ÉNS de Lyon
M2 FEADéP

Cours d'algèbre
2019–2020

Groupes : conjugaison et quotients

Table des matières

1 Groupes en action **3**
- 1.1 Premières définitions . . . 3
- 1.2 Action d'un groupe sur un ensemble . . . 3
- 1.3 Action d'un groupe sur lui-même par multiplication . . . 4

2 Conjugaison et groupes distingués **5**
- 2.1 Action d'un groupe sur lui-même par conjugaison . . . 5
- 2.2 Quotients de groupes . . . 6
- 2.3 Sous-groupes caractéristiques . . . 6

3 Le cas des p-groupes **8**
- 3.1 Résultats fondamentaux . . . 8
- 3.2 Complément sur les parties génératrices de p-groupes finis . . . 8

4 Extensions de groupes **10**
- 4.1 Simplicité . . . 10
- 4.2 Extensions de groupes . . . 10
- 4.3 Le problème de la classification . . . 11
- 4.4 Présentation de groupes . . . 11

5 Résultats à connaître sur les groupes usuels finis **12**

Leçons directement concernées (2020)

(103)* Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

(104) Groupes abéliens et non abéliens finis. Exemples et applications.

(105) Groupe des permutations d'un ensemble fini. Applications.

(108) Exemples de parties génératrices d'un groupe. Applications.

Leçons où on parle naturellement de conjugaison et de groupes distingués

(101) Groupe opérant sur un ensemble. Exemples et applications.

(106) Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.

(107)* Représentations et caractères d'un groupe fini sur un $\mathbb{C}$-espace vectoriel. Exemples.

Leçons qui utilisent des techniques de groupes ou d'action de groupe

(102)* Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

(150)* Exemples d'actions de groupes sur les espaces de matrices.

(190) Méthodes combinatoires, problèmes de dénombrement.

(191) Exemples d'utilisation des techniques d'algèbre en géométrie.

Ce qui est dans le programme

(a) Groupes, morphismes de groupes. Produit direct de groupes. Sous-groupes. Sous-groupe engendré par une partie. Ordre d'un élément. Sous-groupes distingués (ou normaux), groupes quotients. Action d'un groupe sur un ensemble. Stabilisateur d'un point, orbites, espace quotient. Formule des classes. Classes de conjugaison. Application à la détermination des groupes d'isométries d'un polytope régulier en dimension 2 et 3.

(b) Groupes cycliques. Groupes abéliens de type fini. Groupe des racines complexes n-ièmes de l'unité, racines primitives.

(c) Groupe des permutations d'un ensemble fini. Décomposition d'une permutation en produit de transpositions, en produit de cycles à supports disjoints. Signature. Groupe alterné. Application : déterminants.

Bibliographie (autour des groupes en général)

- J.-M. Arnaudiès et J. Bertin, *Groupes, algèbres et géométrie.*
- M. Artin, *Algebra.*
- M. Audin, *Géométrie.*
- A. Bouvier et D. Richard, *Groupes, observation, théorie, pratique.*
- J. Calais, *Éléments de théorie des groupes.*
- P. Caldero et G. Germoni, *Histoires hédonistes de groupes et de géométries.*
- J.-C. Carrega, *Théorie des corps - La règle et le compas.*
- P. Colmez, *Éléments d'analyse et d'algèbre (et de théorie des nombres).*
- F. Combes, *Algèbre et géométrie.*
- M. Demazure, *Cours d'algèbre.*
- R. Goblot, *Algèbre commutative.*
- X. Gourdon. *Algèbre.* Ellipse, 2009.
- R. Mneimné et F. Testard, *Introduction à la théorie des groupes de Lie classiques.* Hermann, 1986.
- A. Paugam, *Agrégation de mathématiques – Questions délicates en algèbre et géométrie.* Dunod, 2007.
- D. Perrin, *Cours d'algèbre.*
- G. Peyré, *L'algèbre discrète de la transformée de Fourier.*
- M. Ramis et A. Warusfel, *Mathématiques, tout-en-un pour la licence*, niveau L2, L3.
- J.-E. Rombaldi, *Mathématiques pour l'agrégation : Algèbre & géométrie.*
- J.-P. Serre, *Représentations linéaires des groupes finis.*
- P. Tauvel, *Algèbre.* Dunod, 2005.

1 Groupes en action

La structure de groupe est la structure algébrique la plus élémentaire qu'on puisse mettre sur un ensemble. Historiquement, les groupes sont apparus comme familles de permutations des racines d'un polynôme, de sorte que les relations qu'entretiennent les racines entre elles soient toujours vérifiées.

Par la suite, la géométrie a connu une évolution retentissante avec le point de vue de Félix Klein : définir une géométrie c'est définir l'action d'un groupe sur un ensemble, par exemple par transformations affines, par isométries d'un espace euclidien, par homographies sur un espace projectif, ...

1.1 Premières définitions

On suppose connues les notions de base : groupe, groupe abélien, sous-groupe, produit direct de groupes, morphisme de groupes, noyau et image d'un morphisme de groupes, ordre d'un élément. On rappelle qu'une réunion croissante ou une intersection quelconque de sous-groupes est un sous-groupe.

1.2 Action d'un groupe sur un ensemble

Ces notions ont été vues en cours de Géométrie.

Définition 1.1. Soir G un groupe et X un ensemble. De manière équivalente, une action (à gauche) de G sur X est la donnée :

(i) d'un morphisme de groupes $\varphi : G \to \mathrm{Bij}(X)$;

(ii) d'une application $\lambda : G \times X \to X$ telle que $\forall g, h \in G,\ \forall x \in X,\ \lambda(gh, x) = \lambda(g, \lambda(h, x))$ et $\lambda(e, x) = x$ où e désigne le neutre de G.

