UN PEU D'HISTOIRE DES GROUPES FINIS ET QUELQUES EXEMPLES SIMPLES

par

Anne-Marie Aubert

1. Introduction

Un angle d'approche de la théorie des groupes finis est fournie par l'analogie entre cette théorie et la théorie des nombres élémentaire. Afin d'illustrer cette analogie, considérons la division des entiers naturels. On dit qu'un entier naturel m divise un entier naturel n s'il existe un entier naturel q tel que $n = mq$. On dit alors que q est le quotient de n par m. Les entiers naturels les plus simples de ce point de vue sont les nombres $p \neq 1$ dont les seuls diviseurs sont 1 et p lui-même : on les appelle les nombres premiers. Un fait central est le résultat suivant : tout entier naturel $n \neq 1$ s'écrit $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ pour des nombres premiers distincts $p_1, p_2, \ldots, p_k$ et des entiers naturels $e_1, e_2, \ldots, e_k$, où chaque couple (p_i, e_i) est uniquement déterminé à permutation des indices près. Afin de mieux montrer l'analogie en vue, nous énonçons ce fait sous la forme équivalente suivante : pour tout entier naturel $n \neq 1$ il existe une suite $n = n_0 \geqslant n_1 \geqslant n_2 \geqslant \cdots \geqslant n_{r-1} \geqslant n_r = 1$ telle que chaque n_i/n_{i+1} est premier, et la suite de nombres premiers ainsi obtenue et ses multiplicités sont uniquement déterminée par n à l'ordre près. Il n'y a clairement pas unicité des entiers n_i eux-mêmes. Ce résultat est fondamental car il montre que les nombres premiers ne sont pas seulement simples du point de vue de la divisibilité mais qu'ils sont aussi les blocs fondamentaux permettant d'obtenir tout entier naturel par multiplications de nombres premiers.

Quelle est l'analogie avec la théorie des groupes finis ? L'analogue de la divisibilité est constitué par la notion de « distinction » : si H est un sous-groupe d'un groupe fini G, le quotient G/H de G par H est formé des classes à gauche de H dans G. Celles-ci sont précisément les classes d'équivalence pour la relation de congruence modulo H, définie par $g \equiv g' \pmod{H}$ si

$g^{-1}g' \in H$. Le quotient G/H est un groupe pour loi de multiplication des classes $gHg'H = gg'H$ si et seulement si H est *distingué* (ou *normal*) dans G, *i.e.*, si $gH = Hg$ pour tout élément de g de G.

Exemple. Prenons pour G le groupe symétrique $\mathfrak{S}_n$ des permutations d'un ensemble à n éléments et pour H l'ensemble $\mathfrak{A}_n$ des permutations paires qui est un sous-groupe normal de G tel que $G/H \simeq Z_2$, le groupe cyclique à 2 éléments.

Quel est, dans ce contexte, l'analogue d'un nombre premier ? Un groupe G dont les seuls sous-groupes distingués sont $\{1\}$ et G lui-même (où 1 désigne l'élément neutre de G). Un tel groupe G est appelé un groupe *simple*.

Quel est l'analogue du résultat arithmétique énoncé ci-dessus ? Nous devons ici nous restreindre aux groupes finis, le théorème suivant n'étant pas vrai pour un groupe infini arbitraire. Traduisant le résultat sous la seconde forme évoquée ci-dessus, nous obtenons le *théorème de Jordan-Hölder*[(1)] *pour les groupes finis* : étant donné un groupe fini G, il existe une suite

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{r-2} \supset G_{r-1} \supset G_r = \{1\}$$

de sous-groupes G_i de G telle que le sous-groupe G_{i+1} est distingué dans G_i et G_i/G_{i+1} est un groupe simple pour tout $i \in \{0, 1, \ldots, r\}$ et la famille de groupes simples ainsi obtenue est unique à permutation près. Une telle suite est appelée une *suite de composition* de G.

Cette analogie présente toutefois quelques imperfections : par exemple, chacun des n_i divise n, alors que G_i n'est pas nécessairement distingué dans G, et l'on peut se demander si les groupes simples constituent les « blocs fondamentaux » des groupes finis.

