm{PGL}_2(\mathbf{F}_3) \xrightarrow{\sim} \mathfrak{S}_4$ sont des isomorphismes. Puisque $\mathfrak{A}_4$ est le seul sous-groupe d'indice 2 dans $\mathfrak{S}_4$, on en déduit l'isomorphisme $\mathrm{PSL}_2(\mathbf{F}_3) \xrightarrow{\sim} \mathfrak{A}_4$.

Pour $q = 4$, on voit que $\mathrm{im}\,(\varphi_4)$ est un sous-groupe d'indice 2 de $\mathfrak{S}_5$, donc est égal à $\mathfrak{A}_5$, d'où l'isomorphisme $\varphi_4 : \mathrm{PSL}_2(\mathbf{F}_4) = \mathrm{PGL}_2(\mathbf{F}_4) \xrightarrow{\sim} \mathfrak{A}_5$.

Enfin, pour $q = 5$, on voit que $\mathrm{im}\,(\varphi_5)$ est un sous-groupe d'indice 6 de $\mathfrak{S}_6$, il est donc isomorphe à $\mathfrak{S}_5$ par le corollaire 6.31, ce qui permet de conclure. □

Remarque 6.36. L'isomorphisme $\mathrm{PGL}_2(\mathbf{F}_5) \cong \mathfrak{S}_5$ permet de construire un automorphisme non intérieur de $\mathfrak{S}_6$ (voir théorème 6.16).

Remarque 6.37. Plus difficile, et utilisant le théorème de Sylow, on peut montrer l'isomorphisme exceptionnel $\mathrm{PSL}_2(\mathbf{F}_9) \cong \mathfrak{A}_6$

6.4.3 Combinatoire et coloriages de polyèdres

On dénombre les coloriages des faces d'un polyèdre avec n couleurs (à rotation près).

Théorème 6.38. *Soit X un ensemble fini muni d'une action d'un groupe fini G. Soit $C = \{1, \ldots, n\}$ l'ensemble des couleurs. Un coloriage de X (avec au plus n couleurs) est un élément de C^X.*

Alors le nombre de coloriages de X (modulo G) est exactement $N = \frac{1}{|G|}\sum_{\sigma\in G} n^{\lambda(\sigma)}$, où $\lambda(\sigma)$ est le nombre de cycles de σ vu comme permutation de X.

Exemple 6.39. Il y a exactement $N = \frac{n^6+3n^4+12n^3+8n^2}{24}$ coloriages des faces du cubes avec (au plus) n couleurs (à rotation près).

Remarque 6.40. Ce théorème est un cas particulier du théorème de Polyà.

6.4.4 Autres applications

Déterminant (cf cours d'algèbre linéaire), polynômes (anti)-symétriques (cf cours sur les polynômes), relations coefficients-racines (idem), Frobenius-Zolotarev (cf cours d'algèbre linéaire), combinatoire du nombre de dérangements, décomposition de Bruhat, tables de caractères de $\mathfrak{S}_n$ et $\mathfrak{A}_n$ ($n \leq 5$)...

7 Groupes de petits cardinaux

On peut procéder de façon élémentaire à la classification des groupes finis de petits cardinaux. Dans ce texte, on se limite à la classification des groupes de cardinal ≤ 11.

Théorème 7.1. *Les groupes de cardinal ≤ 11 et $\neq 8$ sont exactement les groupes suivants, deux-à-deux non isomorphes :*

- *le groupe trivial $\{e\}$ d'ordre 1.*
- *le groupe $\mathbf{Z}/2\mathbf{Z}$ d'ordre 2.*
- *le groupe $\mathbf{Z}/3\mathbf{Z}$ d'ordre 3.*
- *les groupes $\mathbf{Z}/4\mathbf{Z}$ et $(\mathbf{Z}/2\mathbf{Z})^2$ d'ordre 4.*
- *le groupe $\mathbf{Z}/5\mathbf{Z}$ d'ordre 5.*
- *les groupes $\mathbf{Z}/6\mathbf{Z}$ et $\mathbf{D}_3 \cong \mathfrak{S}_3$ d'ordre 6.*
- *le groupe $\mathbf{Z}/7\mathbf{Z}$ d'ordre 7.*
- *les groupes $\mathbf{Z}/9\mathbf{Z}$ $(\mathbf{Z}/3\mathbf{Z})^2$ d'ordre 9.*
- *les groupes $\mathbf{Z}/10\mathbf{Z}$ et $\mathbf{D}_5$ (groupe des isométries du pentagone régulier) d'ordre 10.*
- *le groupe $\mathbf{Z}/11\mathbf{Z}$ d'ordre 11.*

Démonstration. Pour les cardinaux ≤ 5 et 7, 9 et 11, il suffit d'appliquer le corollaire 4.23, la proposition 3.5 et les théorèmes 3.2 et 3.19.

Il reste donc à traiter les groupes non abéliens de cardinaux 6 et 10. Soit G un groupe non abélien d'ordre 6 (resp. 10).

