Actions de groupes

Sommaire

La notion d'action réconcilie la présentation axiomatique de la théorie des groupes et le point de vue plus ancien des « groupes de transformations ». Une action du groupe G sur l'ensemble X permet en effet de représenter les éléments de G comme des transformations de X, donc de leur donner une signification géométrique.

Le but de ce texte est de présenter le vocabulaire de base relatif aux actions et d'en donner quelques illustrations significatives. Il est illusoire d'espérer assimiler des résultats théoriques relatifs aux groupes finis sans une pratique conséquente des exemples de base : groupes monogènes, abéliens finis, diédraux, symétriques, linéaires. La première partie de l'exposé est donc dévolue à des applications « concrètes », alors que la seconde revêt un caractère plus théorique.

Dans tout le texte, G est un groupe dont la loi est notée multiplicativement. On note e le neutre de G, $Z(G)$ le centre de G.

1 Vocabulaire de base, exemples

Cette partie rassemble d'une part le vocabulaire de base relatif aux actions (orbites, transitivité, stabilisateurs), d'autre part quelques exemples géométriques (en un sens large) et quelques applications simples mais séduisantes (dé-

termination du cardinal maximal d'un sous-groupe abélien de $\mathcal{S}_n$, conséquences de la formule de Burnside-Frobenius, en particulier la borne de Cameron-Cohen).

1.1 Définitions

Soit X un ensemble. On appelle *action* ou *opération* de G sur X toute application de $G \times X$ dans X notée :

$$\begin{array}{ccc} G \times X & \to & X \\ (g,x) & \mapsto & g.x \end{array}$$

vérifiant :

i) $\forall x \in X,\ e.x = x$,

ii) $\forall (g_1, g_2) \in G^2,\ \forall x \in X,\ g_2.(g_1.x) = (g_2 g_1).x$.

Un ensemble non vide muni d'une action de G est appelé *G-ensemble*.

Avec ces notations, il est clair que pour tout $g \in G$, l'application :

$$\rho(g)\ :\ \begin{array}{ccc} X & \to & X \\ x & \mapsto & g.x \end{array}$$

est une bijection de X sur lui-même d'inverse $\rho(g^{-1})$ et que ρ est un morphisme de G dans $\mathcal{S}(X)$, ou encore une *représentation de G dans l'espace X*.

Inversement, si ρ est un morphisme de G dans $\mathcal{S}(X)$, l'application de $G \times X$ dans X définie par :

$$\forall (g,x) \in G \times X, \qquad g.x = \rho(g)(x)$$

est une action de G sur X. « Action de G sur X » et « morphisme de G dans $\mathcal{S}(X)$ » sont donc deux notions équivalentes : l'action naturelle de $\mathcal{S}(X)$ sur X est le premier exemple d'action.

Si $x \in X$, l'ensemble :

$$\omega(x) = \{g.x,\ g \in G\}$$

est appelé *orbite de x* (sous-entendu : sous l'action considérée). On attache à l'action une relation d'équivalence sur X définie par :

$$x \sim y \quad \Longleftrightarrow \quad y \in \omega(x).$$

Les classes de $\sim$ sont les orbites de l'action.

L'action est dite *transitive* si X est la seule orbite de la relation d'équivalence, i.e. si et seulement si pour tout x de X, $\omega(x) = X$. Un ensemble muni d'une action transitive de G est appelé un *G-espace homogène*. [1]

Dans le cas général, les orbites définissent une partition de X dont tous les éléments sont stables par G et sur chacun desquels l'action de G par restriction est transitive. Autrement dit, si les orbites sont les X_i pour i dans I, l'image du morphisme ρ s'identifie à un sous-groupe de $\prod_{i \in I} \mathcal{S}(X_i)$ dont l'action sur chaque facteur X_i est transitive.

1. Le terme « homogène » reflète, de manière imagée, la transitivité de l'action.

On notera qu'une action de G sur X en fournit immédiatement beaucoup d'autres : action induite par un sous-groupe H de G sur X, action associées de G sur X^k, sur l'ensemble des parties de X etc ...

La notion d'action de groupe est le point du départ du *programme d'Erlangen* de Félix Klein. Dans ce texte de 1872 apparaît pour la première fois l'idée consistant à voir une géométrie comme l'étude de l'action d'un groupe sur un ensemble : ainsi, la « classification des triangles semblables », qui remonte en substance à l'Antiquité, s'interprète comme la description des orbites de l'action du groupe des similitudes sur l'ensemble des triangles du plan.

1.2 Quelques exemples

1. *Actions du groupe linéaire*
   Si $\mathbb{K}$ est un corps et E un $\mathbb{K}$-espace vectoriel, $\mathrm{GL}(E)$ agit naturellement sur E ; cette action a deux orbites, à savoir $\{0\}$ et $E \setminus \{0\}$ (conséquence du théorème de la base incomplète).

   Le groupe $\mathrm{GL}(E)$ agit aussi sur l'ensemble des sous-espaces vectoriels de E. L'orbite d'un sous-espace V est constituée, si E est de dimension finie, des sous-espaces de E ayant même dimension que V (toujours grâce au théorème de la base incomplète). Si E est de dimension finie n et $d \in \{0, \ldots, n\}$, l'ensemble des sous-espaces de dimension d de E est la *grassmanienne des d-plans de E*, qui apparaît ainsi comme un exemple fondamental d'espace homogène. [2]

2. *Actions du groupe orthogonal euclidien*
   Si E est un espace euclidien, le groupe orthogonal de E agit naturellement sur E ; les orbites sont les sphères centrées sur 0.

   Le groupe orthogonal agit aussi sur l'ensemble des sous-espaces de E, les orbites étant les ensembles de sous-espaces de dimension donnée (théorème de la base orthonormée incomplète).

3. *Classifications des coniques, ellipse de Steiner d'un triangle*
   Le groupe affine d'un plan affine euclidien P agit sur l'ensemble $\mathcal{C}_P$ des coniques non dégénérées de P. En utilisant la conservation de la compacité et de la connexité, on voit qu'il y a au moins trois orbites : l'ensemble des paraboles, celui des ellipses, celui des hyperboles. Il est facile de voir que deux coniques de même « type » sont affinement équivalentes : il y a donc exactement trois orbites.

   Voici une jolie application. Soit à montrer que, si ABC est un triangle de P, il existe une ellipse tangente à chacun des côtés de ce triangle en son milieu (dite « ellipse de Steiner » du triangle). Si le triangle est équilatéral, le cercle inscrit convient. Pour s'y ramener, on envoie ABC sur un triangle équilatéral $A'B'C'$ par une bijection affine g du plan sur lui-même. Si C est le cercle inscrit à $A'B'C'$, $g^{(-1)}(C)$ est une ellipse tangente à chaque côté de ABC en son milieu (car g préserve les milieux et la tangence). [3]

2. L'espace projectif $P^1(E)$ correspond à $d = 1$.

3. Ce type d'utilisation des transformations en géométrie peut évidemment se traiter de manière plus terre à terre mais fondamentalement équivalente par le choix d'un repère adapté à la situation.

Si on fait agir le groupe des isométries affines sur $\mathcal{C}_P$, les classes sont plus nombreuses : les coniques et hyperboles sont classées par le couple (a, b) des longueurs des axes, les paraboles par le paramètre.

Enfin, deux coniques de même nature sont semblables si et seulement si elles ont même excentricité.

4. *Actions matricielles classiques*
   Rappelons plusieurs actions classiques relatives à des phénomènes de « changement de base » en algèbre linéaire ou bilinéaire. Soit $\mathbb{K}$ un corps.

   Si $(m, n) \in \mathbb{N}^{*2}$, le groupe $\mathrm{GL}_m(\mathbb{K}) \times \mathrm{GL}_n(\mathbb{K})$ agit sur $\mathcal{M}_{m,n}(\mathbb{K})$ par $(P, Q).M = PMQ^{-1}$ (« équivalence des matrices »). L'orbite d'une matrice M est l'ensemble des matrices de $\mathcal{M}_{m,n}(K)$ ayant le rang de M.

   De même $\mathrm{GL}_n(K)$ agit sur $\mathcal{M}_n(K)$ par $P.M = PMP^{-1}$ (« similitude des matrices »). L'orbite de M est la classe de similitude de M.

   Enfin, $\mathrm{GL}_n(\mathbb{K})$ agit sur l'espace $S_n(\mathbb{K})$ des matrices symétriques de $\mathcal{M}_n(\mathbb{K})$ par $P.M = PM^tP$ (« congruence des matrices symétriques »).

5. *Action du groupe de Galois d'un polynôme sur les racines*
   Le groupe de Galois d'un polynôme séparable P de $\mathbb{K}[X]$ agit naturellement sur l'ensemble des racines de ce polynôme. L'orbite d'une racine est constituée des racines ayant même polynôme minimal. En particulier, l'action est transitive si et seulement si P est irréductible sur $\mathbb{K}$.

   Variante : si $\mathbb{L}/\mathbb{K}$ est une extension galoisienne, le groupe $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ agit sur $\mathbb{L}$, et l'orbite d'un élément est l'ensemble de ses $\mathbb{K}$-conjugués.

6. *Un résultat relatif aux sous-groupes transitifs de $\mathcal{S}_n$*
   Le résultat précédent explique pourquoi la théorie de Galois a conduit naturellement à s'intéresser aux sous-groupes « transitifs » de $\mathcal{S}_n$. Soit G un tel sous-groupe. Nous allons montrer que si G contient une transposition et un $(n-1)$-cycle, alors $G = \mathcal{S}_n$. [4]

   Quitte à conjuguer G dans $\mathcal{S}_n$, on peut supposer que G contient le $(n-1)$-cycle $c = (1, 2, \ldots, n-1)$. Soit τ une transposition de G. La transitivité de G permet de supposer, quitte à conjuguer par un élément de G, que $\tau = (i, n)$ pour un certain i de $\{1, \ldots, n-1\}$. Les conjugués de τ par les puissances de c sont les (j, n) pour $1 \leq j \leq n-1$, qui engendrent $\mathcal{S}_n$.

7. *Décomposition de Bruhat du groupe linéaire*
   Cet exemple est moins classique. Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}^*$, $\mathcal{B}_n(\mathbb{K})$ le sous-groupe de $\mathrm{GL}_n(K)$ constitué des matrices triangulaires supérieures inversibles. [5]

   Faisons agir le groupe $\mathcal{B}_n(K) \times \mathcal{B}_n(K)$ sur $\mathrm{GL}_n(K)$ par :

   $$(P, Q).M = PMQ^{-1}.$$

   La décomposition de Bruhat de $\mathrm{GL}_n(K)$ est le résultat suivant.

   Théorème 1. *Toute orbite contient une et une seule matrice de permutation.*

4. Il existe de nombreux résultats de ce type, dont certains très élaborés.
5. Souvent nommé *sous-groupe de Borel standard de $GL_n(\mathbb{K})$*.

Preuve. Pour voir que toute orbite contient une matrice de permutation, on utilise les opérations élémentaires. L'orbite d'une matrice M est stable par l'une quelconque des opérations suivantes :

$$L_i \leftarrow L_i + \lambda L_j, \quad 1 \leq i < j \leq n,\ \lambda \in \mathbb{K},$$

$$C_j \leftarrow C_j + \lambda C_i, \quad 1 \leq i < j \leq n,\ \lambda \in \mathbb{K}.$$

Partons alors de M dans $\mathcal{M}_n(\mathbb{K})$ et notons i_1 le plus grand i tel que $M_{i,1} \neq 0$. Par des opérations élémentaires $L_i \leftarrow L_i + \lambda L_{i_1}, i < i_1$, on transforme M en une matrice M^1 dont la première colonne a pour seul terme non nul celui de place $(i_1, 1)$. Par des opérations $C_j \leftarrow C_j + \lambda C_1, j > 1$ on transforme M^1 en M^2 dont la première colonne et la i_1-ième ligne ont pour seul terme non nul celui de place $(i_1, 1)$. On continue en notant i_2 le plus grand i tel que $M^2_{i,2} \neq 0$. On a $i_2 \neq i_1$ et des opérations successives $L_i \leftarrow L_i + \lambda L_{i_2}, i < i_2$, $C_j \leftarrow C_j + \lambda C_2, j > 2$ transforment M^2 en une matrice M^3 ayant même première colonne et même ligne d'indice i_1 que M^2 et une seconde colonne et une i_2-ième ligne dont le seul terme non nul est celui de place $(i_2, 2)$. Répétant n fois cet argument, on obtient une matrice dans l'orbite de M et *monomiale*, c'est-à-dire contenant exactement un terme non nul par ligne et par colonne. Une multiplication par une matrice diagonale transforme cette dernière matrice en matrice de permutation.