Supposons que nous connaissions tous les groupes finis simples. Comment pourrions nous alors déterminer tous les groupes finis ? Tout d'abord, nous aimerions écrire une liste $S_1, S_2, \ldots, S_r$ de facteurs de composition simples. Nous essayerions alors de dresser une liste de tous les groupes G_i possibles tels que $G_i/G_{i+1} \simeq S_{i+1}$. La première étape est facile : puisque $G_r = \{1\}$, nous obtenons $G_{r-1} = G_{r-1}/G_r = S_r$. La deuxième étape consisterait à à déterminer, connaissant $G_{r-2}/G_{r-1} \simeq S_{r-1}$ et G_{r-1}, les possibilités pour G_{r-2}.

(1) Otto Ludwig Hölder s'est intéressé à la théorie des groupes à cause des travaux de Kronecker et de Klein. Il démontra l'unicité à permutation près des facteurs de composition dans une suite de composition d'un groupe fini. En 1892, en utilisant les théorèmes de Sylow, il montra que tous les groupes finis simples d'ordre inférieur à 200 étaient connus. Il étudia aussi les groupes d'ordre p^3, pq^2, pqr et p^4 pour p, q, r premiers. Il introduisit les notions d'automorphisme intérieur et extérieur, et écrivit en 1895 un long article sur les extensions de groupes.

C'est un exemple du *problème d'extension de Hölder*, qui peut s'énoncer sous la forme générale suivante : étant donnés deux groupes K et Q, déterminer tous les groupes G possibles tels que K est distingué dans G et $G/K \simeq Q$. De tels groupes G sont appelés des *extensions* de K par Q. Remarquons que si un groupe simple G est une extension de K par Q, alors $G \simeq K$ ou bien $G \simeq Q$. Le groupe n'est pas uniquement déterminé par la donnée de K et de Q : par exemple, les groupes $\mathfrak{S}_3$ et Z_6 (le groupe cyclique d'ordre 6) sont tous deux extensions de Z_3 par Z_2. La question est : toutes les extensions possibles G peuvent-elles être construites de manière systématique ? La réponse est oui, bien que peu économique. Schreier, dans les années vingt, a développé une technique pour construire toutes les tables de multiplication pour G, mais jusqu'à présent, à ma connaissance, il n'existe pas de méthode générale permettant d'identifier quelles tables de multiplication sont celles de groupes isomorphes (voir [**R**, chap. 7] ou [**Sco**, chap. 9] pour plus de détails). La liste des tables de multiplication possibles comprendrait donc des répétitions inutiles, néanmoins toutes les extensions G de K par Q peuvent être construites.

Maintenant que nous avons vu comment déterminer tous les groupes possibles G_{r-2}, nous pouvons continuer d'appliquer la méthode de Schreier afin de construire toutes les possibilités pour les groupes G_{r-3}, G_{r-4},... Les groupes finis simples apparaissent donc comme les blocs fondamentaux de la théorie des groupes finis.

2. Les groupes finis simples

Un exercice facile consiste à prouver que les groupes cycliques Z_p d'ordre premier p sont simples. Ce sont les seuls groupes finis simple abéliens. Évariste Galois avait essentiellement montré que les groupes alternés $\mathfrak{A}_n$, pour $n \geqslant 5$, constituent une famille infinie de groupes finis simples non abéliens (pour une preuve élémentaire de la simplicité on pourra se référer, par exemple, à [**Jac1**, Vol. I, p. 139]).

Les familles infinies suivantes de groupes finis simples furent découvertes parmi les *groupes classiques*, terminologie introduite par Hermann Weyl dans son livre [**Wey**], publié en 1939. Ce sont les groupes de matrices qui furent introduits pour la première fois par Camille Jordan [**Jo**] et dont la structure fut étudiée de manière intensive par Leonard Dickson [**Dic1, Dic2**]. Dickson fut élève de Eliakim Moore à Chicago [**Par1**]. Son livre [**Dic1**] constitue non seulement la première étude systématique des groupes linéaires classiques mais il contient un travail profond et original sur ces groupes et les familles de groupes simples (pour une biographie de Dickson, voir [**Par2**]). Cependant ses méthodes étaient pour la plupart *ad hoc* et très calculatoires. Une approche plus

élégante et plus lisible fut obtenue plusieurs années après grâce aux travaux d'Emil Artin [**Art1, Art2, Art3**], Jean Dieudonné [**Dieu**], Bertram Huppert [**Hu**, chap. 2] et Nathan Jacobson [**Jac2**].