Le *noyau d'une action* est $\ker \varphi = G_X$.
L'action est *fidèle* si $\ker \varphi = G_X = 1$.

Dès qu'on saura que le noyau d'un morphisme est distingué, on aura :

Fait 1.2 (Fidélisation)**.** *Le groupe quotient $G/\ker\varphi$ agit fidèlement sur X.*

Remarque 1.3. L'équivalence dans la définition est donnée par $\alpha(g, x) = \phi(g)(x)$. On note souvent $g \cdot x$ au lieu de $\lambda(g, x)$.

On peut définir la notion d'action à droite en remplaçant la condition φ morphisme de groupes par φ anti-morphisme de groupes (i.e. $\varphi(gh) = \varphi(h) \circ \varphi(g)\ \forall g, h$). On pose alors $x \cdot g = \rho(g, x) = \varphi(g)(x)$. On a alors la formule $x \cdot (gh) = (x \cdot g) \cdot h$.

Un peu de vocabulaire :

Définition 1.4. On définit le *stabilisateur*

— d'un point : $G_x = \mathrm{Stab}_G(x) = \{g \in G, g \cdot x = x\}$ est un sous-groupe ;

— d'une partie : $G_{\{Y\}} = \mathrm{Stab}_G(\{Y\}) = \{g \in G, g \cdot Y = Y\}$ (attention au signe « = ») ; c'est le stabilisateur du point Y pour l'action de G sur $\mathcal{P}(X)$ par $g \cdot Y = \{g \cdot y,\ y \in Y\}$;

— point par point : $G_Y = \mathrm{Stab}_G(Y) = \{g \in G, g \cdot y = y \quad \forall y \in Y\} = \bigcap_{y \in Y} \mathrm{Stab}_G(y)$.

On définit les *points fixes* (parfois appelé fixateur) :

— d'un élément : $X^g = \{x \in X,\ g \cdot x = x\} = \{x \in X,\ g \in \mathrm{Stab}_G(x)\}$;

— d'un sous-groupe : $X^H = \bigcap_{h \in H} X^h$.

Une action est dite *libre* si tous les stabilisateurs sont triviaux, autrement dit si tous les fixateurs X^g pour $g \neq e$ sont vides.

Fait 1.5. *Une action libre est fidèle.*

Fait 1.6 (Formule des stabilisateurs)**.**

$$\mathrm{Stab}_G(g \cdot x) = g\,\mathrm{Stab}_G(x)g^{-1}.$$

En particulier, si l'action de G sur X est transitive, alors les stabilisateurs d'un point sont des sous-groupes conjugués dans G.

Définition 1.7. Une *orbite* est une partie de X de la forme $\mathcal{O}(x) = G \cdot x = \{g \cdot x,\ g \in G\}$.

Une action est *transitive* s'il n'y a qu'une seule orbite $G \cdot x = X$ pour tout $x \in X$, autrement dit pour tous $x, y \in X$, il existe $g \in G$ tel que $g \cdot x = y$. Elle est *simplement transitive* si elle est libre et transitive.

Une action est dite *n-transitive* si l'action de G sur l'ensemble des parties à n éléments $\mathcal{P}_n(X)$ est transitive. Une action est dite *exactement* n-transitive si elle est n-transitive mais pas $n+1$-transitive.

Pour montrer qu'une partie $\mathcal{O} \subset X$ est une orbite, il suffit de montrer que :

— $\mathcal{O}$ est non vide ;

— $\mathcal{O}$ est G-stable ;

— l'action de G sur $\mathcal{O}$ est transitive.

Exemple 1.8. Un groupe agit simplement transitivement sur lui-même par multiplication à gauche. Le groupe linéaire $\mathrm{GL}(K^n)$ agit simplement transitivement sur les bases de K^n.

L'action de $\mathfrak{S}_n$ sur $[\![1, n]\!]$ est m-transitive pour tout $m \leqslant n$.

L'action de $\mathrm{PGL}_2(K)$ sur $\mathbb{P}^1(K)$ est exactement 3-transitive (cela permet de définir le birapport).

La relation « être dans une même orbite » est une relation d'équivalence, donc X se partitionne en orbites. Une famille de représentants $(x_i)_{i \in I}$ c'est un choix d'un élément x_i dans chaque orbite $i \in I$.

Proposition 1.9 (Équation aux classes)**.**

$$|G \cdot x| = [G : \mathrm{Stab}_G(x)]$$

Démonstration. $G/\mathrm{Stab}_G(x) \to G \cdot x$ est une bijection. □

Corollaire 1.10 (Formule des classes)**.**

$$|X| = \sum_{i \in I} [G : \mathrm{Stab}_G(x_i)]$$

où $(x_i)_{i \in I}$ famille de représentants.

Proposition 1.11 (Formule de Burnside)**.**

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Application de la formule de Burnside : Tout sous-groupe de $\mathfrak{S}_n$ agissant transitivement sur $[\![1, n]\!]$ contient une permutation sans points fixes.

1.3 Action d'un groupe sur lui-même par multiplication

G agit sur lui-même par multiplication à gauche $g \cdot h = gh$ (resp. par multiplication par l'inverse à droite $g \cdot h = hg^{-1}$). Cette action est simplement transitive.

Fait 1.12 (Théorème de Cayley)**.** *Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$, donc à un sous-groupe de $\mathrm{GL}_n(K)$ quel que soit le corps K.*

En particulier, tout sous-groupe H de G agit sur G via cette action.

Définition 1.13. On appelle *classe à gauche* (resp. à droite) les orbites Hg (resp. gH) de cette action. L'indice d'un sous-groupe H de G noté $[G : H]$ est le nombre d'orbites pour cette action.