Il reste à établir que deux matrices de permutation distinctes sont dans deux orbites distinctes, ou encore que l'égalité : $P_{\sigma'}T' = TP_\sigma$ avec T et T' dans $\mathcal{B}_n(\mathbb{K})$ implique $\sigma = \sigma'$. Notons A la matrice $TP_\sigma = P_{\sigma'}T'$. Pour $1 \leq k \leq n$, la première expression de A montre que $\sigma(k)$ est le maximum des i tels que tel que : $A_{i,k} \neq 0$ alors que la seconde établit que $A_{\sigma'(k),k} \neq 0$. On a ainsi $\sigma'(k) \leq \sigma(k)$ pour tout k d'où l'on déduit aisément $\sigma = \sigma'$.

Pour σ dans $\mathcal{S}_n$, on note W_σ l'orbite de P_σ pour l'action précédente, c'est-à-dire la « cellule »

$$W_\sigma = \mathcal{B}_n(\mathbb{K})\ P_\sigma\ \mathcal{B}_n(\mathbb{K}).$$

Il découle de la décomposition de Bruhat qu'un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$ contenant $\mathcal{B}_n(\mathbb{K})$ est déterminé par les matrices de permutation qu'il contient, d'où une injection naturelle respectant l'inclusion entre l'ensemble de ces sous-groupes et celui des sous-groupes de $\mathcal{S}_n$.

Une dernière remarque. Soit σ l'élément de $\mathcal{S}_n$ défini par :

$$\forall j \in \{1, \ldots, n\}, \qquad \sigma(j) = n + 1 - j.$$

L'orbite de P_σ est l'ensemble des produits $P_\sigma LU$ où L (resp. U) est triangulaire inférieure (resp. supérieure) inversible. Or, il est aisé d'établir que les matrices s'écrivant sous la forme LU avec L (resp. U) triangulaire inférieure (resp. supérieure) sont celles dont les matrices extraites : $\{1\}^2$, $\{1,2\}^2$, …, $\{1,2,\ldots,n-1\}^2$, $\{1,2,\ldots,n\}^2$ sont inversibles. [6] L'orbite précédente est donc le complément d'un sous-variété algébrique de

6. Ce résultat, dont la preuve directe est simple, est connu en analyse numérique sous le nom de « décomposition LU ». Il est à la base d'une technique de résolution de systèmes linéaires.

$\mathcal{M}_n(\mathbb{K})$ ce qui justifie son nom de « grosse cellule » de la décomposition de Bruhat.

8. *Nombre d'actions d'un groupe de type fini sur un ensemble fini*

   Cet exemple et celui qui le suit sont plus théoriques. Soient G un groupe de type fini, X une partie génératrice finie de G. Si Γ est un groupe fini, l'ensemble des morphismes de G dans Γ est fini, de cardinal majoré par $|\Gamma|^{|X|}$. Il s'ensuit que l'ensemble des actions de G sur un ensemble fini E de cardinal m, équipotent à l'ensemble des morphismes de G dans $\mathcal{S}_m$ est fini, de cardinal majoré par $(m!)^{|X|}$. Le nombre d'actions de G sur E ne dépend évidemment que de m.

   Pour k dans $\mathbb{N}$, soit $A_k(G)$ le nombre d'actions de G sur un ensemble de cardinal k, avec la convention évidente $A_0(G) = 1$. On sait que $A_k(G)$ est le nombre de morphismes de G dans $\mathcal{S}_k$. Ce nombre peut se calculer dans certains cas. Par exemple, si $r \in \mathbb{N}^*$ et si L_r est le groupe libre sur un alphabet de cardinal r, on a $A_{L_r} = (k!)^r$.

9. *Nombre d'actions transitives d'un groupe de type fini sur un ensemble fini*

   Les notations sont celles de l'exemple précédent. Pour k dans $\mathbb{N}$, soit $A'_k(G))$ le nombre d'actions transitives de G sur un ensemble de cardinal k, avec la convention évidente $A'_0(G) = 1$. Nous allons relier les $A'_k(G)$ aux $A_k(G)$. On observe à cet effet que, pour k dans $\mathbb{N}^*$, une action de G sur $\{1, \ldots, k\}$ est déterminée par les données suivantes :

   - l'orbite de 1 ; si ℓ est le cardinal de cette orbite, il y a $\binom{k}{\ell}$ choix ;

   - l'action transitive de G sur l'orbite de 1, pour laquelle il y a $A_\ell(G)$ choix ;

   - l'action de G sur le complémentaire de l'orbite de 1, pour laquelle il y a $A'_{k-\ell}(G)$ choix.

   On arrive donc à la formule de récurrence :

$$A_k(G) = \sum_{\ell=1}^{k} \binom{k}{\ell} A_\ell(G)\ A'_{k-\ell}(G).$$

Exercice 1. ② *Montrer l'unicité de l'ellipse de Steiner.*

Exercice 2. ③ *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Le groupe $GL(E)$ agit naturellement sur l'ensemble des couples (E_1, E_2) de sous-espaces vectoriels de E. Décrire les orbites.*

Exercice 3. ③ *Le groupe $\mathcal{B}_n(\mathbb{K})$ des matrices triangulaires supérieures inversibles agit naturellement sur $\mathbb{K}^n$. Décrire les orbites.*

Exercice 4. ④ *Soient $(E, \langle\ ,\rangle)$ un espace euclidien, m dans $\mathbb{N}^*$. On fait agir naturellement $\mathcal{O}(E)$ sur E^m. Montrer que l'orbite de $(x_1, \ldots, x_m)$ est l'ensemble des $(y_1, \ldots, y_m)$ tels que*

$$\forall (i,j) \in \{1, \ldots, m\}^2, \qquad \langle y_i, y_j \rangle = \langle x_i, x_j \rangle .$$

En d'autres termes, les orbites sont décrites par les matrices de Gram.

Exercice 5. ④ *Soient p un nombre premier, G un sous-groupe de $\mathcal{S}_p$ agissant transitivement sur $\{1,\dots,p\}$ et contenant une transposition. Montrer $G=\mathcal{S}_p$.*

Exercice 6. ③ *Déterminer les sous-groupes de $GL_n(\mathbb{K})$ contenant $\mathcal{B}_n(\mathbb{K})$ pour $n=2$, puis pour $n=3$.*

Exercice 7. ③ *Soit M dans $GL_n(\mathbb{K})$. Traduire l'appartenance de M à la grosse cellule à l'aide de l'algorithme utilisé pour établir l'existence de la décomposition de Bruhat.*

Exercice 8. ④ *Soit V un $\mathbb{K}$-espace vectoriel de dimension n. On appelle drapeau de V toute suite $\mathcal{V}=(V_1,V_2,\dots,V_n)$ de sous-espaces de V croissante pour l'inclusion et telle que, pour tout i, $\dim V_i=i$. Une base $(e_1,\dots,e_n)$ de V est dite adaptée au drapeau $(V_1,\dots,V_n)$ si, pour tout i de $\{1,\dots,n\}$, $(e_1,\dots,e_i)$ est une base de V_i.*

En utilisant la décomposition de Bruhat, montrer que, si $\mathcal{V}=(V_1,\dots,V_n)$ et $\mathcal{V}'=(V'_1,\dots,V'_n)$ sont deux drapeaux de V il existe σ dans $\mathcal{S}_n$ et une base $(e_1,\dots,e_n)$ de V adaptée à $\mathcal{V}$ telle que $(e_{\sigma(1)},\dots,e_{\sigma(n)})$ soit adaptée à $\mathcal{V}'$.

Exercice 9. ⑤ *Dénombrer chaque orbite de la décomposition de Bruhat si $\mathbb{K}=\mathbb{F}_q$.*

Exercice 10. ⑤ *Soit G un sous-groupe de $SO_3(\mathbb{R})$ agissant transitivement sur la sphère unité canonique S^2 de $\mathbb{R}^3$. Montrer que $G=SO_3(\mathbb{R})$.*

Exercice 11. ③ *Soient k,ℓ,n dans $\mathbb{N}^*$ avec $k\leq\ell\leq n/2$, et pour $1\leq i\leq n$, P_i l'ensemble des parties de cardinal i de $X=\{1,\dots,n\}$. On fait agir naturellement $\mathcal{S}_n$ sur $P_k\times P_\ell$. Décrire les orbites.*

Exercice 12. ③ *Soit p un nombre premier n un élément de $\mathbb{N}^*$. Déterminer $A_n(\mathbb{Z}/p\mathbb{Z})$.*

1.3 Actions d'un groupe versus structure

Revenons au morphisme ρ de **1.1**. L'action est dite *fidèle* si ρ est injectif, auquel cas G est isomorphe à un sous-groupe de $\mathcal{S}(X)$. Cette notion appelle deux commentaires.

1. Pour montrer que le groupe G est isomorphe à un sous-groupe de $\mathcal{S}_n$, il suffit de le faire agir fidèlement sur un ensemble de cardinal n.

2. Même si G est un sous-groupe de $\mathcal{S}(X)$, des actions non fidèles de G apparaissent naturellement par restriction aux orbites. Il est donc inévitable, pour comprendre les plongements de G dans $\mathcal{S}(X)$, de généraliser la notion de plongement en celle d'action.

Lorsque le groupe G agit sur un ensemble X, on appelle *propriétés géométriques* de G (sous-entendu : agissant sur X) les propriétés liées à l'action, par opposition aux propriétés algébriques qui sont celles ne faisant intervenir que la structure « abstraite » de groupe.

Les propriétés algébriques imposent des restrictions aux actions de G. Autrement dit, les actions de G aident à comprendre sa structure. Ce fait, déjà implicite dans le point 1 ci-dessus, est illustré par les exemples suivants.

Exemples.

1. *Plongement de $\mathcal{D}_n$ dans $\mathcal{S}_n$ pour $n \geq 3$*
   Par définition, le groupe diédral $\mathcal{D}_n$ agit sur un ensemble de cardinal n, à savoir le polygone régulier à n sommets. Pour $n \geq 3$, cette action est fidèle (car le polygone engendre vectoriellement le plan et l'action est linéaire) et $\mathcal{D}_n$ se plonge donc dans $\mathcal{S}_n$.

2. *Le quotient de $\mathcal{S}_4$ par $\mathcal{V}$ s'identifie à $\mathcal{S}_3$*
   Soient $X = \{1, 2, 3, 4\}$, E l'ensemble des paires $\{A, X \setminus A\}$ où A parcourt l'ensemble des parties de cardinal 2 de X : E est de cardinal 3. Le groupe $\mathcal{S}(X)$ agit naturellement sur E. Comme l'action de $\mathcal{S}(X)$ sur l'ensemble des parties de cardinal 2 de X est transitive, le morphisme de $\mathcal{S}(X)$ dans $\mathcal{S}(E)$ associé à cette action est surjectif. On vérifie que le noyau de ce morphisme est le *groupe de Klein* $\mathcal{V}$, constitué de l'identité et des trois doubles transpositions.

3. *Petits groupes $PGL_2(\mathbb{F}_q)$.*
   Si E est un espace vectoriel sur le corps K, le quotient $\mathrm{PGL}(E)$ du groupe $\mathrm{GL}(E)$ par le sous-groupe des homothéties inversibles de E agit naturellement sur l'ensemble $P(E)$ des droites de E (*espace projectif associé à E*). L'action est transitive (théorème de la base incomplète) et fidèle (caractérisation des homothéties).

   Pour $K = \mathbb{F}_q$ et E de dimension 2, $P(E)$ est de cardinal $q + 1$, d'où un plongement de $PGL(E)$ dans $\mathcal{S}_{q+1}$. Or $|PGL(E)| = q^3 - q$. On en déduit deux *isomorphismes exceptionnels* très simples.

   Théorème 2. *Le groupe $PGL_2(\mathbb{F}_2) = GL_2(\mathbb{F}_2)$ est isomorphe à $\mathcal{S}_3$, le groupe $PGL_2(\mathbb{F}_3)$ à $\mathcal{S}_4$.*

   Il existe de nombreux autres isomorphismes exceptionnels.