La première famille de groupes classiques est la famille des *groupes linéaires généraux* $\mathrm{GL}(V)$ formés des automorphismes (*i.e.*, des transformations linéaires inversibles) d'un espace vectoriel V sur un corps commutatif k. Le groupe $\mathrm{GL}(V)$ est isomorphe au groupe $\mathrm{GL}_N(k)$ des matrices carrées d'ordre N inversibles à coefficients dans le corps k, où N est la dimension de V sur k. Les *groupes spéciaux linéaires* $\mathrm{SL}(V)$ (resp. $\mathrm{SL}_N(k)$) formés des automorphismes de V (resp. matrices matrices carrées d'ordre N à coefficient dans k) de déterminant égal à 1. Le groupe $\mathrm{SL}_N(k)$ est égal au groupe des commutateurs[(2)] de $\mathrm{GL}_N(k)$, excepté dans le cas $N = 2$ et $k = \mathbb{F}_2$ (le corps à deux éléments).

Les autres groupes classiques sont les groupes d'automorphismes de formes non dégénérées sur V (espace vectoriel sur un corps commutatif k). Une *forme* sur V est une application $f\colon V \times V \to k$ telle que $f(v_1 + v_2, v') = f(v_1, v') + f(v_2, v')$ et $f(v, v'_1 + v'_2) = f(v, v'_1) + f(v, v'_2)$ pour tous v, v_1, v_2, v', v'_1, v'_2 dans V. La forme f est *non dégénérée* si ses noyaux gauche et droit

$$\big\{v \in V \mid f(v, v') = 0 \ \text{ pour tout } v' \in V\big\},$$
$$\big\{v' \in V \mid f(v, v') = 0 \ \text{ pour tout } v \in V\big\}$$

sont tous deux réduits à $\{0\}$. Le *groupe d'automorphismes* de la forme f est l'ensemble des automorphismes u de V qui préservent f au sens suivant : $f(uv, uv') = f(v, v')$ pour tout $(v, v') \in V \times V$.

Une forme F est *bilinéaire symétrique* si $f(v, v') = f(v', v)$ et $f(\lambda v, v') = \lambda f(v, v')$ pour tout $(v, v') \in V \times V$ et tout $\lambda \in k$. Le groupe d'automorphismes d'une telle forme est appelé un *groupe orthogonal* et sera noté $\mathrm{O}_N(k, f)$. Une forme f est *bilinéaire antisymétrique* si $f(v', v) = -f(v, v')$ et $f(\lambda v, v') = \lambda f(v, v')$ pour tout $(v, v') \in V \times V$ et tout $\lambda \in k$. Le groupe d'automorphismes d'une telle forme est appelé un *groupe symplectique* et sera noté $\mathrm{Sp}_N(k, f)$.

Si la caractéristique du corps k est égale à 2, les définitions ci-dessus des groupes orthogonaux et symplectiques coïncident. Les groupes usuellement appelés groupes orthogonaux doivent préserver une forme quadratique en sus de la forme bilinéaire symétrique. C'est pourquoi certains des énoncés ci-après concernant les groupes orthogonaux doivent être raffinés lorsque la caractéristique de k est 2 (pour plus de détails, on pourra se référer à [**Che1**, chap. 1]).

(2) Le *groupe des commutateurs* $G' = [G, G]$ d'un groupe G est le sous-groupe de G engendré par les *commutateurs* $g_1 g_2 g_1^{-1} g_2^{-1}$ avec g_1, g_2 éléments de G. Si N est un sous-groupe distingué de G, le groupe quotient G/N est abélien si et seulement si N contient G'.

Les autres formes qui nous intéressent ici sont les formes sesquilinéaires hermitiennes. Ici k est une extension quadratique séparable d'un corps k_0 telle qu'il existe un automorphisme $\lambda \mapsto \overline{\lambda}$ de k sur k_0 d'ordre 2. Une forme f est *sesquilinéaire hermitienne* si $f(v', v) = \overline{f(v, v')}$ et $f(\lambda v, v') = \lambda f(v, v')$ pour tout $(v, v') \in V \times V$ et tout $\lambda \in k$. Le groupe d'automorphismes d'une telle forme est appelé un *groupe unitaire* et sera noté $\mathrm{U}_N(k, f)$.

Les groupes classiques restant (*i.e.*, autres que $\mathrm{GL}_n(k)$ et $\mathrm{SL}_n(k)$) sont les groupes d'automorphismes de formes non dégénérées de l'un des trois types ci-dessus.