Fait 1.14 (Théorème de Lagrange)**.** *Si G est fini alors l'ordre d'un sous-groupe divise l'ordre de G et, en particulier, l'ordre d'un élément divise l'ordre du groupe.*

2 Conjugaison et groupes distingués

2.1 Action d'un groupe sur lui-même par conjugaison

Un groupe agit sur lui-même par conjugaison, c'est-à-dire que

$$\begin{array}{rccc} \varphi : & G & \to & \mathrm{Bij}(G) \\ & g & \mapsto & \mathrm{Int}(g) = (h \mapsto ghg^{-1}) \end{array}$$

est un morphisme de groupes. On appelle *classe de conjugaison* une orbite pour cette action.

Exemple 2.1. Les classes de conjugaison de $\mathfrak{S}_n$ sont décrites par les tailles des cycles dans une décomposition en produit de cycles à supports disjoints.

Les classes de conjugaison dans $\mathrm{GL}_2(K)$ sont les $\{M \in \mathcal{M}_2(K),\ \chi_M = (X-\lambda)(X-\mu)\}$, les $\{M \in \mathcal{M}_2(K),\ \mu_M = (X-\lambda)^2\}$ et les $\{\lambda I_2\}$ pour $\lambda, \mu \in K^*$ avec $\lambda \neq \mu$.

Définition 2.2. On appelle *automorphismes intérieurs* les éléments de l'image de φ (qui sont bien des automorphismes de groupe).

Le noyau de φ noté $\mathcal{Z}(G)$ est appelé le *centre* de G. C'est l'ensemble des éléments de G qui commutent avec tous les éléments de G.

On note $\mathrm{Int}(G) = \mathrm{im}\,\varphi$ et $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Int}(G)$.

Remarque 2.3.
1. Le sous-groupe $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$ donc $\mathrm{Out}(G)$ est un groupe.
2. Par construction, on a un isomorphisme $\mathrm{Int}(G) \simeq G/\mathcal{Z}(G)$.
3. Cette action est fidèle si, et seulement si, $\mathcal{Z}(G) = 1$. Donc l'action par conjugaison n'est vraiment pas fidèle si G est abélien.
4. Cette action est libre si, et seulement si, $G = 1$.

Définition 2.4. Si X est une partie de G,
- le *centralisateur* de X dans G, noté $\mathcal{Z}_G(H)$, est le stabilisateur point par point de X pour l'action par conjugaison de G sur lui-même.
- le *normalisateur* de X dans G, noté $\mathcal{N}_G(H)$ est le stalibisateur de la partie X.

Fait 2.5.

$$\mathcal{Z}_G(X) = \{g \in G,\ \forall h \in X,\ ghg^{-1} = h\}$$
$$\mathcal{N}_G(X) = \{g \in G,\ gXg^{-1} = X\}$$

Définition 2.6. On dit qu'un sous-groupe H est
- *normal* si $\mathcal{N}_G(H) = G$;
- *central* si $\mathcal{Z}_G(H) = G$.

Fait 2.7. *Le normalisateur de X est le plus grand sous-groupe normal H de G contenant X.*

Proposition 2.8. *Soit H un sous-groupe de G. S'équivalent :*

(i) H est un sous-groupe normal de G, i.e. $\mathcal{N}_G(H) = G$;

(ii) H est stable par tout automorphisme intérieur ;

(iii) Pour tout $g \in G$, on a $gHg^{-1} = H$;

(iv) H est le noyau d'un morphisme de groupes.

Si H vérifie ces conditions, on dit que H est distingué *dans G et on note $H \lhd G$.*

Démonstration. Pour $(iv) \Rightarrow (i) \Rightarrow (ii) \Rightarrow (iii)$, c'est immédiat par définition. Montrons $(iii) \Rightarrow (iv)$. On sait que H agit sur G par multiplication à droite. On considère l'application $f : G \to G/H$ qui à g associe l'orbite gH. D'une part, on observe que G/H est un groupe d'élément neutre H. D'autre part, on observe que f est un morphisme de groupes car $f(g)f(g') = gHg'H = g(Hg')H = g(g'H)H = (gg')H = f(gg')$. Enfin, $\ker f = \{g \in G,\ gH = H\} = H$. □

Fait 2.9. *(1) Tout sous-groupe d'indice 2 est distingué (même si G est infini !).*

(2) Plus généralement, si p est le plus petit nombre premier qui divise l'ordre d'un groupe fini G, alors tout sous-groupe d'indice p de G est distingué.

(2) Si $\varphi : G \to H$ morphisme de groupes et $K \lhd H$, alors $\varphi^{-1}(K) \lhd G$.

Remarque 2.10. Le sous-groupe $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$.

L'image directe d'un sous-groupe distingué n'est pas un sous-groupe distingué en général.ù Par exemple, le morphisme de groupes injectif $j : \mathbb{Z}/2\mathbb{Z} \to \mathfrak{S}_3$ qui envoie $j(1) = (1\ 2)$.

2.2 Quotients de groupes

Définition 2.11. Si H est un sous-groupe distingué de G, alors l'espace quotient G/H est naturellement muni d'une structure de groupe et on a un morphisme naturel de groupes $\pi_H : G \to G/H$ donné par $\pi_H(g) = gH$ de noyau H appelé *morphisme quotient*.

Définition 2.12. Un *morphisme quotient* est la donnée d'un groupe K et d'un morphisme de groupes $p : G \to K$ tel que $\ker p = H$ et pour tout morphisme de groupes $f : G \to G'$ tel que $\ker f \supset H$, il existe un unique morphisme de groupes $\overline{f} : K \to G'$ tel que $\overline{f} \circ p = f$.

Exemple 2.13. Le morphisme $\pi_H : G \to G/H$ précédemment défini est un morphisme quotient, c'est-à-dire qu'il satisfait :

> Pour tout morphisme de groupes $f : G \to G'$ tel que $H \subset \ker f$, il existe un unique morphisme de groupes $\overline{f} : G/H \to G'$ tel que $\overline{f} \circ \pi_H = f$.