4. *Groupe du tétraèdre.*
   Soient E l'espace affine euclidien tridimensionnel, a_1, a_2, a_3, a_4 les sommets d'un tétraèdre régulier, G le groupe des isométries affines de E stabilisant $X = \{a_i, 1 \leq i \leq 4\}$. Par définition, G agit sur X. Puisque les images de quatre points non coplanaires déterminent une application affine, l'action est fidèle.

   Par ailleurs, $\mathrm{Im}\rho = \mathcal{S}(X)$. En effet, si $1 \leq i < j \leq 4$, la symétrie $\sigma_{i,j}$ par rapport au plan médiateur de $[a_i, a_j]$ s'envoie sur la transposition (a_i, a_j), d'où le résultat puisque les transpositions engendrent $\mathcal{S}(X)$. Ainsi, G est isomorphe à $\mathcal{S}_4$.

   Théorème 3. *Le groupe des isométries du tétraèdre régulier est $\mathcal{S}_4$.*

5. *Groupe du cube*
   Soient maintenant $a_1, \ldots, a_8$ les sommets d'un cube C de l'espace affine euclidien tridimensionnel E, G le groupe des isométries de E stabilisant $S = \{a_1, \ldots, a_8\}$, G^+ le sous-groupe des déplacements de G. Les éléments de G stabilisent l'isobarycentre o des a_i ; on vectorialise donc E en o de sorte que les éléments de G deviennent des isométries vectorielles.

   L'action naturelle de G sur S donne un morphisme de G dans $\mathcal{S}_8$. On peut plus efficacement faire agir G sur un ensemble de cardinal 4. Notons $\delta_1, \ldots, \delta_4$ les « grandes diagonales » de C, Δ leur ensemble. Puisque les éléments de G sont des isométries, ils envoient un couple de sommets

de C appartenant à une même grande diagonale sur un couple de même nature. En d'autres termes, G agit naturellement sur Δ.

Le noyau du morphisme ρ associé à l'action de G sur Δ est constitué des $g \in G$ stabilisant les δ_i. Les droites vectorielles δ_i pour $1 \leq i \leq 4$ sont stables par les éléments de $\mathrm{Ker}(\rho)$, donc propres pour ces éléments. Les valeurs propres associées appartiennent à $\{1, -1\}$ (isométries), et les éléments de $\mathrm{Ker}(\rho)$ sont des symétries orthogonales. Aucune des δ_i n'étant orthogonale aux trois autres, $\mathrm{Ker}(\rho) = \{Id, -Id\}$ et l'action obtenue par restriction à G^+ est fidèle.

Il reste à vérifier que $\rho(G^+)$ contient les transpositions pour obtenir l'isomorphie de G^+ et $\mathcal{S}_4$. Mais si $1 \leq i < j \leq 4$, le demi-tour r autour de la droite passant par les milieux des arêtes contenant les extrémités de δ_i et δ_j vérifie $\rho(r) = (\delta_i, \delta_j)$.

Théorème 4. *Le groupe des isométries directes du cube est $\mathcal{S}_4$.*

Un sous-produit de ce résultat est une réalisation géométrique de l'isomorphisme de $\mathcal{S}_4/\mathcal{V}$ et de $\mathcal{S}_3$. Si F est une face de C, soit D_F la droite passant par le centre de F et orthogonale à F. Les droites D_F et $D_{F'}$ sont égales si et seulement si les faces F et F' sont égales ou opposées. L'ensemble Δ des D_F est donc de cardinal 3. Le groupe G^+ agit transitivement sur Δ (une rotation d'angle $\pi/2$ dans le plan de deux des droites les échange), d'où un morphisme de G^+ dans $\mathcal{S}_3$. Le noyau du morphisme associé est constitué des éléments de G^+ qui stabilisent chacune des trois droites ; dans une base adaptée les éléments de ce noyau sont donc les :

$$\begin{pmatrix} \varepsilon_1 & 0 & 0 \\ 0 & \varepsilon_2 & 0 \\ 0 & 0 & \varepsilon_3 \end{pmatrix},$$

avec : $(\varepsilon_1, \varepsilon_2, \varepsilon_3) \in \{\pm 1\}^3$ et : $\varepsilon_1\varepsilon_2\varepsilon_3 = 1$. Ce groupe est isomorphe à $\mathcal{V}$ et agit par doubles transpositions sur l'ensemble Δ.

On peut étudier de manière analogue les groupes des autres polyèdres réguliers. Le groupe des isométries de l'icosaèdre est ainsi isomorphe à $\mathcal{A}_5$.

6. *Exemples de couples de matrices engendrant un groupe libre*

Disons que deux éléments a et a' de G ne vérifient aucune relation non triviale, ou encore que a et a' sont libres si, pour $m_1, \ldots, m_r, m'_1, \ldots m'_r$ dans $\mathbb{Z}$, on a l'implication

$$a'^{m'_r} a^{m_r} \ldots a'^{m'_1} a^{m_1} = e \implies \forall i \in \{1, \ldots, r\},\ m_i = m'_i = 0.$$

Si tel est le cas, le groupe engendré par a et b est un *groupe libre à deux générateurs*[7].

Soient z et z' deux nombres complexes de modules ≥ 2,

$$T = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad T'^{-} = \begin{pmatrix} 1 & 0 \\ z' & 1 \end{pmatrix}.$$

7. Cette terminologie mériterait d'être précisée par un résultat d'unicité à isomorphisme près et la preuve du caractère intrinsèque du cardinal (ici 2) de l'ensemble des générateurs.

Nous allons montrer que les deux éléments T et T' du groupe $\mathrm{SL}_2(\mathbb{C})$ ne vérifient aucune relation non triviale, i.e. que le sous-groupe de $\mathrm{SL}_2(\mathbb{C})$ engendré par ces matrices est isomorphe au groupe libre L_2. Pour cela, soient :

$$\Omega_1 = \{(x,y) \in \mathbb{C}^2, |x| < |y|\}, \quad \Omega_2 = \{(x,y) \in \mathbb{C}^2, |y| < |x|\}.$$

Si m et m' sont des éléments de $\mathbb{Z}^*$, on a :

$$(T)^m(\Omega_1) \subset \Omega_2, \qquad (T')^{m'}(\Omega_2) \subset \Omega_1,$$

d'où le résultat grâce au théorème ci-après, qui est un cas particulier de l'*argument du ping-pong* de Klein.

Théorème 5. *On suppose que G agit sur un ensemble X que a et b sont deux éléments de G, qu'il existe deux parties X_1 et X_2 de X telles que $X_1 \not\subset X_2$ et que*

$$\forall m \in \mathbb{Z}^*, \qquad a^m(X_1) \subset X_2, \quad b^m(X_2) \subset X_1.$$

Alors a et b ne satisfont aucune relation non triviale.

Preuve. Soit c un mot en a et b non réduit à une puissance de a. En conjugant c par une puissance de a, on obtient un élément c' de G de la forme : $a^{k_1}b^{l_1}...b^{l_{p-1}}a^{k_p}$ où $p \geq 2$ et où les k_i et l_i sont dans $\mathbb{Z}^*$. On a :

$$c'(X_1) \subset X_2,$$

ce qui montre que c' ne peut être égal à e. Il en est de même de c.

7. *Quaternions et isomorphisme de $SO_3(\mathbb{R})$ et $PSU_2(\mathbb{C})$.*
Soit $\mathcal{H}$ l'ensemble des matrices de la forme

$$\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}, \qquad (a,b) \in \mathbb{C}^2.$$

Il est clair que $\mathcal{H}$ est une sous-algèbre réelle de dimension 4 de $\mathcal{M}_2(\mathbb{C})$ (mais pas une sous-algèbre complexe). De plus, $\mathcal{H}$ est une algèbre à division : c'est *l'anneau à division des quaternions réels*.

Les nombres complexes de module 1 paramètrent les rotatons d'un plan euclidien. De même, les quaternions permettent de représenter les rotations d'un espace euclidien de dimension 3 ou 4.
Munissons $\mathcal{H}$ de la norme euclidienne N donnée par : $N(h) = \sqrt{\det(h)}$ si $h \in \mathcal{H}$. Soit $\mathcal{H}_0$ le sous-espace réel (de dimension 3) des matrices de $\mathcal{H}$ de trace nulle. Le groupe $\mathrm{SU}_2(\mathbb{C})$ n'est autre que la sphère unité de l'espace euclidien $(\mathcal{H}, N)$. On le fait agir sur $\mathcal{H}_0$ en posant,

$$\forall (g,h) \in \mathrm{SU}_2(\mathbb{C}) \times \mathcal{H}_0, \qquad g.h = ghg^{-1}.$$

Notons ρ le morphisme associé à cette action. Chaque $\rho(g)$ est une isométrie de l'espace $(\mathcal{H}_0, N)$, d'où un morphisme de $\mathrm{SU}_2(\mathbb{C})$ dans $\mathcal{O}_3(\mathbb{R})$. Nous allons démontrer le :

Théorème 6. *Le morphisme ρ vérifie :*

$$Ker(\rho) = \{Id, -Id\}, \qquad Im(\rho) = SO_N(\mathcal{H}_0).$$

Par conséquent, ρ induit, par passage au quotient et identification de $SO_N(\mathcal{H}_0)$ à $SO_3(\mathbb{R})$, un isomorphisme de $PSU_2(\mathbb{C})$ sur $SO_3(\mathbb{R})$.

Pour la première assertion, il suffit de vérifier que les éléments de $\mathrm{Ker}(\rho)$ sont des homothéties, i.e. que ces éléments stabilisent toute droite de $\mathbb{C}^2$. Mais si D est une telle droite, il existe $h \in \mathrm{SU}_2(\mathbb{C})$ dont D est un espace propre. Or, puisque

$$\mathcal{H} = \mathcal{H}_0 \oplus \mathbb{C}I_2,$$

les éléments de $\mathrm{Ker}(\rho)$ sont centraux dans $\mathrm{SU}_2(\mathbb{C})$ et stabilisent donc les espaces propres de tout élément de $\mathrm{SU}_2(\mathbb{C})$.

Pour la seconde assertion, on observe d'abord que la connexité de $\mathrm{SU}_2(\mathbb{C})$ entraîne que ρ est à valeurs dans $\mathrm{SO}_N(\mathcal{H}_0)$. Il reste à montrer que tout demi-tour de $(\mathcal{H}_0, N)$ appartient à $\mathrm{Im}(\rho)$. Cherchons donc, si $h \in \mathcal{H}_0 \backslash \{0\}$, un antécédent par ρ au demi-tour d'axe $\mathbb{R}h$. Un tel antécédent commute à h et a pour carré Id ou $-Id$. Réciproquement, si $g \in \mathrm{SU}_2(\mathbb{C})$ commute à h et a pour carré Id ou $-Id$, $\rho(g)$ est une symétrie orthogonale de déterminant 1 fixant h ; si de plus g n'est pas une homothétie, $\rho(g)$ n'est pas l'identité, et est donc nécessairement le demi-tour d'axe $\mathbb{R}h$. L'existence de h vérifiant ces conditions se prouve facilement en diagonalisant unitairement h ; précisément, on vérifie qu'il y a (comme il se doit) exactement deux matrices convenables, toutes deux de spectre $\{i, -i\}$ et ayant comme espaces propres ceux de h. [8]

Exercice 13. ② *Vérifier qu'une action d'un groupe simple est triviale ou fidèle.*

Exercice 14. ③ *Montrer que le groupe des isométries directes du tétraèdre régulier est isomorphe à $\mathcal{A}_4$.*

Exercice 15. ② *Montrer que le groupe G de l'exemple 5 ci-dessus est isomorphe à $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.*

Exercice 16. ③ *Montrer que $PSL_2(\mathbb{F}_3)$ est isomorphe à $\mathcal{A}_4$, $PSL_2(\mathbb{F}_4)$ à $\mathcal{A}_5$. On pourra utiliser la simplicité de ces groupes.*

Exercice 17. ④ *Soit $n \geq 2$ un entier. Montrer que, génériquement, deux matrices de $GL_n(\mathbb{C})$ ne vérifient aucune relation non triviale* [9].

Exercice 18. ③*Soient G un groupe, a et b deux éléments de G ne vérifiant aucune relation non triviale. Pour i dans $\mathbb{N}$, soit $c_i = a^i b a^i$. Montrer que les $c_i, i \in \mathbb{N}$ ne vérifient aucune relation non triviale, ce qui signifie que, si $i_1, \ldots, i_r$ sont des éléments de $\mathbb{N}$ tels que, pour tout j, $i_j \neq i_{j+1}$ et $(n_1, \ldots, n_r)$ un élément de $\mathbb{Z}^r$, on ait*

$$c_{i_r}{}^{n_r} \times \cdots \times c_{i_1}{}^{n_1} = e \quad \Longrightarrow \quad \forall j \in \{1, \ldots, r\}, \qquad n_j = 0.$$

Ainsi, un groupe libre à deux générateurs contient un groupe libre à une infinité dénombrable de générateurs.