Par le théorème de Cauchy, il existe un élément r d'ordre 3 (resp. 5) dans G. De même, il existe un élément s d'ordre 2 dans G. Alors par cardinalité, on a $G = \langle r, s\rangle$. Puisque s est d'ordre 2, on calcule immédiatemment que $sr = r^2 s$ (resp. $sr = r^4 s$). On décrit facilement les éléments de G comme étant e, r, r^2, s, sr, sr^2 (resp. e, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4). On vérifie enfin que la table de multiplication de G correspond alors exactement à celle du groupe diédral de même cardinal.

Remarquons que si G est un groupe non abélien d'ordre 6, il admet un élément d'ordre 2 par Cauchy, Cet élément n'est pas central (sinon G est abélien), et son orbite pour l'action de G par conjugaison (i.e. sa classe de conjugaison) est donc de cardinal 3. Donc G agit par conjugaison sur cette classe de conjugaison X, induisant un morphisme $G \to \mathfrak{S}(X) \cong \mathfrak{S}_3$. Un élément dans le noyau de ce morphisme commute avec les trois éléments d'ordre 3 de X, donc avec tout élément de G, ce qui assure que le noyau est trivial (sinon G est abélien). Donc par cardinalité, c'est un isomorphisme $G \xrightarrow{\sim} \mathfrak{S}_3$. □

Théorème 7.2. *Les groupes de cardinal 8 sont exactement les groupes suivants, deux-à-deux non isomorphes :*

- *les groupes abéliens $\mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et $(\mathbf{Z}/2\mathbf{Z})^3$.*
- *le groupe diédral $\mathbf{D}_4$ des isométries du carré.*
- *le groupe des quaternions $H_8 := \{\pm 1, \pm i, \pm j, \pm k\}$.*

Démonstration. Soit G un groupe d'ordre 8. Notons N l'ordre maximal d'un élément de G (c'est l'exposant de G ici). Alors $N \in \{2, 4, 8\}$. On distingue donc trois cas :

1. si $N = 2$, alors G est d'exposant 2, donc abélien, donc par la classification des groupes abéliens finis, G est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^3$ (on peut éviter la classification en disant que G est naturellement un $\mathbf{Z}/2\mathbf{Z}$-espace vectoriel, et par cardinalité, sa dimension doit être 3).
2. si $N = 8$, alors G est cyclique, donc G est isomorphe à $\mathbf{Z}/8\mathbf{Z}$.
3. si $N = 4$, il existe un élément $a \in G$ d'ordre 4. Notons $H := \langle a \rangle$. Pour tout $b \in G \setminus H$, on a clairement $G = \langle a, b \rangle$. Notons que H est distingué dans G car il est d'indice 2. On a alors deux sous-cas :
   (a) s'il existe $b \in G \setminus H$ d'ordre 2. On choisit alors un tel b. On a alors deux possibilités :
   — si a et b commutent, alors G est abélien, et le morphisme $\langle a \rangle \times \langle b \rangle \to G$ défini par $(a^k, b^\ell) \mapsto a^k b^\ell$ est un isomorphisme entre G et $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
   — si a et b ne commutent pas, alors bab^{-1} est un élément de H (puisque H est distingué), distinct de a et d'ordre 4. On en déduit que $bab^{-1} = a^3 = a^{-1}$. Finalement, G est engendré par a d'ordre 4 et b d'ordre 2 vérifiant $ba = a^{-1}b$, ses éléments sont donc $e, a, a^2, a^3, b, ab, a^2b, a^3b$, et G a exactement la même table de multiplication que le groupe $\mathbf{D}_4$, donc G est isomorphe à $\mathbf{D}_4$.
   (b) si tout élément de $G \setminus H$ est d'ordre 4 : soit b un tel élément. Comme H est d'indice 2, b^2 est un élément d'ordre 2 dans H, donc $b^2 = a^2$. Comme a et b engendrent G, $a^2 = b^2$ est dans le centre de G. En outre, a et b ne commutent pas, sinon $ab \in G \setminus H$ serait d'ordre 2, ce qui est exclu. Comme plus haut, on a donc nécessairement $bab^{-1} = a^{-1}$. Notons $c := ab$. Alors $c \in G \setminus H$ vérifie également $c^2 = a^2$ et $ca = a^2ac$. On a donc $G = \{e, a, a^2, a^3, b, b^3, c, c^3\}$ et la bijection $G \to H_8$ envoyant e sur 1, a^2 sur -1, a (resp. b, resp. c) sur i (resp. j, resp. k) et a^3 (resp. b^3, resp. c^3) sur $-i$ (resp. $-j$, resp. $-k$), est un isomorphisme de groupes, ce qui conclut la preuve.

□

Remarque 7.3. Il y a exactement cinq classes d'isomorphismes de groupes d'ordre 12, dont deux abéliens, le groupe diédral $\mathbf{D}_6$ des isométries de l'hexagone régulier et le groupe $\mathfrak{A}_4$. La description du dernier groupe d'ordre 12 est moins évidente sans utiliser le produit semi-direct.