Proposition 2.14 (Propriété universelle des quotients)**.** *Soit G un groupe et H un sous-groupe distingué de G. Si $p : G \to K$ et $p' : G \to K'$ sont des morphismes quotients, alors il existe un unique isomorphisme $\varphi : K \to K'$ tel que $p' = \varphi \circ p$.*

Corollaire 2.15. *Si $f : G \to G'$ est un morphisme de groupes, alors $\overline{f} : G/\ker f \to \mathrm{im}(f)$ est un isomorphisme de groupes.*

Démonstration. La méthode est la même que pour les quotients d'espaces vectoriels. □

Théorème 2.16 (Théorème d'isomorphisme)**.** *Si H, K sont deux sous-groupes de G avec $H \lhd G$ alors $H \cap K \lhd K$ et $HK/H \cong K/H \cap K$.*

Démonstration. On considère le morphisme de groupes $\pi_H : G \to G/H$. On a $\mathrm{im}(\pi_H|_K) = KH/H$ et $\ker \pi_H|_K = H \cap K$. Donc $H \cap K$ est distingué dans K comme noyau et $\pi_H|_K$ induit l'isomorphisme $K/K \cap H \cong KH/H$. □

2.3 Sous-groupes caractéristiques

Définition 2.17. On dit qu'un sous-groupe H de G est *caractéristique* s'il est stable par tout automorphisme.

Exemple 2.18. Le centre d'un groupe $\mathcal{Z}(G)$ est un sous-groupe caractéristique.

Fait 2.19. *Un sous-groupe caractéristique est distingué.*

Démonstration. Les automorphismes intérieurs sont des automorphismes. □

Proposition 2.20. *Soient G, H, K des groupes tels que H est distingué (resp. caractéristique) dans G et K est caractéristique dans H. Alors K est un sous-groupe distingué (resp. caractéristique) de G.*

Démonstration. Par hypothèse sur K, on a $\forall \varphi \in \mathrm{Aut}(H),\ \varphi(K) = K$. Soit $\psi \in \mathrm{Int}(G)$ (resp. $\mathrm{Aut}(G)$). Alors $\varphi = \psi|_H \in \mathrm{Aut}(H)$ car H est distingué (resp. caractéristique) dans G. Donc $\varphi(K) = K = \psi(K)$. □

Remarque 2.21. Tout autre énoncé similaire admet un contre-exemple qui peut se trouver dans le groupe $\mathfrak{S}_4$. Le groupe de Klein K formé par les doubles transpositions de $\mathfrak{S}_4$ est un sous-groupe caractéristique de $\mathfrak{S}_4$, abélien et isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$, mais aucun sous-groupe strict non-trivial de K n'est distingué dans $\mathfrak{S}_4$.

Définition 2.22. On appelle sous-groupe dérivé d'un groupe G, noté $\mathcal{D}(G)$, le sous-groupe de G engendré par les commutateurs d'éléments de G.

Fait 2.23. *(1) C'est un sous-groupe caractéristique de G.*
(2) C'est aussi le plus petit sous-groupe distingué de G tel que $G/\mathcal{D}(G)$ est distingué.

Démonstration. (1) Soit $\psi \in \mathrm{Aut}(G)$ et $H = \psi(\mathcal{D}(G))$. Alors pour tous $x, y \in G$, on a $\psi([x, y]) = [\psi(x), \psi(y)] \in \mathcal{D}(G)$. Ainsi $\mathrm{im}(\psi) \subset \mathcal{D}(G)$ car c'est le cas sur une partie génératrice. Comme $\psi(\mathcal{D}(G)) \subset \mathcal{D}(G)$ pour tout $\psi \in \mathrm{Aut}(G)$, on a également $\mathcal{D}(G) = \psi^{-1}(\psi(\mathcal{D}(G))) \subset \psi^{-1}(\mathcal{D}(G))$, d'où l'égalité.

(2) Le groupe $G' = G/\mathcal{D}(G)$ est abélien car pour tout $u, v \in G'$, si x, y sont des représentants de u, v, on a $[u, v] = \pi_{\mathcal{D}(G)}([x, y]) = e$. Soit H un sous-groupe distingué de G tel que G/H est abélien. Soit $\pi_H : G \to G/H$ le morphisme quotient et $x, y \in G$. Alors $\pi_H([x, y]) = [\pi_H(x), \pi_H(y)] = e$ car G/H abélien, donc $[x, y] \in \ker \pi_H = H$. Ainsi, $H \supset \mathcal{D}(G)$ car H contient une partie génératrice de $\mathcal{D}(G)$. □

Définition 2.24. On dit qu'un groupe est *résoluble* s'il existe une suite finie $(G_i)_{0\leqslant i\leqslant n}$ de sous-groupes distingués de G, appelée *suite de résolubilité* telle que :

— $G_0 = G$ et $G_n = 1$;

— pour tout $1 \leqslant i \leqslant n$, $G_i \lhd G_{i-1}$ et G_{i-1}/G_i est abélien.

Si G est un groupe. On appelle *suite dérivée* de G, la suite de sous-groupes de G définie par récurrence par $G_0 = G$ et pour tout $n \geqslant 1$, $G_n = \mathcal{D}(G_{n-1})$.

Proposition 2.25. *Un groupe G est résoluble si, et seulement si, sa suite dérivée est une suite de résolubilité.*

Ceci est laissée en exercice à ceux qui voudront, par exemple, présenter en développement :

Théorème 2.26 (Lie-Kolchin)**.** *Soit G un sous-groupe connexe de $\mathrm{GL}_n(\mathbb{C})$. Alors G est cotrigonalisable si, et seulement si, G est résoluble.*

3 Le cas des p-groupes

3.1 Résultats fondamentaux

Un p-groupe fini P est un groupe d'ordre une puissance de p. Le résultat suivant est fondamental.