8. Topologiquement, le morphisme ρ est un *revêtement à deux feuillets*. Puisque $\mathrm{SU}_2(\mathbb{C})$ n'est autre que la sphère S^3, simplement connexe, on peut en déduire que le groupe fondamental de $\mathrm{SO}_3(\mathbb{R})$ est de cardinal 2.

9. Il faut évidemment donner un sens précis au mot « générique ».

Terminons par une application amusante et un peu plus savante du théorème 5. Disons que G est *virtuellement fini* s'il possède suffisamment de quotients finis pour séparer les points, c'est-à-dire si pour tout $g \neq e$, il existe un morphisme φ de G dans un groupe fini tel que $g \notin \mathrm{Ker}(\varphi)$. En considérant les morphismes de réduction modulo m :

$$\mathrm{SL}_2(\mathbb{Z}) \longmapsto \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}),$$

on voit immédiatement que le groupe $\mathrm{SL}_2(\mathbb{Z})$ est virtuellement fini. Pour le groupe libre L_2, on peut utiliser les plongements du théorème 5 pour établir un résultat plus fort : pour tout nombre premier p, L_2 a suffisamment de quotients qui sont des p-groupes finis pour séparer les points. C'est l'objectif de l'exercice suivant.

Exercice 19. ⑤ *Si $m \in N^*$, on note $\Gamma_2(m)$ l'ensemble des matrices de $SL_2(\mathbb{Z})$ congrues à I_2 modulo $m\mathcal{M}_2(\mathbb{Z})$.*

a) Vérifier que $\Gamma_2(m)$ est un sous-groupe de $SL_2(\mathbb{Z})$.

b) Soient p un nombre premier, m un entier ≥ 2. Montrer que $\Gamma_2(p^m)$ est un sous-groupe normal de $\Gamma_2(p)$. Montrer que $\Gamma_2(p)/\Gamma_2(p^m)$ est fini, en déterminer le cardinal.

c) Soit p un nombre premier. Montrer que, si u est un élément non nul de L_2, il existe un morphisme ρ de L_2 dans un p-groupe fini dont le noyau ne contient pas u.

1.4 Stabilisateurs

Si le groupe G agit sur l'ensemble X, l'ensemble :

$$G_x = \{g \in G,\ g.x = x\}$$

est un sous-groupe de G appelé *stabilisateur de x*. Notons que le noyau du morphisme ρ associé à l'action n'est autre que

$$\bigcap_{x \in X} G_x.$$

La proposition ci-après, immédiate mais fondamentale, relie les notions d'orbite et de stabiliseur.

Proposition 1. *En associant à la classe de g modulo G_x, l'élément $g.x$ de X, on définit une bijection de l'ensemble quotient G/G_x sur $\omega(x)$. Si G est fini, on a donc :*

$$|G| = |G_x|\ |\omega(x)|.$$

Preuve. Pour $(g, g') \in G^2$ et $x \in X$, on a : $g.x = g'.x \iff g^{-1}g' \in G_x$.

Si l'action est transitive, i.e. si X est un G-espace homogène, la bijection de la proposition 1 identifie X et G/G_x. Un ensemble muni d'une action transitive de G est appelé un *G-espace homogène*.

Applications

1. *Nombre de drapeaux de $\mathbb{F}_q{}^n$*

   Soient E un espace vectoriel de dimension n sur $\mathbb{F}_q$. Le groupe $G = \mathrm{GL}(E)$ agit transitivement sur l'ensemble des drapeaux de E. Le stabilisateur d'un drapeau est le sous-groupe des automorphismes de E dont la matrice dans une base adaptée à ce drapeau est triangulaire supérieure. On en déduit que le nombre de drapeaux de E est

   $$\frac{\prod_{k=0}^{n-1}(q^n - q^k)}{(q-1)^n q^{1+2+\cdots+(n-1)}} = \prod_{j=0}^{n-1}\left(1 + \cdots + q^j\right).$$

2. *Lemme de Cauchy*

   Démontrons le résultat suivant, appelé *lemme de Cauchy*.

   Théorème 7. *Si G est un groupe fini et p un diviseur premier de $|G|$, G contient un élément d'ordre p.*

   On part de l'ensemble :

   $$X = \{(x_1, \ldots, x_p) \in G^p,\ x_1 \ldots x_p = e\},$$

   qui a pour cardinal $|G|^{p-1}$. Si $x = (x_1, \ldots, x_p)$ est dans X, il en est de même de $\tilde{x} = (x_p, x_1, \ldots, x_{p-1})$, ce qui fournit une action du groupe cyclique à p éléments sur X. Les orbites sont de cardinal 1 ou p, et les orbites de cardinal 1 sont les $(x, \ldots, x)$ où $x \in G$ vérifie $x^p = e$. En écrivant que X est réunion disjointe des orbites, on voit alors que p divise le cardinal de $\{x \in G,\ x^p = e\}$, d'où le résultat.

Exercice 20. ③ *Quel est le cardinal de l'ensemble des matrices de rang r de $\mathcal{M}_{m,n}(\mathbb{F}_q)$ si $0 \leq r \leq min(m,n)$?*

Exercice 21. ③ *Dénombrer l'ensemble $\mathcal{S}_n(\mathbb{F}_q)$ des M de $\mathcal{M}_n(\mathbb{F}_q)$ de carré égal à I_n. On observera que, pour r dans $\{0, \ldots, n\}$, l'ensemble des M de $\mathcal{S}_n(\mathbb{F}_q)$ dont l'espace des points fixes est de dimension r est une orbite dans l'action de $GL_n(\mathbb{F}_q)$ sur $\mathcal{M}_n(\mathbb{F}_q)$ par conjugaison.*

Exercice 22. ③ *Dénombrer les matrices nilpotentes d'indice n de $\mathcal{M}_n(\mathbb{F}_q)$.*

Exercice 23. ③ *Montrer que le nombre de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$ est*

$$\sum_{\substack{(n_1,\ldots,n_q)\in\mathbb{N}^q \\ \sum_{i=1}^q n_i = n}} \frac{\prod_{j=0}^{n-1}(q^n - q^j)}{\prod_{i=1}^q \prod_{i_j=0}^{n_j-1}(q^{n_j} - q^{i_j})}.$$

Exercice 24. ③ *Soient E un $\mathbb{F}_q$-espace vectoriel de dimension $n \in \mathbb{N}^*$. Si $1 \leq m \leq n-1$, dénombrer les sous-espaces de dimension m de E.*

Exercice 25. ② *Soit G un groupe abélien fini dont le cardinal n'est divisible par aucun carré de nombre premier. Déduire du lemme de Cauchy que G est cyclique.*

Actions doublement transitives

En vue de l'exercice suivant et d'applications ultérieures, introduisons un peu de terminologie. Une action d'un groupe G sur un ensemble X contenant au moins deux éléments distincts est dite *doublement transitive* si, pour tous couples (x, x') et (y, y') de points distincts de X, il existe g dans G tel que

$$g.x = y, \qquad g.x' = y'.$$

Le résultat suivant est immédiat.

Proposition 2. *L'action de G sur X est doublement transitive si et seulement si l'action de G sur X^2 donnée par*

$$\forall (x, y) \in G^2, \qquad g.(x, y) = (g.x, g.y)$$

a deux orbites, à savoir la diagonale de X^2 et son complémentaire dans X^2.

Exercice 26. ③ *Le groupe G agit sur l'ensemble X ; X contient au moins deux éléments distincts et l'action est doublement transitive. Montrer que, pour tout x de X, G_x est un sous-groupe maximal de G.*

Exercice 27. ③ *Soient $n \in \mathbb{N}^*$, X un ensemble contenant au moins n éléments distincts, G un groupe agissant sur X. On dit que l'action est n fois transitive si l'action naturelle de G sur les n-uplets d'éléments distincts de $\{1, \ldots, n\}$ est transitive.*

a) Supposons $G = \mathcal{S}(X)$. Montrer que l'action naturelle de G sur X est n fois transitive.

b) Pour $x = (x_1, \ldots, x_n) \in X^n$, on définit la relation d'équivalence R_x sur $\{1, \ldots, n\}$ par

$$iR_xj \iff x_i = x_j.$$

Montrer que, dans l'action naturelle de $\mathcal{S}_X$ sur X^n, x et y sont dans la même orbite si et seulement si $R_x = R_y$.

c) On note B_n le nombre de relations d'équivalences sur un ensemble de cardinal n. Montrer que le nombre d'orbites de l'action de G sur X^n est supérieur ou égal à B_n, avec égalité si et seulement si l'action de départ est n fois transitive.

1.5 Conjugaison des stabilisateurs

La remarque ci-après est essentielle.

Proposition 3. *Deux points d'une même orbite ont des stabilisateurs conjugués dans G.*

Preuve. Avec des notations évidentes, $h.(g.x) = g.x \iff h \in gG_xg^{-1}$.

Voici une conséquence immédiate.

Proposition 4. *Si le groupe G est abélien et l'action transitive, tous les points de X ont même stabilisateur. Si de plus l'action est fidèle, les stabilisateurs sont réduits à $\{e\}$ et toute orbite est en bijection avec G.*

Application *Cardinal maximal d'un sous-groupe abélien de $\mathcal{S}_n$*

Nous allons déterminer le cardinal maximal d'un sous-groupe abélien de $\mathcal{S}_n$. Soit G un tel sous-groupe. On commence par noter que si $X_1, \ldots, X_r$ sont les orbites distinctes de l'action de G sur $X = \{1, \ldots, n\}$, l'application :

$$\sigma \mapsto (\sigma_{|X_1} \ldots \sigma_{|X_r})$$

est un morphisme injectif de G dans $\mathcal{S}(X_1) \times \cdots \times \mathcal{S}(X_r)$ dont l'image est contenue dans un produit $G_1 \times \cdots \times G_r$, où G_i est pour tout i un sous-groupe abélien de $\mathcal{S}(X_i)$ agissant transitivement sur X_i. Or, la proposition 4 montre qu'un sous-groupe abélien de $\mathcal{S}_m$ agissant transitivement sur $\{1, \ldots, m\}$ est de cardinal m. En reprenant les notations ci-dessus, on voit donc que $|G|$ est majoré par $\prod_{i=1}^{r} |X_i|$, a fortiori par α_n, où α_n est le maximum des produits $\prod_{i=1}^{r} m_i$ où r et les m_i sont dans $\mathbb{N}^*$ et la somme des m_i vaut n.

Ce majorant est optimal : en prenant un r-uplet $(m_1, \ldots, m_r)$ réalisant α_n, une partition de X en r ensembles $X_1, \ldots, X_r$ de cardinaux respectifs $m_1, \ldots, m_r$ et, pour tout i, un m_i-cycle γ_i de support X_i, le sous-groupe de $\mathcal{S}_n$ engendré par $\gamma_1, \ldots, \gamma_r$ est abélien de cardinal α_n. Il existe d'ailleurs d'autres sous-groupes abéliens de $\mathcal{S}_n$ de cardinal α_n : par exemple $\mathcal{V}_4$ dans $\mathcal{S}_4$.

Théorème 8. *Le cardinal maximal d'un sous-groupe abélien de $\mathcal{S}_n$ est α_n.*

Il reste pour conclure à préciser α_n. On vérifie que $\alpha_1 = 1$ et que, pour $n \geq 2$:

$$\alpha_n = \begin{cases} 3^{n/3} & \text{si} \quad n \equiv 0\ [3] \\ 4.3^{(n-4)/3} & \text{si} \quad n \equiv 1\ [3] \\ 2.3^{(n-2)/3} & \text{si} \quad n \equiv 2\ [3] \end{cases}$$

Exercice 28. ③*Vérifier ce dernier point.*

Il existe un analogue du théorème 8 pour les sous-groupes résolubles de $\mathcal{S}_n$.

1.6 La formule de Cauchy-Frobenius-Burnside

Pour g dans G, on note

$$\text{Fix } (g) = \{x \in X,\ g.x = x\}$$

l'ensemble des points fixes de G.