Les formes antisymétriques sont non dégénérées seulement si N est pair [**Art1**]. Nous poserons alors $m := N/2$. D'autre part, deux formes non dégénérées antisymétriques sur V définissent des groupes symplectiques isomorphes. Nous écrirons donc simplement $\mathrm{Sp}_{2m}(k)$ pour $\mathrm{Sp}_{2m}(k, f)$. Les éléments de $\mathrm{Sp}_{2m}(k)$ ont leur déterminant égal à 1 et $\mathrm{Sp}_{2m}(k)$ coïncide avec son groupe des commutateurs, excepté lorsque $m = 1$ et k a deux ou trois éléments, et lorsque $m = 2$ et k a deux éléments. Lorsque k est fini, deux formes bilinéaires symétriques non dégénérées sur V définissent des groupes orthogonaux isomorphes lorsque N est impair (nous écrirons alors simplement $\mathrm{O}_N(k)$ pour $\mathrm{O}_N(k, f)$), et il y a exactement deux classes d'isomorphismes de groupes orthogonaux si N est pair, elles correspondent au cas où l'indice de Witt de la forme f est maximal ou non [**Art1**]. Nous écrirons $\mathrm{O}_N^+(k)$ et $\mathrm{O}_N^-(k)$ pour $\mathrm{O}_N(k, f)$ respectivement dans le premier et le second cas. Le groupe des commutateurs de $\mathrm{O}_N(k, f)$, noté $\Omega_N(k, f)$, est en général un sous-groupe propre du groupe de rotations $\mathrm{SO}_N(k, f)$ formé des éléments de $\mathrm{O}_N(k, f)$ de déterminant égal à 1. Toujours sous l'hypothèse k fini, deux formes sesquilinéaires hermitiennes non dégénérées sur V définissent des groupes unitaires isomorphes, et nous écrirons $\mathrm{U}_N(k)$ pour $\mathrm{U}_N(k, f)$. Lorsque $N \geqslant 3$, excepté le cas $N = 3$ et $|k| = 4$, le groupe des commutateurs de $\mathrm{U}_N(k)$ coïncide avec le sous-groupes $\mathrm{SU}_N(k)$ des éléments de $\mathrm{U}_N(k)$ de déterminant égal à 1. Lorsque $N = 2$, le groupe $\mathrm{SU}_2(k)$ est isomorphe au groupe $\mathrm{SL}_2(k)$.

Il existe une procédure uniforme permettant d'associer un groupe simple à un groupe classique G arbitraire. On considère le groupe des commutateurs G' de G et l'on forme le groupe quotient $G'/\mathrm{Z}(G')$ de G' par son centre $\mathrm{Z}(G')$. Le groupe $\mathrm{Z}(G')$ est formé de multiples scalaires de l'identité et n'est pas un groupe compliqué. Lorsque k est fini, $\mathrm{Z}(G')$ est un sous-groupe du groupe multiplicatif (cyclique) de k. La plupart du temps, $G'/\mathrm{Z}(G')$ est un groupe simple [**Art1**], [**Dieu**]. Il y a quelques exceptions en petites dimensions et sur de petits corps, et d'autres exceptions dans le cas unitaire lorsque la forme f

est anisotrope[3]. L'on obtient ainsi six familles de groupes dont les membres sont le plus souvent simples :

$$\begin{aligned} \mathrm{PSL}_n(k) &:= \mathrm{SL}_n(k)/\text{ Centre}, \\ \mathrm{PSp}_{2m}(k) &:= \mathrm{Sp}_{2m}(k)/\text{ Centre}, \\ \mathrm{PSU}_n(K) &:= \mathrm{SU}_n(K)/\text{ Centre}, \end{aligned}$$

et trois familles de groupes orthogonaux

$$\Omega_{2m+1}(k)/\text{ Centre}, \quad \Omega^+_{2m}(k)/\text{ Centre} \quad \text{et} \quad \Omega^-_{2m}(k)/\text{ Centre}.$$

Lorsque k est fini, malgré quelques cas d'isomorphismes entre des groupes appartenant à des familles différentes, on obtient six familles doublement infinies.

Dickson découvrit aussi des familles de groupes simples associés aux algèbres de Lie simples de type G_2 et E_6 sur le corps $\mathbb{C}$ des nombres complexes dans trois articles **[Dic3]**, **[Dic4]**, **[Dic5]**.