Lemme 3.1. *Soit P un p-groupe fini agissant sur un ensemble fini X. Alors $\left|X^G\right| = |X| \mod p$.*
En particulier, si $|X| = 0 \mod p$ alors $X^P \neq \emptyset$.

Démonstration. Pour $x \in X \setminus X^P$, on a $P \cdot x \neq \{x\}$. En particulier $p | |P \cdot x| = [P : \mathrm{Stab}_P(x)]$.
On écrit $X = X^P \sqcup \bigsqcup_{j \in J} P \cdot x_j$. Alors $|X| = \left|X^P\right| + \underbrace{\sum_{j \in J} |G \cdot x_j|}_{\equiv 0 \mod p} \equiv \left|X^P\right| \mod p$. □

Proposition 3.2. *Tout p-groupe fini admet un centre non trivial.*

Démonstration. G agit sur lui-même $X = P$ par conjugaison et $\mathcal{Z}(P) = X^P$. Donc $\mathcal{Z}(P)$ contient un nombre d'éléments divisible par p. □

Le résultat suivant n'est pas immédiat et utilise l'action du groupe cyclique d'ordre p.

Théorème 3.3 (Théorème de Cauchy)**.** *Un groupe fini G d'ordre divisible par p contient un élément d'ordre p.*

Démonstration. Soit $X = \{g \in G, g^p = e\}$ l'ensemble des éléments d'ordre divisant p de G. On fait agir $P = \mathbb{Z}/p\mathbb{Z}$ sur $Y = \{(x_0, \dots, x_{p-1}) \in G^p,\ x_0 \cdots x_{p-1} = e\}$ par permutations cycliques. On observe que X est en bijection avec Y^P via $x \mapsto (x, \dots, x)$. On observe également que Y est en bijection avec G^{p-1} via $(x_0, \dots, x_{p-1}) \mapsto (x_1, \dots, x_{p-1})$. Ainsi $|Y| \equiv 0 \mod p$. Le lemme donne alors $Y^P \neq \{e\}$. Donc il existe un élément non trivial de G d'ordre divisant p : son ordre est donc exactement p. □

On note

$$U_n(K) = \begin{pmatrix} 1 & * & * \\ & \ddots & * \\ 0 & & 1 \end{pmatrix} \subset \mathrm{SL}_n(K)$$

le sous-groupe des matrices triangulaires supérieures strictes de taille n à coefficient dans K. Si $K = \mathbb{F}_{p^m}$ est un corps fini (par exemple $K = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$) où p est un nombre premier, alors $U_n(\mathbb{F}_{p^m})$ est un p-groupe d'ordre $(p^m)^{\frac{n(n-1)}{2}}$. Ce groupe est non-abélien dès que $n \geqslant 3$.

Théorème 3.4 (Théorèmes de Sylow)**.** *Soit G un groupe fini et p un nombre premier divisant l'ordre de G. On écrit $|G| = p^\alpha m$ avec m premier à p. Alors*

1. *G admet des sous-groupes d'ordre p^α, on les appelle* p-sous-groupes de Sylow *ou plus simplement p-Sylow ;*
2. *les p-Sylow sont deux à deux conjugués ;*
3. *si n_p est le nombre de p-Sylow de G, alors $n_p \equiv 1 \mod p$ et $n_p | m$.*

Démonstration. Les théorèmes de Sylow sont à traiter en exercice. □

Voici un autre résultat possible sur les p-groupes :

Proposition 3.5. *Tout p-groupe fini est isomorphe à un sous-groupe de $U_n(\mathbb{F}_p)$ pour un certain $n \in \mathbb{N}$ et, en particulier, est résoluble. De plus, un p-groupe fini admet des sous-groupes distingués de tous les indices possibles.*

3.2 Complément sur les parties génératrices de p-groupes finis

Une bonne référence à ce qui suit se trouve dans le livre de Zavidovique, *Un max de maths*. Attention, cette section n'est pas au programme de l'agrégation mais peut constituer l'objet d'un développement par exemple.

Définition 3.6. Soit G un groupe. Un sous-groupe M de G est dit *maximal* si c'est un sous-groupe strict de G qui est maximal pour l'inclusion.

On appelle sous-groupe de Frattini et on note $\mathrm{Frat}(G)$ l'intersection des sous-groupes maximaux de G.

Lemme 3.7. *Si G est un p-groupe fini, alors tout sous-groupe maximal M de G est distingué et $G/M \simeq \mathbb{Z}/p\mathbb{Z}$.*

Démonstration. G agit sur G/M par translation à gauche et si $N = \mathcal{N}_G(M)$, alors $p|\operatorname{Card}(N/M)$ qui est aussi le cardinal de l'ensemble des points fixes dans G/M sous l'action par translation à gauche de M. Ainsi $|N| > |M|$ et, par maximalité, on a $N = G$. En particulier, M est un sous-groupe normal de G. Comme M est maximal, le groupe quotient G/M n'a pas de sous-groupe propre donc $G/M \simeq \mathbb{Z}/p\mathbb{Z}$. □

Proposition 3.8. *Soit G un groupe fini (pas nécessairement un p-groupe.*

(1) Le sous-groupe de Frattini $\operatorname{Frat}(G)$ *est un sous-groupe distingué de G.*

(2) Une partie $X \subset G$ engendre G si, et seulement si, $X/\operatorname{Frat}(G)$ engendre le groupe quotient $G/\operatorname{Frat}(G)$.

Démonstration. (1) Si M est maximal, alors gMg^{-1} aussi pour tout $g \in G$. Donc l'intersection est encore stable par conjugaison.