Dans ce paragraphe, le groupe fini G agit sur l'ensemble fini X. La proposition ci-après est souvent attribuée à Burnside ; elle était en fait connue de Frobenius et, en substance, de Cauchy. Elle exprime le nombre d'orbites de l'action d'un groupe fini sur un ensemble fini en fonction des cardinaux des ensembles Fix (g), dont le calcul est souvent accessible[10].

Proposition 5. *Si G et X sont finis, le nombre d'orbites de l'action est :*

$$\frac{1}{|G|} \sum_{g \in G} |\mathit{Fix}\ (g)|.$$

10. Cette formule a été complétée par Polya en une jolie théorie que nous n'aborderons pas ici.

Preuve. En dénombrant de deux façons l'ensemble

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

on voit que :

$$\sum_{g\in G} |\text{Fix } (g)| = \sum_{x\in X} |G_x|.$$

Grâce à la proposition 2, cette somme est égale à

$$|G| \sum_{x\in X} \frac{1}{|\omega(x)|}.$$

Or, la somme des $1/|\omega(x)|$ pour x décrivant une orbite fixée vaut 1. Il s'ensuit que la somme

$$\sum_{x\in X} \frac{1}{|\omega(x)|}$$

est égale au nombre d'orbites, d'où le résultat.

Exemples

1. *Le problème des colliers de Polya*

   On se donne deux entiers n et q de $\mathbb{N}^*$, une liste de q couleurs. On cherche le nombre de colliers que l'on peut construire en enfilant régulièrement n perles ayant les couleurs choisies sur un cercle, deux colliers étant considérés comme égaux lorsqu'ils se déduisent l'un de l'autre par rotation. On formalise en notant $X = \{1, \ldots, q\}$ et en faisant agir U_n sur $\mathcal{F}(U_n, X)$ en posant, pour u dans U_n, f dans $\mathcal{F}(U_n, X)$, z dans U_n :

   $$u.f(z) = f(uz).$$

   Le nombre recherché est le nombre d'orbites de l'action ainsi définie. Pour le calculer, on applique la proposition 5 en notant que pour tout diviseur d de n et tout ω de U_n d'ordre d, on a $|\text{Fix } (u)| = q^{\frac{n}{d}}$ (un élément de Fix (u) est déterminé par les images des éléments d'une classe de U_n modulo le sous-groupe engendré par u). Comme il y a $\varphi(d)$ éléments d'ordre d dans U_n, le nombre recherché est :

   $$\frac{1}{n} \sum_{d|n} \varphi(d) q^{\frac{n}{d}}.$$

2. *Un théorème de Jordan*

   Le groupe fini G agit transitivement sur X, où l'ensemble X est fini de cardinal ≥ 2. Montrons l'existence de $g \in G$ tel que Fix $(g) = \emptyset$. La proposition 5 donne :

   $$\sum_{g\in G} |\text{Fix } (g)| = |G|.$$

   Comme Fix $(e) = |X| > 1$, il suit de l'égalité précédente qu'existe g dans G tel que Fix $(g) = 0$. C'est l'assertion désirée. Formulons le résultat.

   Théorème 9. *Si le groupe fini G agit transitivement sur un ensemble fini de cardinal ≥ 2, il existe au moins un élément qui agit sans point fixe.*

Par exemple, si P est un polynôme irréductible séparable de $\mathbb{K}[X]$, il existe au moint un élément de $\mathrm{Gal}_{\mathbb{K}}(P)$ qui ne fixe aucune racine.

3. *La borne de Cameron-Cohen*

Cameron et Cohen ont établi l'amélioration suivante du théorème 9 (1983).

Théorème 10. *Soient G un groupe fini agissant transitivement sur un ensemble fini X de cardinal $n \geq 2$, Γ l'ensemble des éléments de G agissant sans point fixe. Alors*

$$\frac{|\Gamma|}{|G|} \geq \frac{1}{n}.$$

Preuve. Pour g dans G, notons $N(g)$ le cardinal de Fix (g). Le point de départ est l'action naturelle de G sur X^2, donnée par :

$$\forall (g, x, x') \in G \times X \times X, \quad g.(x, x') = (g.x, g.x')\,.$$

Si $N_2(g)$ le nombre de points fixes de l'élément g de G dans cette action, il est immédiat que

$$N_2(g) = N(g)^2.$$

D'autre part, la moyenne

$$\frac{1}{|G|} \sum_{g \in G} N_2(g)$$

est le nombre d'orbites de l'action de G sur X^2. Puisque la diagonale

$$\Delta = \{(x, x),\ x \in G\}$$

est stable, le nombre d'orbites de cette action est supérieur ou égal à 2, avec égalité si et seulement si l'action de G sur X est doublement transitive (proposition 1). [11] Au total, on a l'inégalité :

$$\frac{1}{|G|} \sum_{g \in G} N_2(g) \geq 2,$$

avec égalité si et seulement si l'action de G sur X est doublement transitive. Formons la quantité

$$\tau = \frac{1}{|G|} \sum_{g \in G} (n - N(g))\ (N(g) - 1)\,.$$

Pour g dans Γ,

$$(n - N(g))\ (N(g) - 1) = -n,$$

alors que, pour g dans $G \setminus \Gamma$,

$$(n - N(g))\ (N(g) - 1) \geq 0.$$

Par conséquent :

$$\tau \geq -n \frac{|\Gamma|}{|G|}.$$

11. Formulation probabiliste : la variance du nombre de points fixes est supérieure ou égale à 1, avec égalité si et seulement si l'action est dublement transitive.

Mais, d'autre part,

$$\tau = \frac{1}{|G|}\sum_{g\in G}\left(-N(g)^2 + (n+1)N(g) - n\right) \leq -2 + (n+1) - n,$$

c'est-à-dire

$$\tau \leq -1.$$

Le théorème s'en déduit.

La démonstration précédente montre que l'inégalité du théorème 9 est une égalité si et seulement si l'action de G sur X est doublement transitive et si, pour g dans $G \setminus \Gamma$, $N(g)$ vaut 1 ou n. Si on suppose l'action de G sur X fidèle, cette condition revient à dire que l'action est doublement transitive et que tout élément autre que e agit avec au plus un point fixe. Tel est par exemple le cas pour l'action naturelle du groupe affine $G = \mathrm{Aff}_1(\mathbb{F}_q)$ sur $X = \mathbb{F}_q$: les éléments de Γ sont les translations autres que l'identité, donc :

$$|\Gamma| = q - 1 = \frac{|G|}{|X|}.$$

On peut en fait étudier plus avant le cas d'égalité et montrer que $\Gamma \cup \{1\}$ est, dans ce cas, un sous-groupe de G.

4. *Sous-groupes finis de $SO_3(\mathbb{R})$: principe de la classification*

Soit G un sous-groupe fini de $\mathrm{SO}_3(\mathbb{R})$. Soit X l'ensemble des points de la sphère unité S^2 de $\mathbb{R}^3$ qui sont point fixe d'un élement de $G \setminus \{I_3\}$ (c'est-à-dire appartiennent à l'axe de cet élément). Le groupe G stabilise X. Notons $x_1, \ldots, x_r$ un système de représentants de la relation d'équivalence associée à l'action. En écrivant que les orbites des x_i pour $1 \leq i \leq r$ partitionnent X, on a

$$(1) \qquad |X| = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}, \qquad \frac{|X|}{|G|} = \sum_{i=1}^{r} \frac{1}{|G_{x_i}|}.$$

Par ailleurs, puisqu'un élément de $G \setminus \{I_3\}$ a exactement deux points fixes dans X, la proposition 5 fournit

$$(2) \qquad r = \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}\ (g)| = \frac{1}{|G|}\left(2(|G|-1) + |X|\right) = 2 - \frac{2}{|G|} + \frac{|X|}{|G|}.$$

Au total :

$$\sum_{i=1}^{r} \frac{1}{|G_{x_i}|} = r - 2 + \frac{2}{|G|}, \qquad \sum_{i=1}^{r}\left(1 - \frac{1}{|G_{x_i}|}\right) = 2 - \frac{2}{|G|}.$$

La dernière relation met en évidence que les possibilités pour r et les $|G_{x_i}|$ sont limitées : dès que $|G_{x_i}|$ est grand, le terme

$$1 - \frac{1}{|G_{x_i}|}$$

est proche de 1. Précisons. D'abord, puisque chaque G_{x_i} est de cardinal au moins 2, la dernière relation impose

$$2 > 2 - \frac{2}{|G|} \geq \frac{r}{2}, \qquad r \leq 3.$$

Il faut ensuite analyser plus finement la situation. Si $r = 2$, on voit en reprenant (2) que $|X| = 2$. Ainsi $G \setminus \{I_3\}$ est formé de rotations ayant toutes même axe, donc G est isomorphe à un sous-groupe de $\mathrm{SO}_2(\mathbb{R})$ donc cyclique. Si $r = 3$, on montre facilement que les triplets donnant les cardinaux des trois orbites rangés dans l'ordre croissant sont de l'une des formes

$$(2, 2, n), \qquad (2, 3, 3), \qquad (2, 3, 4), \qquad (2, 3, 5).$$

Le cardinal de G est alors respectivement $2n$, 12, 24, 60. Le premier cas correspond à un groupe diédral, les trois derniers aux groupes d'isométries directes de polyèdres réguliers. La discussion n'est pas difficile mais longue. Elle aboutit à la classification complète, à conjugaison dans $\mathrm{SO}_3(\mathbb{R})$ près, des sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$, due en substance à Jordan.

Exercice 29. ③ *a) Si G agit sur l'ensemble X et si g et g' sont des éléments conjugués de G, vérifier que Fix (g) et Fix (g') sont équipotents.*

b) Les notations sont celles de la proposition 5. Notons $C_1, \ldots, C_r$ les classes de conjugaison de G. Pour $1 \leq i \leq r$, soit g_i un élément de C_i. Montrer que le nombre d'orbites de G sur X est

$$\frac{1}{|G|} \sum_{i=1}^{r} |C_i| \, |Fix\ (g_i)|.$$

Exercice 30. ④ *Reprendre le problème des colliers mais en considérant également comme équivalents deux colliers qui se déduisent l'un de l'autre par symétrie, c'est-à-dire en remplaçant $\mathbb{Z}/n\mathbb{Z}$ par le groupe diédral $\mathcal{D}_n$.*

Exercice 31. ③ *a) Déterminer le nombre moyen de points fixes d'un élément de $\mathcal{S}_n$?*

b) On fixe k dans $\{1, \ldots, n\}$. Quel est le nombre moyen de k-cycles d'un élément de $\mathcal{S}_n$?

Exercice 32. ③ *Déterminer le nombre moyen de sous-espaces vectoriels de dimension d stables par un élément de $GL_n(\mathbb{F}_q)$ si $0 \leq d \leq n$, puis le nombre moyen de sous-espaces vectoriels stables par un élément de $GL_n(\mathbb{F}_q)$.*

Exercice 33. ② *Déduire le petit théorème de Fermat du problème des colliers.*

Exercice 34. ③ *Pour σ dans $\{1, \ldots, n\}$, notons $c(\sigma)$ le nombre d'orbites de l'action de σ sur $\{1, \ldots, n\}$. Si G est un sous-groupe de $\mathcal{S}_n$, montrer que le nombre de parties de $\{1, \ldots, n\}$ stables par G est*

$$\frac{1}{|G|} \sum_{\sigma \in G} 2^{c(\sigma)}.$$

Exercice 35. ③ *Soit G un groupe fini d'ordre n, r le nombre de classe de conjugaison de G, c le nombre de couples (x, y) de G^2 tels que $xy = yx$. Montrer que $c = rn$.*

Exercice 36. ② *Les notations sont celles des théorèmes 8 et 9. Montrer, en reprenant la démonstration du théorème 8, que $|\Gamma| \geq n - 1$.*

Exercice 37. ③ *Soit, pour $n \in \mathbb{N}$, B_n le nombre de relations d'équivalence sur un ensemble de cardinal n (avec, par convention $B_0 = 1$).*

a) Montrer, pour $n \in \mathbb{N}$, la relation $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$.

b) Calculer B_n si $n \leq 6$. Déterminer la somme de la série formelle $\sum_{k=0}^{n} \frac{B_n}{n!} X^n$.

c) Le groupe fini G agit sur un ensemble fini X de cardinal supérieur ou égal à n. Montrer que

$$\frac{1}{|G|} \sum_{g \in G} N(g)^n \leq B_n,$$

avec égalité si et seulement si l'action est n fois transitive.