Jusqu'en 1955, on ne découvrit pas d'autre groupe fini simple excepté cinq groupes apparemment isolés qui avaient été découverts par Émile Mathieu en 1861 et 1873 **[Ma1]**, **[Ma2]**. Avant de décrire les groupes de Mathieu, il est nécessaire d'introduire quelques éléments de terminologie des groupes de permutations. Une *représentation de permutation* d'un groupe fini G est un homomorphisme $\rho\colon G \to \mathfrak{S}(X)$ de G dans le groupe symétrique $\mathfrak{S}(X)$ des permutations d'un ensemble X. La représentation ρ est *fidèle* si son noyau est réduit à $\{1\}$, où 1 désigne l'élément neutre de G. L'image d'une représentation de permutation, ou sous-groupe quelconque de $\mathfrak{S}(X)$, est un *groupe de permutations* sur l'ensemble X. Si H est un groupe de permutation sur X, et x un élément de X, le *stabilisateur* H_x de x est l'ensemble $\{h \in H \mid hx = x\}$. Il est facile de vérifier que H_x est un sous-groupe de H. Étant donné un groupe de permutation H sur X, on définit une relation d'équivalence $\sim$ sur X par $x \sim x'$ s'il existe $h \in H$ tel que $x' = hx$. Les classes d'équivalence de $\sim$ sont les *orbites* de H sur X ou simplement les H–orbites. Si X est lui-même une H–orbite, on dit que H est un *groupe de permutations transitif*. Si x et x' appartiennent à une même H–orbite, leurs stabilisateurs H_x et $H_{x'}$ sont des sous-groupes conjugués de H. En particulier, tous les stabilisateurs sont conjugués lorsque H est un groupe de permutations transitif sur X. Un groupe de permutation G sur un ensemble X est dit *m–transitif* si tout m–uplet d'éléments distincts de X peut être envoyé sur n'importe quel m–uplet d'éléments distincts de X par une permutation appartenant à G. Un groupe est 1-transitif si et seulement s'il est transitif.

[3] Une forme f est *anisotrope* si $f(v, v) \neq 0$ pour tout $v \neq 0$ dans V.

Exemples. Le groupe symétrique $\mathfrak{S}_n$ des permutations d'un ensemble à n éléments est m–transitif pour tout entier $m \leqslant n$. Le groupe alterné $\mathfrak{A}_n$ est m–transitif pour tout entier $m \leqslant n-2$. Les groupes symétriques $\mathfrak{S}_n$ (pour $n \geqslant 6$) et les groupes alternés $\mathfrak{A}_n$ (pour $n \geqslant 8$) sont les seuls groupes de permutations connus qui sont m–transitifs pour tout entier entier $m \geqslant 6$. Par ailleurs, il existe une infinité d'exemples de groupes de permutations 2–transitifs ou même 3–transitifs autres que les groupes symétriques et alternés. Les groupes d'automorphismes des géométries projectives sur les corps finis sont toujours 2–transitifs sur les points et, dans le cas des droites projectives, ils sont même 3–transitifs sur les points [**Carm**, chap. 12].

À côté des groupes symétriques et alternés, il y a seulement quatre groupes de permutations connus qui sont 4–transitifs ou 5–transitifs sur un ensemble fini. Ce sont les *groupes de Mathieu* découverts par Mathieu en 1861 et 1873. Le groupe de Mathieu M_{12} est un groupe d'ordre $95040 = 2^6 3^3 5 \cdot 11$ qui est 5–transitif sur un ensemble de cardinal 12. Le groupe de Mathieu M_{24} est un groupe d'ordre $244\,823\,040 = 2^{10} 3^3 5 \cdot 7 \cdot 11 \cdot 23$ qui est 5–transitif sur un ensemble de cardinal 24. Le stabilisateur d'un point quelconque dans M_{12} (resp. M_{24}) est le groupe de Mathieu M_{11} (resp. M_{23}) : c'est un groupe d'ordre $7920 = 2^4 3^2 5 \cdot 11$ (resp. $10\,200\,960 = 2^7 3^2 5 \cdot 7 \cdot 11 \cdot 23$) qui est 4–transitif sur un ensemble de cardinal 11 (resp. 23). Le stabilisateur d'un point quelconque dans M_{23} est le groupe de Mathieu M_{22} : c'est un groupe d'ordre $443\,520 = 2^7 3^2 5 \cdot 7 \cdot 11$. Les cinq groupes de Mathieu M_{11}, M_{12}, M_{22}, M_{23} et M_{24} sont simples et ne sont isomorphes ni à un groupe alterné ni à un groupe fini de type de Lie. Puisqu'ils ne figurent dans aucune famille infinie de groupes simples, William Burnside [**Wag**], dans son livre [**Bur**, Note N. page 504], les appela *groupes simples sporadiques* et le terme *sporadique* est maintenant utilisé pour tout groupe fini simple qui n'appartient à aucune famille infinie de groupes simples.