(2) Le sens direct est un résultat classique car si $\pi : G \to G/H$ est un morphisme de groupes quotients et X engendre G, alors $\pi(X)$ engendre G/H. Montrons la réciproque par contraposée.

Soit X une partie qui n'engendre pas G et H un sous-groupe maximal de G contenant X. Alors $\operatorname{Frat}(G) \subset H \subsetneq G$. Donc $H/\operatorname{Frat}(G) \subsetneq G/\operatorname{Frat}(G)$ et $X/\operatorname{Frat}(G)$ engendre $H/\operatorname{Frat}(G)$ donc n'engendre pas $G/\operatorname{Frat}(G)$. □

Remarque 3.9. Autrement dit, le sous-groupe de Frattini est l'ensemble des éléments de G qui n'appartiennent à aucune famille minimale de générateurs.

La situation des p-groupes est exceptionnelle en le sens suivant :

Théorème 3.10. *Si G est un p-groupe fini, alors $G/\operatorname{Frat}(G)$ est un $\mathbb{F}_p$-espace vectoriel de dimension finie.*

Démonstration. Lorsque G est un p-groupe fini, on a vu que pour tout sous-groupe maximal M de G, le quotient G/M est un groupe abélien (et même le groupe cyclique d'ordre p). Donc le groupe dérivé $\mathcal{D}(G)$ est un sous-groupe de M. Ainsi $\mathcal{D}(G) \subset \bigcap\{M \text{ maximal}\} = \operatorname{Frat}(G)$, donc $G/\operatorname{Frat}(G)$ est abélien.

De plus, si $x \in G$ et M est un sous-groupe maximal de G, alors $G/M \simeq \mathbb{Z}/p\mathbb{Z}$ donc $x^p \in M$. Donc $x^p \in \bigcap\{M \text{ maximal}\} = \operatorname{Frat}(G)$, ce qui permet de munir $G/\operatorname{Frat}(G)$ de la structure de $\mathbb{F}_p$-espace vectoriel $\overline{n} \cdot \overline{g} = \overline{g}^n$ et $\overline{g} + \overline{h} = \overline{gh}$. □

Remarque 3.11. On a également montré que $\operatorname{Frat}(G) = [G,G]G^p$ est le sous-groupe de G engendré par les commutateurs et les puissances p-èmes d'éléments de G.

Corollaire 3.12. *Dans un p-groupe fini, toute famille minimale de générateurs est de cardinal* $\dim_{\mathbb{F}_p}(G/\operatorname{Frat}(G))$.

Démonstration. Une famille minimale de générateurs d'un $\mathbb{F}_p$-espace vectoriel est une base et, en dimension finie, toutes les bases ont même cardinal. □

Exemple 3.13. Le groupe $T_n(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix},\ * \in \mathbb{F}_p \right\} \subset \mathrm{GL}_n(\mathbb{F}_p)$ des matrices unitriangulaires supérieures sur $\mathbb{F}_p$ est un p-groupe. On a $(T_n(\mathbb{F}_p))^p \subset \mathcal{D}\left(T_n(\mathbb{F}_p)\right) = \left\{ \begin{pmatrix} 1 & 0 & & * \\ & \ddots & \ddots & \\ & & \ddots & 0 \\ 0 & & & 1 \end{pmatrix},\ * \in \mathbb{F}_p \right\}$. D'où $T_n(\mathbb{F}_p)/\operatorname{Frat}(T_n(\mathbb{F}_p)) = T_n(\mathbb{F}_p)/\mathcal{D}(T_n(\mathbb{F}_p)) \simeq \mathbb{F}_p^{n-1}$. Donc $T_n(\mathbb{F}_p)$ est engendré par $n-1$-éléments qui sont les matrices de transvection :

$$\begin{pmatrix} 1 & 1 & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix}.$$

4 Extensions de groupes

Pourquoi s'intéresse-t-on aux quotients de groupes ?

La première raison a déjà été fournie via les questions de dénombrement : on a l'équation au classes, la formule des classes via des quotients de groupes. Ceci étant, on n'a en général pas besoin de quotienter par un sous-groupe distingué pour les questions de comptage.

Une motivation plus convaincante est de ramener une question sur un groupe compliqué en des questions sur des groupes plus simples. Par exemple, on ramène les groupes résolubles à des extensions de groupes résolubles plus petits par des groupes abéliens. Ceci permet de faire des récurrences si on connait des résultats sur les groupes abéliens (on pense par exemple au problème de Galois inverse).

Comme les nombres premiers sont les nombres entiers indivisibles, on dispose d'une notion analogue de groupe non simplifiable.

4.1 Simplicité

Définition 4.1. Un groupe est *simple* s'il n'admet pas de sous-groupe strict distingué non trivial.

Exemple 4.2. On peut montrer que $\mathcal{A}_n$ est simple pour $n \geqslant 5$.

En général, le groupe $\mathrm{SL}_n(K)$ n'est pas simple car son centre est $\mu_n(K)$ qui est en général non trivial. Néanmoins, ce groupe « n'est pas très loin d'être simple ». Plus précisément, il satisfait la définition :

Définition 4.3. Un groupe G est *parfait* si $G = \mathcal{D}(G)$.

On observera en particulier qu'un groupe parfait n'est pas résoluble.

Fait 4.4. *Tout groupe simple est soit parfait, soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

4.2 Extensions de groupes

Définition 4.5. Soit G, H, K des groupes et $g : G \to H$ et $h : H \to K$ deux morphismes de groupes. On dit que la suite $G \to H \to K$ est *exacte* si $\mathrm{im}(g) = \ker(h)$.

Pour dire que g est injectif, on note donc $1 \to G \to H$.

Pour dire que h est surjectif, on note donc $H \to K \to 1$.

Sous ces conditions, on dira alors que $1 \to G \to H \to K \to 1$ est une *suite exacte courte*.