2 Applications à la théorie des groupes

Dans cette seconde partie, on présente quelques applications de la notion d'action à la théorie des groupes, plus spécifiquement à la théorie des groupes finis. On regroupe les considérations liées aux actions par translation dans les trois premiers paragraphes, celles liées à la conjugaison dans les suivants. Cette organisation est très arbitraire : la notion de conjugaison, déjà présente dans la proposition 3 réapparaît évidemment dans les paragraphes **2.2** et **2.3**.

On trouvera ici des théorèmes centraux (centre d'un p-groupe, premier théorème de Sylow) aussi bien que des résultats esthétiques mais plus périphériques (minoration du cardinal d'un groupe fini en fonction de son nombre de classes de conjugaison, entiers n tels que tout groupe de cardinal n soit cyclique).

2.1 Action de G sur lui-même par translation

On peut faire agir G sur lui-même par translation en posant

$$\forall (g, x) \in G \times G, \qquad g.x = gx.$$

Le morphisme associé associe à g la translation à gauche par g. Il est clairement injectif, ce qui donne l'énoncé suivant, dû à Cayley.

Proposition 6. *L'action de G sur lui-même par translation identifie G à un sous-groupe de $\mathcal{S}(G)$.*

Ainsi, un groupe fini de cardinal n peut être vu comme un sous-groupe de $\mathcal{S}_n$. La représentation de G dans $\mathcal{S}(G)$ donnée par la proposition 6 est appelée *représentation régulière de G*. Le procédé consistant à transformer un élément en application a bien d'autres applications en mathématiques.

Exercice 38. ③ *Soient G un groupe fini, ρ la représentation régulière de G.*

a) Si $g \in G$, quelle est la signature de $\rho(g)$?

b) À quelle condition $\rho(G)$ est-il contenu dans $\mathcal{A}(G)$?

c) On suppose $|G|$ congru à 2 modulo 4. Montrer que G admet un sous-groupe normal d'indice 2, donc que G n'est pas simple.

Exercice 39. ⑤ *a) Soit ρ la représentation régulière de G. Montrer que si g_1 et g_2 sont deux éléments de G de même ordre, fini ou infini, $\rho(g_1)$ et $\rho(g_2)$ sont conjugués dans $\mathcal{S}(G)$.*

b) Montrer qu'il existe un groupe $\tilde{G}$ contenant G (à isomorphisme près) et tels que deux éléments de même ordre de $\tilde{G}$ soient conjuguées dans $\tilde{G}$.

Exercice 40. ④ *Soient n un élément de $\mathbb{N}^*$, G un groupe fini. Montrer l'équivalence entre les deux conditions suivantes :*

- G se plonge dans $\mathcal{S}_n$;

- il existe un entier $m \geq 1$, m sous-groupes $G_1, \ldots, G_m$ de G tels que

$$\sum_{i=1}^{m} |G/G_i| \leq n, \qquad \bigcap_{i=1}^{m} \left(\bigcap_{g \in G} g G_i g^{-1} \right) = \{e\}.$$

2.2 Action de G sur G/H par translation

Nous allons généraliser la construction du paragraphe précédent.

Soit H un sous-groupe du groupe G. Rappelons que l'ensemble quotient G/H est l'ensemble des classes à droite de G modulo H, c'est-à-dire des parties de la forme

$$gH, \qquad g \in G.$$

Attention, « G/H n'est pas un groupe ». Précisément, pour que l'on puisse munir G/H d'une structure de groupe « naturelle » (c'est-à-dire telle que la surjection canonique de G sur G/H soit un morphisme), il faut et il suffit que H soit normal dans G.

L'ensemble G/H a été utilisé dans la preuve du théorème de Lagrange, ce qui conduit à poser

$$\forall (g, x) \in G^2, \qquad g.xH = gxH.$$

On définit ainsi une action transitive de G sur l'ensemble quotient G/H. Le stabilisateur de xH est xHx^{-1}, qui est le *conjugué de H par x*.

En particulier : $G_H = H$. Notant ρ_H le morphisme de G dans $\mathcal{S}(G/H)$ associé, on a donc

$$\ker \rho_H = \bigcap_{x \in G} xHx^{-1}.$$

Le sous-groupe $\ker \rho_H$, noté H_G dans la suite, est appelé *coeur de H dans G* ; il est normal dans G (comme noyau d'un morphisme), contenu dans H avec égalité si et seulement si H est normal dans G. On a ainsi établi la :

Proposition 7. *L'action de G sur G/H par translation identifie G/H_G à un sous-groupe transitif de $\mathcal{S}(G/H)$, H/H_G à un sous-groupe de $\mathcal{S}((G/H) \setminus \{H\})$.*

Exemple *Le quotient $\mathcal{S}_4/\mathcal{V}$*

Prenons $G = \mathcal{S}_4$, $H = \mathcal{V}$ (exemple 2, paragraphe **1.3**). Alors H est normal dans G et la proposition donne un morphisme injectif de G/H dans $\mathcal{S}_3$. Par égalité des cardinaux, on retrouve que $\mathcal{S}_4/\mathcal{V}$ est isomorphe à $\mathcal{S}_3$.

Exercice 41 (F)**.** *Soient H et K deux sous-groupes de G d'indices finis respectifs h et k. Montrer que $G/(H_G \cap K_G)$ se plonge dans $\mathcal{S}_{h+k}$.*

Exercice 42 (M)**.** *Soit G un groupe admettant deux sous-groupes d'indice 2 distincts. Montrer que G a un quotient isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$, puis que G admet au moins trois sous-groupes d'indice 2.*

Quoique très simple, la proposition 7 a beaucoup d'applications. Nous en donnerons deux (les propositions 8 et 9), la première étant prolongée par quelques exercices.

Proposition 8. *Supposons que H est un sous-groupe d'indice fini m de G. Alors H_G est un sous-groupe normal de G d'indice divisant $m!$.*

Ainsi, si G contient au moins $m! + 1$ éléments, G n'est pas simple. Tel est en particulier le cas si G est infini.

Exemple *Nombre de sous-groupes d'indice donné d'un groupe de type fini*

Soient G un groupe possédant une partie génératrice de cardinal $n \in \mathbb{N}^*$, m un élément de $\mathbb{N}^*$. À tout sous-groupe H d'indice m de G, on associe une action transitive de G sur G/H, action pour laquelle H est le stabilisateur de la classe H de e dans G/H.

Réciproquement, pour une action transitive de G sur un ensemble X de cardinal m, les stabilisateurs des éléments de X sont des sous-groupes de G (deux à deux conjugués) d'indice m. Ces arguments montrent que le nombre $N_m(G)$ de sous-groupes d'indice m de G est fini. Plus précisément, si $A'_m(G)$ est le nombre d'actions transitives de G sur un ensemble de cardinal m [12], on a

$$N_m(G) = \frac{A'_m(G)}{(m-1)!}.$$

Exercice 43. ④ *Si G est un groupe simple qui n'est pas cylique d'ordre premier, montrer que G n'a pas de sous-groupe d'indice ≤ 4. On rappelle qu'un groupe simple non cyclique d'ordre premier est de cardinal supérieur ou égal à 60.*

Exercice 44. ③ *Soit G un groupe de cardinal 6. Déduire du lemme de Cauchy et de l'action de G sur G/H par translation que G est soit cyclique soit isomorphe à $\mathcal{S}_3$.*

Le résultat de l'exercice suivant est dû à Baer.

Exercice 45. ③ *Soient $(m, n) \in \mathbb{N}^{*2}$, G un groupe admettant une partie génératrice de cardinal n.*

a) Montrer que l'ensemble des sous-groupes normaux de G d'indice au plus m est fini, de cardinal majoré par $(m!)^n$.

b) Montrer que l'ensemble des sous-groupes de G d'indice m est fini ; majorer son cardinal par une quantité ne dépendant que de m et n.

12. Introduit dans l'exemple 8 de **1.2**

Exercice 46. ④ *Montrer que $\mathcal{S}_n$ est isomorphe à un sous-groupe de $\mathcal{A}_{n+2}$ mais que, si $n \geq 3$, que $\mathcal{S}_n$ n'est pas isomorphe à un sous-groupe de $\mathcal{A}_{n+1}$.*

La seconde application généralise le fait simple et classique selon lequel un sous-groupe d'indice 2 d'un groupe est normal. La preuve de la généralisation est moins naïve que celle de ce cas particulier, mais découle simplement des considérations de ce paragraphe.

Proposition 9. *Si G est un groupe fini et p le plus petit diviseur premier de $|G|$, tout sous-groupe d'indice p de G est normal dans G.*

Preuve. Soit H un sous-groupe d'indice p de G. Il suffit de montrer que $H = H_G$, ou encore, vu que $H_G \subset H$, que H_G est d'indice au plus p dans G. Mais l'indice en question divise $|G|$ et $p!$, donc p.

2.3 Classification des actions

Ce paragraphe, non utilisé dans la suite, est consacré à la classification des actions. Introduisons pour commencer un peu de vocabulaire.

Morphisme et isomorphisme de G-ensembles

On se donne donc deux G-ensembles X et X'. On appelle *morphisme de G-ensemble* de X dans X' toute application σ de X dans X' telle que

$$\forall (g,x) \in G \times X, \qquad \sigma(g.x) = g.\sigma(x).$$

Si on note ρ et ρ' les morphismes de G respectivement dans $\mathcal{S}(X)$ et $\mathcal{S}(X'$ associés aux deux actions, la condition précédente s'écrit :

$$\forall g \in G, \qquad \sigma \circ \rho(g) = \rho'(g) \circ \sigma.$$

Si σ est une bijection de X sur X', on dit que σ est un *isomorphisme de G-ensembles*, ou encore une *équivalence d'action*.

Dire qu'il existe un isomorphisme de G-ensembles de X sur X', c'est dire que G agit « de la même façon » sur X et X'. Avec les notations précédentes, l'application σ s'interprète comme un changement de coordonnées et on a, entre autres, les faits suivants :

- l'application σ transporte les orbites de la première action sur celles de la seconde,

- le stabilisateur de l'élément x de X pour ρ est égal au stabilisateur de $\sigma(x)$ pour ρ'.

Si les actions sont transitives, une application u vérifiant la condition de la définition est appelée *isomorphisme de G-espaces homogènes*.

Universalité de l'action de G sur G/H par translation

La proposition immédiate ci-après explicite en quoi l'action de G sur G/H par translation est universelle.

Proposition 10. *Si G agit transitivement sur X et si $x \in X$, l'action est équivalente à celle de G sur G/G_x par translation.*

En développant la proposition 10, on obtient une description « théorique » des G-espaces homogènes, qui montre l'équivalence entre l'étude des actions transitives de G et celle des classes de conjugaison de sous-groupes de G.

Proposition 11. *i) Tout G-espace homogène est isomorphe à un espace G/H où H est un sous-groupe de G.*

ii) Si H et H' sont deux sous-groupes de G, les G-espaces homogènes G/H et G/H' sont isomorphes si et seulement si H et H' sont conjugués dans G.

Preuve. Le premier point est la proposition 10. Notons maintenant ρ_H et $\rho_{H'}$ les morphismes associés aux actions de G sur G/H et G/H' respectivement. Si $H' = a^{-1}Ha$ avec $a \in G$, le stabilisateur de aH' pour $\rho_{H'}$ est $aH'a^{-1} = H$. Grâce à la proposition 10, $\rho_{H'}$ est équivalente à ρ_H.

Supposons réciproquement les G-espaces homogènes G/H et G/H' isomorphes, On dispose d'une bijection u de G/H sur G/H' telle que

$$\forall g \in G, \qquad u \circ \rho_H(g) = \rho_{H'}(g) \circ u.$$

Mais alors H, qui est le stabilisateur de l'élément H de G/H pour ρ_H est égal au stabilisateur de $u(H)$ pour $\rho_{H'}$. Posant $u(H) = aH'$, ce second stabilisateur n'est autre que $aH'a^{-1}$: H et H' sont conjugués.

Il y a donc, à équivalence près, autant d'actions transitives de G que de classes de conjugaison de sous-groupes de G. Ainsi, si G est fini de cardinal m et si, pour $1 \leq i \leq m$, a_i est le nombre de classes de conjugaison de sous-groupes d'indice i de G, le nombre de classes d'actions non équivalentes de G sur un ensemble X de cardinal n est le nombre u_n de $(x_1, \ldots, x_m) \in \mathbb{N}^m$ tels que :

$$\sum_{i=1}^{m} a_i x_i = n.$$

On calcule facilement la série génératrice des u_n :

$$F = \sum_{n=0}^{+\infty} u_n X^n = \prod_{i=1}^{m} \frac{1}{1 - X^{a_i}}.$$

On notera que $a_1 = 1$, de sorte que tous les pôles de F autre que 1 sont de multiplicité $< m - 1$, 1 étant quant à lui de multiplicité m, le coefficient de $1/(X-1)^m$ valant $\gamma = \frac{(-1)^m}{\prod_{i=1}^m a_i}$.