Dans son célèbre article [**Che2**], Claude Chevalley développa une procédure de construction de familles infinies de groupes simples (appelés *groupes de Chevalley*) associés aux diverses *algèbres de Lie simples*[(4)] complexes de dimension finie. La classification des algèbres de Lie simples complexes de dimension finie, commencée par Wilhelm Killing, fut complétée en 1894 par Elie Cartan. Les groupes classiques sur $k = \mathbb{C}$ sont des *groupes de Lie* et leurs sous-groupes simples correspondent canoniquement aux algèbres de Lie simples complexes. Il y a donc plus qu'une analogie entre groupes simples et algèbres de

[(4)] Une *algèbre de Lie* complexe L est une algèbre (un espace vectoriel muni d'un produit bilinéaire noté $[\ ,\ ]$) telle que les identités $[x,x] = 0$ et $[[x,y],z] + [[y,z],x] + [[z,x],y] = 0$ sont satisfaites. Un idéal I de L est sous-espace vectoriel tel que $[x, I] \subset I$ pour tout $x \in L$. Une algèbre de Lie L est *simple* si $[L,L] \neq 0$ et si les seuls idéaux de L sont $\{0\}$ et L.

Lie simples. Chevalley a montré que les familles infinies de groupes finis simples associées aux algèbres de Lie simples de type F_4, E_7 et E_8 étaient nouvelles. Des variations sur la méthode de Chevalley permirent à Robert Steinberg et Jacques Tits de construire de nouvelles familles infinies de groupes simples. Enfin Rimhak Ree montra qu'une famille construite de manière différente par Michio Suzuki [**ABFS**] dans [**Su**] pouvait s'interpréter à l'aide d'un automorphisme du diagramme d'une algèbre de Lie de type B_2, et construisit des groupes analogues dans les cas G_2 et F_4, voir [**Car**].

3. Groupes extra-spéciaux, groupes de Heisenberg, groupe métaplectique

Préliminaires

Groupe de Frattini [**Em**]. Soit G un groupe fini. Nous notons $\mathrm{Z}(G)$ et G' respectivement son centre et son groupe dérivé.

Définition 3.1. *Le* groupe de Frattini *d'un groupe fini G, noté $\Phi(G)$, est l'intersection des sous-groupes propres maximaux de G.*

Proposition 3.2. *Soient p un nombre premier et P un p–groupe fini (*i.e., *un groupe fini dont le cardinal est une puissance de p).*

(a) *Le groupe de Frattini de P est le plus petit des sous-groupes distingués H de P tels que le groupe quotient P/H soit abélien élémentaire.*

(b) *Le groupe $P/\Phi(P)$ a une structure naturelle d'espace vectoriel sur le corps $\mathbb{F}_p$ à p éléments. Cet espace vectoriel est appelé l'*espace de Frattini *de P. La dimension de l'espace de Frattini est le nombre minimum de générateurs de P.*

(c) *Si P est d'exposant p, on a $\Phi(P) = P'$.*

Remarque. Si G est un groupe fini, alors G' est le plus petit des sous-groupes distingués H de G tels que G/H est abélien. Si P est un p–groupe, on a donc $P' \subset \Phi(P)$.