Définition 4.6. Si H et N sont deux groupes, on dit qu'un groupe G est une *extension de H par N* s'il existe une suite exacte courte $1 \to N \to G \to H \to 1$, ce qui signifie qu'on a un morphisme surjectif $G \twoheadrightarrow H$ dont le noyau est isomorphe à N.

On dit qu'une extension $1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$ est *scindée* s'il existe un morphisme de groupes $s : H \to G$ tel que $p \circ s = \mathrm{id}_H$. Le morphisme s est alors appelé une *section*.

Proposition 4.7 (Caractérisation externe des produits semi-directs)**.** *Soit $1 \to N \to G \to H \to 1$ une extension de H par N. Alors G est un produit semi-direct $N \rtimes H$ si, et seulement si, l'extension est scindée.*

Démonstration. Voir TD1 exercice 11 du cours de Géométrie. □

Exercice 1. Montrer que les groupes suivants sont des produits semi-directs et préciser les sections correspondantes :

1. un produit direct de deux groupes $N \times H$;
2. $\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$;
3. $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$;
4. $\mathrm{GL}_n(K) \simeq \mathrm{SL}_n(K) \rtimes K^*$.

4.3 Le problème de la classification

Culturellement, on admet (ou pas) qu'il existe une classification des groupes finis simples. Cette classification repose sur des techniques complexes, utilisant – entre autres – des techniques de théorie des représentations.

On se demande alors s'il est possible de classifier tous les groupes finis ou, ce qui revient au même, de classifier les extensions. Cela signifie qu'étant donnés deux groupes N, H, on se demande quels sont les groupes qui s'insèrent dans une suite exacte courte $1 \to N \to G \to H \to 1$. C'est toujours le cas du produit direct $G = N \times H$ et d'un produit semi-direct $N \rtimes_\varphi H$ pour $\varphi : H \to \mathrm{Aut}(N)$, mais il en existe souvent d'autres. Attention, il existe des extensions de groupes qui ne sont pas des produits semi-directs.

Exemple 4.8. Le groupe $\mathbb{Z}/4\mathbb{Z}$ n'est pas le produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$. Le groupe des quaternions $H = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk = 1\rangle$ ne peut pas s'écrire comme produit semi-direct non-trivial bien qu'il admette également des sous-groupes distingués (e.g. $\{1, i\}$).

Définition 4.9. On dit que deux extensions $1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$ et $1 \to N \xrightarrow{i'} G' \xrightarrow{p'} H \to 1$ sont isomorphes s'il existe un isomorphisme de groupes $\varphi : G \to G'$ tel que $\varphi \circ i = i'$ et $p' \circ \varphi = p$.

Remarque 4.10. Attention, il existe des extension qui ne sont pas isomorphes mais telles que les groupes obtenus G et G' sont malgré tout isomorphes.

Proposition 4.11. *Soit N et H deux groupes. Les extensions scindées de H par N sont en bijection avec les morphismes de groupes $H \to \mathrm{Aut}(N)$.*

Démonstration. Si $\varphi : H \to \mathrm{Aut}(N)$ est un morphisme de groupes, alors on sait construire le produit semi-direct $G_\varphi = N \rtimes_\varphi H$. On dispose alors d'une suite exacte $1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$ où $i : n \in N \mapsto (n, 1) \in G$ et $p : (n, h) \mapsto h$ scindée par la section $s : h \in H \to (1, h)$. On vérifie que s est bien un morphisme de groupes car $s(h)s(h') = (1, h)(1, h') = (1 \cdot \varphi(h)(1), hh') = (1, hh') = s(hh')$.

Réciproquement, si $1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$ est une suite exacte scindée par une section $s : H \to G$, alors on définit un morphisme de groupes $\psi : H \to \mathrm{Int}(G)$ par $\psi(h) = \mathrm{Int}(s(h))$. Pour alléger les notations, on identifie par abus N et $i(N)$. Comme $N \triangleleft G$, on observe que $\psi(h)(N) = N$ donc $\psi(h)$ induit un automorphisme de groupes $\psi(h) \in \mathrm{Aut}(N)$ et on peut définir le produit semi-direct $G' = N \rtimes_\psi H$. On définit alors $\varphi : G' \to G$ par $\varphi(n, h) = i(n)s(h)$. On vérifie que c'est un isomorphisme de groupes qui induit un isomorphisme d'extensions (exo). □

Ainsi, les produits semi-directs sont classifiés par $\mathrm{Hom}_{\mathrm{gr}}(H, \mathrm{Aut}(N))$. En particulier, on rappelle que $\mathrm{Aut}(N)$ est une extension de $\mathrm{Int}(N) \simeq N/\mathcal{Z}(N)$ par $\mathrm{Out}(N)$, ce qui peut parfois aider.

Pour ceux qui souhaitent présenter en développement le fait que tout automorphisme de $\mathfrak{S}_n$ pour $n \neq 6$ est intérieur, demandez-vous quels sont les morphismes possibles d'un groupe dans $\mathfrak{S}_n$ et pourquoi ça ne marche pas pour $n = 6$.

Une autre situation dans laquelle on sait dire des choses est l'étude des extensions centrales, c'est-à-dire $1 \to A \xrightarrow{i} G \xrightarrow{p} H \to 1$ où $i(A) \subset \mathcal{Z}(G)$. Il y a alors des résultats de classification en termes de cohomologie des groupes mais on n'en dira pas plus.

4.4 Présentation de groupes

Comme pour les parties génératrices d'un groupe qui permettent de simplifier un problème de groupes, l'idée des présentations de groupes par générateurs et relations est de proposer une forme plus simple.