Exercice 47. ③ *Donner un équivalent de u_n lorsque n tend vers $+\infty$.*

Quand deux G-ensembles finis sont-ils isomorphes ?

Nous allons maintenant établir un critère permettant de décider si deux G-ensembles finis sont isomorphes. L'outil essentiel est la généralisation suivante des ensembles Fix (g). Si Γ est une partie de G, on note

$$X^\Gamma = \{x \in X,\ \forall g \in \Gamma,\ g.x = x\} = \bigcap_{g \in \Gamma} \text{Fix } (g).$$

Il est clair que, si $\langle \Gamma \rangle$ désigne le sous-groupe de G engendré par Γ, on a

$$X^\Gamma = X^{\langle \Gamma \rangle}.$$

Théorème 11. *Soient X et X' deux G-ensembles finis. Les assertions suivantes sont équivalentes :*

(i) les G-ensembles X et X' sont isomorphes ;

(ii) pour tout sous-groupe H de G, on a

$$|X^H| = |X'^H|.$$

Preuve. Si σ est un isomorphisme de G-ensembles de X sur X', on a, pour tout sous-groupe H de G :

$$\sigma(X^H) = X'^H.$$

L'implication (i) $\Rightarrow$ (ii) en découle.

Observons d'abord que (ii) implique, en prenant $H = \{e\}$, l'égalité

$$|X| = |X'|.$$

On montre alors l'implication (ii) $\Rightarrow$ (i) en raisonnant par récurrence sur $|X|$. Le cas où $|X| = 1$ est trivial. Supposons le résultat vrai si $|X| \leq n-1$, où $n \geq 2$ est un entier et considérons deux G-ensembles X et X' de cardinal n vérifiant (ii). Soit H un sous-groupe de G tel que

$$X^H \neq \emptyset$$

et de cardinal maximal parmi les sous-groupes de G possédant cette propriété. Soit x dans X^H. On a $H \subset G_x$, d'où par maximalité

$$H = G_x.$$

Si x' est un élément de X'^H, on a de même

$$H = G_{x'}.$$

Les deux espaces homogènes $\omega(x)$ et $\omega(x')$ sont donc tous deux isomorphes à G/H, ce qui montre l'existence d'une bijection σ_1 de $\omega(x)$ sur $\omega(x')$ vérifiant

$$\forall (g, y) \in G \times \omega(x), \qquad \sigma_1(g.y) = g.\sigma_1(y).$$

Mais alors $X \setminus \omega(x)$ et $X' \setminus \omega(x')$ sont deux G-espaces vérifiant l'hypothèse (ii) et de cardinaux inférieurs ou égaux à $n-1$. Il existe donc une bijection σ_2 de $X \setminus \omega(x)$ sur $X' \setminus \omega(x')$ telle que

$$\forall (g, y) \in G \times (X \setminus \omega(x)), \qquad \sigma_2(g.y) = g.\sigma_2(y).$$

L'application de X dans X' coïncidant avec σ_1 sur $\omega(x)$, avec σ_2 sur $X \setminus \omega(x)$ est un isomorphisme de G-ensembles de X sur X'.

2.4 Le premier théorème de Sylow

Le théorème de Lagrange admet-il une réciproque ? Autrement dit, étant donnés un groupe fini G de cardinal n et un diviseur d de n, existe-t-il un sous-groupe fini de G de cardinal d ?

La réponse est non en général. Ainsi, le groupe $\mathcal{A}_4$ n'admet pas de sous-groupe de cardinal 6. En effet, un tel sous-groupe G serait d'indice 2, donc normal dans $\mathcal{A}_4$. Il contiendrait tous les carrés d'éléments de $\mathcal{A}_4$ (quotient de cardinal 2), donc tous les 3-cycles. Comme les 3-cycles engendrent $\mathcal{A}_4$, G serait finalement égal à $\mathcal{A}_4$, contradiction.

Exercice 48. ③ *En utilisant le théorème de structure des groupes abéliens finis, montrer que, si G est un groupe abélien d'ordre n et d un diviseur de n, alors G contient un sous-groupe d'ordre d.*

Si G est un groupe fini, p un nombre premier divisant $|G|$, le lemme de Cauchy établi dans le paragraphe **1.4** montre que G contient un élément d'ordre p. Le premier théorème de Sylow en est une généralisation très substantielle.

Théorème 12. *Soient G un groupe fini, p un nombre premier divisant $|G|$, m la p-valuation de $|G|$. Il existe un sous-groupe de G de cardinal p^m.*

Preuve. Faisons agir G sur l'ensemble X_m de ses parties de cardinal p^m par translation :

$$\forall (g,P) \in G \times X_j, \qquad g.P = gP = \{g.x,\ x \in P\}\,.$$

Le stabilisateur de l'élément P de X_m est

$$G_P = \bigcap_{x \in P} Px^{-1}.$$

En particulier, ce stabilisateur est contenu dans un translaté à droite de P et est donc de cardinal majoré par p^m. Nous allons montrer qu'il existe P dans X_m tel que

$$(1) \qquad \frac{|G|}{|G_P|} \wedge p = 1, \qquad \text{i.e.} \quad |\omega(P)| \wedge p = 1.$$

Si tel est le cas, $|G_P|$, simultanément divisible par p^m et majoré par p^m, est égal à p^m ; G_P est un sous-groupe de G de cardinal p^m.

Pour montrer qu'existe P dans X_m vérifiant (1), il suffit, puisque X_m se partitionne en orbites $\omega(P)$, de montrer que $|X_m|$ n'est pas divisible par p. Or,

$$|X_m| = \binom{n}{p^m}.$$

La démonstration est alors réduite à un petit exercice d'arithmétique. Rappelons la *formule de Legendre* : si v_p est la fonction « valuation p-adique », on a

$$\forall k \in \mathbb{N}^*, \qquad v_p(k!) = \sum_{r=1}^{+\infty} \left\lfloor \frac{k}{p^r} \right\rfloor,$$

la somme du second membre étant évidemment finie.

Revenons à la démonstration. Posant $n = p^m u$ où u est un entier naturel premier à p, il s'agit de prouver que la p-valuation de $\binom{n}{p^m}$ est nulle. Or, la formule de Legendre entraîne

$$v_p\left(\binom{n}{p^m}\right) = v_p(n!) - v_p((n-p^m)!) - v_p((p^m)!),$$

somme qui est aussi égale à

$$\sum_{r=1}^{+\infty} \left(\left\lfloor up^{m-r} \right\rfloor - \left\lfloor (u-1)\, p^{m-r} \right\rfloor - \left\lfloor p^{m-r} \right\rfloor\right).$$

Montrons que chaque terme de la somme est nul, ce qui amènera la conclusion désirée. Pour $r \leq m$, on a

$$\left\lfloor up^{m-r} \right\rfloor - \left\lfloor (u-1)\, p^{m-r} \right\rfloor - \left\lfloor p^{m-r} \right\rfloor = up^{m-r} - (u-1)\, p^{m-r} - p^{m-r} = 0.$$

Pour $r > m$, on note $d = \lfloor up^{m-r} \rfloor$. Puisque up^{m-r} est une fraction non entière de dénominateur p^{r-m}, on a

$$d + (p-1)p^{m-r} \geq u\, p^{m-r} \geq d + p^{m-r},$$

ce qui entraîne

$$(u-1)p^{m-r} \geq d, \quad \left\lfloor (u-1)p^{m-r} \right\rfloor = d, \quad \left\lfloor up^{m-r} \right\rfloor - \left\lfloor (u-1)\, p^{m-r} \right\rfloor - \left\lfloor p^{m-r} \right\rfloor = 0.$$

Remarques

1. *Sous-groupes de cardinal primaire*
   Si p est premier et m dans $\mathbb{N}^*$, on peut montrer que tout groupe de cardinal p^m contient, pour tout i de $\{0, \ldots, m\}$, au moins un sous-groupe de cardinal p^i. En combinant ce résultat au théorème 12, on voit que « la réciproque du théorème de Lagrange » est vraie pour un diviseur primaire de $|G|$. L'exercice 42 propose un raffinement de ce dernier point.
2. *Les théorèmes de Sylow*
   Si p est un nombre premier et G un groupe fini, appelons p-Sylow de G tout sous-groupe de G de cardinal $p^{v_p(|G|)}$. Le premier théorème de Sylow assure que G admet au moins un p-Sylow. Le second théorème de Sylow dit que les p-Sylow de G sont conjugués, ce qui implique (action par conjugaison) que leur nombre divise $|G|$. Le troisième précise le premier : le nombre de p-Sylow est congru à 1 modulo p. Il y a de nombreuses preuves des théorèmes de Sylow. La plupart reposent sur une utilisation ingénieuse des actions.

Exercice 49. ⑤ *Les notations sont celles du théorème 12, j est un élément de $\{1, \ldots, m\}$. On montre ici que le nombre $n_G(p^j)$ de sous-groupes de G de cardinal p^j est congru à 1 modulo p, ce qui est une généralisation due à Frobenius du troisième théorème de Sylow.*

Soit X_j l'ensemble des parties de G de cardinal p^j. On fait agir G sur X_j par translation à gauche.

a) Soient $P \in X_j$ et G_P le stabilisateur de A pour l'action précédente. Montrer que $|G_P| \leq p^j$, et qu'il y a égalité si et seulement si P est une classe à droite selon un sous-groupe de cardinal p^j.

b) Déduire de a) que :

$$\binom{n}{p^j} \equiv up^{m-j} n_G(p^j) \ \left[p^{m-j+1}\right].$$

c) Conclure. Pour éviter des calculs de valuations, on pourra appliquer la question précédente au cas particulier des groupes cycliques.

Exercice 50. ③ *Soient p un nombre premier, n un élément de $\mathbb{N}^*$. Montrer que le groupe des matrices triangulaires supérieures à termes diagonaux égaux à 1 est un p-Sylow de $GL_n(\mathbb{F}_p)$.*

Exercice 51. ⑤ *Soient p un nombre premier, n dans $\mathbb{N}$. Construire un p-Sylow de $\mathcal{S}_n$, d'abord si $p \leq n < p^2$, puis si $n = p^2$.* [13]

2.5 Action de G sur lui-même par conjugaison

Si G est un groupe, G agit sur lui-même par conjugaison en posant

$$\forall (g, x) \in G^2, \qquad g.x = gxg^{-1}.$$

L'orbite de x est la classe de conjugaison $\mathrm{Conj}_G(x)$ de x dans G.

Pour des groupes de transformations, deux éléments conjugués sont, de manière un peu vague, deux éléments qui agissent de la même façon, les « éléments géométriques » étant déplacés par le « conjugant ». Ainsi, deux éléments de $\mathcal{S}_n$ sont conjugués dans $\mathcal{S}_n$ si et seulement si leurs décompositions canoniques en cycles à supports disjoints sont de même type, l'ensemble des conjugués d'une translation de vecteur non nul dans le groupe affine d'un espace affine est l'ensemble de toutes les translations de vecteur non nul, l'ensemble des conjugués d'une réflexion orthogonale (hyperplane) dans un espace euclidien est l'ensemble de toutes les réflexions orthogonales.

Exercice 52. ② *On suppose que G est infini et qu'il existe x dans $G \setminus \{e\}$ tel que $Conj_G(x)$ soit finie. Montrer que G n'est pas simple.*

Exercice 53. ③ *Déterminer les classes de conjugaison de $\mathcal{A}_5$.*

Pour cette action, le stabilisateur de x n'est autre que son commutant :

$$C(x) = \{g \in G,\ gx = xg\}.$$

On en déduit un résultat très utile.

Proposition 12. *Si G est un groupe fini, on a, pour $x \in G$:*

$$|Conj_G(x)| \times |C(x)| = |G|.$$

En particulier, le cardinal de $Conj_G(x)$ divise $|G|$.