Un résultat sur les groupes de classe 2

Proposition 3.3. *Soit G un groupe de classe* 2, *(*i.e., *tel que $G' \subset \mathrm{Z}(G)$). Alors :*

(a) *pour tout élément g de G, l'application $x \mapsto [g, x]$ est un morphisme de groupes de G dans G' ;*

(b) *pour tout entier $k \geqslant 1$, et tout couple (g_1, g_2) d'éléments de G, on a*

$$(g_1 g_2)^k = [g_2, g_1]^{\Sigma(k)}\, g_1^k\, g_2^k, \quad \textit{avec } \Sigma(k) := 1 + 2 + \cdots + (k-1).$$

Définition et exemples de groupes extra-spéciaux généralisés

Proposition 3.4

(a) *Le centre d'un p–groupe est non trivial.*

(b) *Tout groupe fini G qui possède un sous-groupe Z central (*i.e., *contenu dans $\mathrm{Z}(G)$) et tel que le quotient G/Z est cyclique, est abélien.*

Définition 3.5. *Un p–groupe est dit* extra-spécial généralisé *(resp.* extra-spécial*) s'il possède un sous-groupe Z d'ordre p tel que $\Phi(E) \subset Z \subset \mathrm{Z}(E)$ (resp. si $\Phi(E)$ est d'ordre p et égal à $\mathrm{Z}(E)$).*

Proposition 3.6. *Tout p-groupe extra-spécial généralisé E est de l'un des types suivants :*

(a) *si E est abélien, il est*
- *abélien élémentaire (de type $(p, \ldots, p)$),*
- *ou du type $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}$;*

(b) *si E est non abélien, alors son groupe de Frattini est central d'ordre p (et dans ce cas $Z = E' = \Phi(E)$).*

En particulier, tout p–groupe extra-spécial généralisé non abélien est de classe 2.

Remarque. Soit E un groupe d'ordre p^3 non abélien. Le centre $\mathrm{Z}(E)$ de E n'est pas trivial, et n'est pas d'indice p, donc est d'ordre p. Le quotient $E/\mathrm{Z}(E)$ n'est pas cyclique, donc est un groupe de type (p, p). Donc, $\mathrm{Z}(E)$ contient $\Phi(E)$. Comme ce dernier groupe n'est pas trivial, (sinon, E serait de type (p, p, p)), on voit que $\Phi(E) = \mathrm{Z}(E)$. Enfin, le groupe dérivé E' est contenu dans $\Phi(E)$ et n'est pas trivial, donc est égal à $\Phi(E)$.

Tout groupe non cyclique d'ordre p^3 est extra-spécial généralisé.

Rappelons qu'un sous-groupe d'un groupe fini G est dit *caractéristique* s'il est stable par toute automorphisme de G (en particulier, tout sous-groupe caractéristique de G est distingué dans G).

Si E est un p-groupe extra-spécial généralisé non abélien, le groupe de Frattini de E et le groupe dérivé de E sont cycliques et centraux dans E. Ceci nous amène à donner la définition suivante.

Définition 3.7. *Un CC–*groupe *est un groupe fini résoluble non abélien E dont tout sous-groupe caractéristique propre est cyclique et central dans E.*

Proposition 3.8. *Le groupe dérivé E' d'un CC–groupe est d'ordre premier p et E/E' est abélien p–élémentaire.*

Les CC-groupes apparaissent comme un cas particulier des groupes du type suivant. Soit E un groupe fini non abélien possédant un sous-groupe central Z

d'ordre p, pour lequel on suppose choisi une fois pour toutes un isomorphisme avec le groupe additif de $\mathbb{Z}/p\mathbb{Z}$.

Si le groupe E/Z est abélien élémentaire, ce groupe est muni d'une structure naturelle d'espace vectoriel sur $\mathbb{F}_p$; on note V cet espace vectoriel. Un tel groupe E est appelé une *extension centrale* de V par $\mathbb{Z}/p\mathbb{Z}$. On a alors $1 \neq E' \subset \Phi(E) \subset Z$. Donc, $E' = \Phi(E) = Z$, et E est un groupe extra-spécial généralisé non abélien. En particulier, un CC-groupe est un p-groupe extra-spécial généralisé non abélien.

Réciproquement, soit E un p-groupe extra-spécial généralisé non abélien. De la relation $E' = \Phi(E)$, il résulte que E/E' est un p-groupe abélien élémentaire : c'est donc un espace vectoriel sur $\mathbb{F}_p$, que l'on note V et dont la loi est notée additivement. On a la suite exacte

$$1 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow E \longrightarrow V \longrightarrow 1.$$

Puisque $E' \subset \mathrm{Z}(E)$, le groupe E est de classe 2.

Structure des groupes extra-spéciaux généralisés

Soit E un p–groupe extra-spécial généralisé non abélien. Soit z un élément qui engendre E', choisi une fois pour toutes. Soit ζ l'application $\zeta\colon E' \to \mathbb{F}_p$ définie par $\zeta(z) := 1$. En d'autres termes, on a $\zeta([x,y]) = \alpha$, si $[x,y] = z^\alpha$.