Si on dispose d'une famille, disons finie pour simplifier, de générateurs $S = \{s_i\}_{i \in I}$ d'un groupe G, alors on va réaliser G comme quotient d'un groupe « universel », appelé groupe libre engendré par n éléments $F_S \twoheadrightarrow G$. Alors $R = \ker F_S \twoheadrightarrow G$ est un sous-groupe distingué de F_S. Une famille de relations en les $\{s_i\}_{i \in I}$ est une famille $\{r_j\}_{j \in J}$ de F_S telle que le plus petit sous-groupe distingué de F_S contenant les r_j est égal à R. On dit alors que G est présenté par les générateurs $\{s_i\}_{i \in I}$ et les relations $\{r_j\}_{j \in J}$ et on note alors $G = \langle \{s_i\}_{i \in I} \mid \{r_j\}_{j \in J}\rangle$. Voici les exemples pour les groupes finis usuels.

Exemple 4.12.
- $\mathbb{Z}/n\mathbb{Z} = \langle x \mid x^n\rangle$ est la présentation donnée par n'importe quel générateur $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- $D_n = \langle s, t \mid s^2, t^2, (st)^n\rangle$ est la présentation donnée par deux réflexions « voisines ».
- $\mathfrak{S}_n = \langle t_1, \dots, t_{n-1} \mid (t_i)^2, (t_i t_{i+1})^3, (t_i t_j)^2 \text{ pour } |i - j| \geqslant 2\rangle$ est la présentation donnée par les générateurs $t_i = (i\ i+1)$.
- $\mathfrak{S}_n = \langle t, c \mid t^2, c^n, (ct)^{n-1}, ([c, t])^3, [c, t^j]^2 \text{ pour } 2 \leqslant j \leqslant n-2\rangle$ est la présentation donnée par les générateurs $t = (1\ 2)$ et $c = (1\ \dots\ n)$.

5 Résultats à connaître sur les groupes usuels finis

Groupes monogènes et cycliques ; groupes abéliens de type fini

- Groupe monogène : groupe engendré par 1 élément, est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$.
- Groupe cyclique d'ordre n, noté C_n : groupe monogène fini, isomorphe au groupe $\mathbb{Z}/n\mathbb{Z}$.
- Sous-groupes de $\mathbb{Z}$ ou de $\mathbb{Z}/n\mathbb{Z}$: ce sont les $d\mathbb{Z}/n\mathbb{Z}$ où $d|n$ avec par convention $n = 0$ pour $\mathbb{Z}$.
- Si $x, y \in G$ abélien sont d'ordres m et n, il existe un élément dans $\langle x, y\rangle$ d'ordre $\text{ppcm}(m, n)$.
- Structure des groupes abéliens finis et de type fini.
- Le groupe dual de $(\mathbb{Z}/n\mathbb{Z})$ est canoniquement isomorphe à $(\mathbb{Z}/n\mathbb{Z})$.
- Le groupe dual d'un groupe abélien est isomorphe à lui-même, son bidual canoniquement isomorphe.
- Générateurs de $(\mathbb{Z}/n\mathbb{Z})$: les classes $k + n\mathbb{Z}$ pour $k \wedge n = 1$, i.e. les inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
- Les automorphismes de $(\mathbb{Z}/n\mathbb{Z})$ sont les $x \mapsto ax$ avec $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Le groupe des racines de l'unité On note $\mathbb{U}$ le groupe des nombres complexes de module 1.

Si K est un corps et $n \in \mathbb{N}^*$, on note $\mu_n(K)$ le sous-groupe de K^* formé des racines du polynôme $X^n - 1$. En particulier, $\mu_n(\mathbb{C})$ est un sous-groupe de $\mathbb{U}$.

- Tout sous-groupe fini de K^* est cyclique. En particulier, $\mu_n(K)$ est cyclique d'ordre divisant n.
- Le groupe $\mathbb{U}$ est connexe, compact, abélien, isomorphe à $\mathrm{SO}_2(\mathbb{R})$.
- Tout sous-groupe discret de $\mathbb{U}$ est isomorphe à un $\mu_n(\mathbb{C})$.
- L'application $\mathbb{R} \to \mathbb{U}$ définie par $x \mapsto e^{ix}$ est un morphisme de groupes surjectif, de noyau $2\pi\mathbb{Z}$.
- Il faut savoir décrire la structure de $\mathrm{SO}_2(\mathbb{R})$ comme groupe de rotations. Ce groupe permet de définir les angles orientés (cf. cours de Géométrie).

Groupe de permutations

- Conjugaison d'une permutation écrite comme produit de cycles à supports disjoints
- Savoir décrire les classes de conjugaison de $\mathfrak{S}_n$.
- La signature est l'unique morphisme non trivial de $\mathfrak{S}_n$ dans $\{\pm 1\}$ (et même $\mathbb{C}^*$).
- Les k-cycles avec $k \leq n - 2$ sont conjugués dans $\mathfrak{A}_n$.
- Familles de générateurs classiques de $\mathfrak{S}_n$: les transpositions, $\{(i\ i+1), i \in \{1, \cdots, n-1\}\}$, et $\{(1\,2), (1\ \cdots\ n)\}$. Il faut au minimum $n - 1$ transpositions pour engendrer $\mathfrak{S}_n$ donc la deuxième famille est minimale.
- Le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles pour $n \geq 3$.
- $(*)$ Tous les automorphismes de $\mathfrak{S}_n$ sont intérieurs sauf pour $n = 6$.
- Simplicité de $\mathfrak{A}_n$ pour $n \geq 5$, groupe de Klein pour $n = 4$.
- Le groupe $\mathfrak{A}_n$ est le groupe dérivé de $\mathfrak{S}_n$ pour tout n, et de lui-même pour $n \geq 5$.

Groupe diédral

- Isométries d'un polygone régulier ; action transitive sur les paires de points liés par une arête.
- Engendré par deux réflexions consécutives.
- Facilement présenté par générateurs et relations.
- Produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/n\mathbb{Z}$.