Proposition 3.9. *Soit E un p–groupe extra-spécial généralisé non abélien.*

(a) *L'application* $E \times E \to \mathbb{F}_p$

$$(x,y) \longmapsto \zeta([x,y])$$

induit par passage au quotient une forme bilinéaire $a_E\colon V \times V \to \mathbb{F}_p$, qui est alternée.

(b)

- *Si $p \neq 2$, l'application* $E \to \mathbb{F}_p$

$$x \longmapsto \zeta(x^p)$$

induit par passage au quotient une forme linéaire $f_E\colon V \to \mathbb{F}_p$. Alors G est d'exposant p si et seulement si f_E est la forme nulle.

- *Si $p = 2$, l'application* $E \to \mathbb{F}_2$

$$x \longmapsto \zeta(x^2)$$

induit par passage au quotient une forme quadratique $q_E\colon V \to \mathbb{F}_2$, de forme bilinéaire associée a_E.

Démonstration. Soit $\pi\colon E \to E/E'$ la projection canonique. Nous définissons a_E par

$$a_E(\pi(x), \pi(y)) := \zeta([x,y])$$

Puisque $E' \subset \mathrm{Z}(E)$, a_E est bien définie. C'est une forme bilinéaire alternée (puisque $[x,x]=1$). L'application $E \to \mathbb{F}_p$, $x \mapsto \zeta(x^p)$, définit bien une application f_E de V dans $\mathbb{F}_p$. On a $\Sigma(2)=1$ et, pour $p \neq 2$, $\Sigma(p) \equiv 0 \pmod p$. Si $p \neq 2$ $(xy)^p = x^p y^p$, donc $f_E(\pi(x)+\pi(y)) = f_E(\pi(x)) + f_E(\pi(y))$, f_E est une forme linéaire. Le groupe E est d'exposant p si tout élément $x \neq 1$ de E est d'ordre p, *i.e.*, si $f_E = 0$. Si $p=2$, on a $(xy)^2 = x^2y^2[x,y]$, puisque $[y,x]$ est d'ordre au plus 2. Donc q_E est une forme quadratique de forme bilinéaire associée a_E. □

Corollaire 3.10. *Soit E un p-groupe extra-spécial ou un CC-groupe. Alors, la forme a_E est non dégénérée, et :*

(a) *si E est un p-groupe extra-spécial, il existe un entier n tel que $|E| = p^{2n+1}$.*

(b) *si E est un CC-groupe et $p \neq 2$, il est d'exposant p.*

Démonstration

(a) Nous supposons que E est un p-groupe extra-spécial : Si $\pi(x)$ appartient au noyau de a_E, par définition, pour tout y dans E, on a $[x,y]=1$, donc $x \in \mathrm{Z}(E)$, et par conséquent $\pi(x) = \pi(1)$, et a_E est non dégénérée. La théorie des formes alternées montre que V est de dimension paire sur $\mathbb{F}_p$, soit $2n$ cette dimension. On a donc $|V| = p^{2n}$ et $|E| = p^{2n+1}$.

(b) Supposons maintenant que E est un CC-groupe et que $p \neq 2$. Les éléments d'ordre au plus p de E forment un sous-groupe caractéristique d'indice au plus p, et par conséquent, E est d'exposant p. L'image réciproque dans E du radical de la forme a_E est un sous-groupe caractéristique abélien p-élémentaire, et donc la forme est non dégénérée.

□

CC-groupes et groupes de Heisenberg

Définition 3.11. *Soit F un corps de caractéristique différente de 2. Soit V un espace vectoriel de dimension $2n$ sur F. Soit $\langle\ ,\ \rangle$ une forme alternée non dégénérée sur V. On associe à V un groupe, noté $H(V)$, appelé* groupe de Heisenberg *de $(V, \langle\ ,\ \rangle)$ et défini de la façon suivante : $H(V)$ est l'ensemble $V \times F$, (muni de la topologie produit lorsque F est un corps topologique), et de la loi de groupe*

$$(v,t)(v',t') = (v+v', t+t'+\tfrac{1}{2}\langle v, v'\rangle).$$

Nous verrons à la proposition 3.15 que, lorsque F est un corps premier $\mathbb{F}_p$ à p éléments (p impair), le groupe $H(V)$ est un p–groupe extra-spécial.