Exercice 54. ④ *Dénombrer la classe de conjugaison d'un élément σ de $\mathcal{S}_n$. En déduire le cardinal du groupe des éléments de $\mathcal{S}_n$ qui commutent à σ.*

L'action par conjugaison est donc utile pour étudier les problèmes de commutation. Voici un exemple important. Si p est un nombre premier, on appelle *p-groupe* tout groupe fini dont le cardinal est une puissance de p. On a alors le théorème suivant, qui est un des premiers résultats reliant les propriétés arithmétiques de $|G|$ aux propriétés algébriques de G.

Théorème 13. *Le centre d'un p-groupe n'est pas réduit à l'élément neutre.*

13. Le cas $n = p^2$, plus difficile et donne une idée du cas général, traité par Kaloujnine et Krasner (circa 1945).

Preuve. Soient G un p-groupe, x dans G. La classe de conjugaison de x est de cardinal 1 si x est central. Sinon, le cardinal de cette classe est de la forme $p^m, m \in \mathbb{N}^*$, en particulier divisible par p. En écrivant que les classes de conjugaison forment une partition de G, on obtient que le cardinal de $Z(G)$ est divisible par p.

Il vaut la peine d'observer que le raisonnement fait pour établir le théorème 11 donne une propriété très générale relative aux actions d'un p-groupe.

Théorème 14. *Soit G un p-groupe. On suppose que G agit sur l'ensemble fini X. Alors*

$$|X^G| \equiv |X| \ [p].$$

Exercice 55. ③ *Soit p un nombre premier, G un groupe d'ordre p^2. Montrer que G est abélien, puis que G est isomorphe à l'un des deux groupes additifs $\mathbb{Z}/p^2\mathbb{Z}$, $(\mathbb{Z}/p\mathbb{Z})^2$.*

Exercice 56. ③ *Soient p un nombre premier, G un p-groupe, H un sous-groupe normal de G. Montrer que $Z(G) \cap H$ n'est pas réduit à $\{e\}$.*

Exercice 57. ④ *Soit G un groupe fini d'ordre ≥ 2. Montrer que le groupe $Aut\ (G)$ des automorphismes de G agit transitivement sur $G\backslash\{e\}$ si et seulement s'il existe un nombre premier p et un entier $n \geq 1$ tels que G soit isomorphe au groupe additif $(\mathbb{Z}/p\mathbb{Z})^n$.*

Exercice 58. ④ *Identifier les groupes finis G tels que l'action de $Aut\ (G)$ sur $G \setminus \{e\}$ soit doublement transitive.*

Le théorème de Landau ci-après (1903) donne une seconde illustration, anecdotique mais plaisante, de l'action de G sur lui-même par conjugaison.

Théorème 15. *Notons $k(G)$ le nombre de classes de conjugaison du groupe fini G. Alors*

$$k(G) \underset{|G|\to+\infty}{\longrightarrow} +\infty.$$

Preuve. Soit G un groupe fini tel que $k(G) = r$. Notons $C_1, \ldots, C_r$ les classes de conjugaison de G, avec $C_1 = \{e\}$. Pour tout i, soit g_i un élémentde C_i. En écrivant que G est réunion disjointe des classes, on obtient

$$|G| = \sum_{i=1}^{r} |C_i|, \quad \text{i.e.} \quad 1 = \sum_{i=1}^{r} \frac{1}{|C(g_i)|}.$$

Admettons provoirement que, pour r dans $\mathbb{N}^*$ et q dans $\mathbb{Q}^{+*}$ fixés, l'ensemble

$$E_{r,q} = \left\{ (x_1, \ldots, x_r) \in \mathbb{N}^{*r},\ \sum_{i=1}^{r} \frac{1}{x_i} = q \right\}$$

est fini, notons $M_{r,q}$ le maximum des y de $\mathbb{N}^*$ tels qu'existe $(x_1, \ldots, x_r)$ dans $E_{r,q}$ avec $x_1 = y$. Alors

$$|G| = |C(g_1)| \leq M_{r,1}.$$

Ainsi, on dispose d'une majoration de la forme

$$|G| \leq f(k(G)).$$

Le résultat suit.

Preuve de la finitude de $E_{r,q}$. On raisonne par récurrence sur r, le cas $r = 1$ étant évident. Supposons $r \geq 2$, le résultat vrai à l'ordre $r-1$, soit $(x_1, \ldots, x_r)$ dans $E_{r,q}$. Soit $j \in \{1, \ldots, r\}$ tel que x_j soit minimal. Alors

$$r/x_j \geq q, \qquad x_j \leq r/q.$$

Il n'y a donc qu'un nombre fini de choix pour x_j. Comme

$$\sum_{i=1}^{r} \frac{1}{x_i} = q \Longleftrightarrow \sum_{i \in \{1,\ldots,r\} \setminus \{j\}} \frac{1}{x_i} = q - \frac{1}{x_j},$$

on peut conclure en appliquant l'hypothèse de récurrence.

Exercice 59. ③ *Déterminer les groupes finis G tels que $k(G) = 2$, puis tels que $k(G) = 3$.*

Exercice 60. ⑤ *Donner une minoration de $k(G)$ par une fonction explicite de $|G|$ tendant vers $+\infty$ en $+\infty$.*

2.6 Action de G sur $\mathcal{P}(G)$ par conjugaison ; normalisateur

Généralités

On fait agir G par conjugaison sur l'ensemble $\mathcal{P}(G)$ des parties de G en posant :

$$\forall (g, P) \in G \times \mathcal{P}(G), \qquad g.P = gPg^{-1}.$$

Le stabilisateur de P est appelé *normalisateur de P dans G* ; c'est l'ensemble

$$N_G(P) = \{g \in G,\ gPg^{-1} = P\}.$$

Si H est un sous-groupe de G, $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal.

La proposition 2 prend ici la forme suivante.

Proposition 13. *Supposons G fini. Le nombre de conjugués d'une partie P de G est égal à*

$$\frac{|G|}{|N_G(P)|}.$$

Exercice 61. ③ *Soient n dans $\mathbb{N}^*$, $\mathbb{K}$ un corps, $H_1 = D_n(\mathbb{K})$ le sous-groupe de $G = GL_n(\mathbb{K})$ constitué des matrices diagonales, $H_2 = \mathcal{B}_n(\mathbb{K})$. le sous-groupes des matrices triangulaires supérieures inversibles de G. Identifier les normalisateurs $N_G(H_1)$ et $N_G(H_2)$.*

Exercice 62. ③ *Soit $n \geq 2$ un entier. Quel est le normalisateur du sous-groupe $SO_n(\mathbb{R})$ dans $GL_n(\mathbb{R})$?*

Exercice 63. ③ *Soient E un espace affine, $G = \mathcal{S}(E)$, H le sous-groupe de G constitué des translations. Montrer que $N_G(H)$ est le groupe affine de E.*

Exercice 64. ③ *Soient G un groupe fini, p un nombre premier divisant G. En utilisant le fait que les p-Sylow de G sont conjugués, déterminer leur nombre. Dénombrer les p-Sylow de $GL_n(\mathbb{F}_p)$.*

Exercice 65. ② *Montrer que si le groupe simple G possède une classe de conjugaison de cardinal m, G se plonge dans $\mathcal{S}_m$.*

Réunion des conjugués d'un sous-groupe

L'énoncé ci-après, dû à Frobenius, est une application intéressante et utile de la notion de normalisateur.

Théorème 16. *Soient G un groupe fini, H un sous-groupe strict de G. Alors la réunion des conjugués de H dans G est de cardinal majoré par :*

$$1 + (|H| - 1)\frac{|G|}{|N_G(H)|}, \quad \textit{donc par} \quad |G| + 1 - \frac{|G|}{|H|}.$$

En particulier :

- la réunion des conjugués de H dans G n'est pas égale à G ;

- le seul sous-groupe de G coupant toute classe de conjugaison de G est G.

Preuve. Dans l'action par conjugaison de G sur l'ensemble des conjugués de H, il y a $|G|/|N_G(H)|$ orbites, i.e. $|N_G(H)|/|H|$ conjugués distincts de H. Ces conjugués sont de cardinal $|H|$ et contiennent e, d'où la première majoration. La seconde vient du fait que $N_G(H)$ contient H. Enfin, le second point est un corollaire immédiat du premier, formulé de deux manières différentes.

Exercice 66. ③ *Les notations sont celles du théorème 16. En appliquant le théorème 9 du paragraphe* **1.6** *à l'action naturelle de G sur sur G/H, retrouver le fait que G n'est pas réunion des conjugués de H.*

Remarques

1. Les couples (G, H) où G est un groupe fini, H un sous-groupe de G tel que
$$\left| \bigcup_{g \in G} gHg^{-1} \right| = |G| + 1 - \frac{|G|}{|H|}$$
sont appelés *couples de Frobenius*. La preuve du théorème 15 montre que, pour que (G, H) soit un couple de Frobenius, il faut et il suffit que $N_G(H) = H$ et que deux conjugués distincts de H aient leur intersection réduite à $\{e\}$. Les couples de Frobenius apparaissent dans diverses questions et sont l'objet d'un très beau théorème de Frobenius, dont la preuve repose sur la théorie des caractères.
2. La seconde partie du théorème 16 ne s'étend pas aux groupes infinis : le groupe linéaire $\mathrm{GL}_n(\mathbb{C})$ est réunion des conjugués du sous-groupe $\mathcal{B}_n(\mathbb{C})$ des matrices triangulaires supérieures. L'exercice ci-après montre que le résultat subsiste cependant si H est d'indice fini dans G.

Exercice 67. ④ *Montrer que si H est un sous-groupe strict de G et d'indice fini dans G, alors G n'est pas réunion des conjugués de H.*

L'exercice ci-après montre que l'étude du cas d'égalité dans la borne de Cameron-Cohen (théorème 9 de **1.6**) fait apparaître un couple de Frobenius.

Exercice 68. ③ *Le groupe G agit fidèlement sur X, qui est fini de cardinal $n \geq 2$. On suppose que l'action est doublement transitive et que les éléments de $G \setminus \{e\}$ agissent avec au plus un point fixe. Soit x un élément de X. Montrer que (G, G_x) est un couple de Frobenius.*

Exercice 69. ④ *Soient p un nombre premier, $G = GL_2(\mathbb{F}_p)$, B le sous-groupe de G constitué des matrices triangulaires supérieures.*

a) Montrer qu'il existe g dans G d'ordre $p^2 - 1$.

b) Soient $g \in G$ d'ordre $p^2 - 1$ et C le sous-groupe de G engendré par g. Montrer que tout élément de G est conjugué à un élément de $C \cup B$.

Plongement de $N_G(H)/C_G(H)$ dans Aut (H)

Si H est un sous-groupe de G et g un élément de $N_G(H)$, l'automorphisme intérieur de G provenant de g induit par restriction un automorphisme $i_{g,H}$ de H. L'application de $N_G(H)$ dans Aut (H) qui à g associe $i_{g,H}$ est un morphisme de $N_G(H)$ dans Aut (H) ; son noyau est le sous-groupe $C_G(H)$ des éléments de G commutant à tous les éléments de H, appelé *centralisateur* de H dans G. On obtient la proposition ci-après, très utile en dépit de la simplicité de sa preuve.

Proposition 14. *Le groupe $N_G(H)/C_G(H)$ est isomorphe à un sous-groupe de Aut (H). En particulier $G/Z(G)$ est isomorphe à un sous-groupe de Aut (G).*

Exercice 70. ② *Montrer que, si le groupe Aut (G) des automorphismes de G est monogène, alors G est abélien.*

2.7 Entiers n tels que tout groupe d'ordre n soit cyclique

Nous allons caractériser les entiers n tels qu'il y ait, à isomorphisme près, un unique sous-groupe d'ordre n. Ce résultat, marginal mais plaisant, est dû à G. Miller (1903). Le théorème suivant y joue un rôle décisif.

Théorème 17. *Si G est un groupe non abélien fini dont tous les sous-groupes stricts sont abéliens, G n'est pas simple.*

Preuve. Étape 1. Soit G un groupe simple. Si H et K sont deux sous-groupes maximaux distincts de G, tous deux abéliens, alors $H \cap K = \{e\}$.

Puisque H et K sont maximaux distincts, G est engendré par $H \cup K$. D'autre part, puisque H et K sont abéliens, $H \cap K$ est normal dans H et dans K, donc dans G. Par simplicité : $H \cap K = \{e\}$.

Étape 2. Soit G un groupe simple, H un sous-groupe maximal de G. Si H est abélien, (G, H) est un couple de Frobenius.

Comme G est simple et H maximal, $N_G(H) = H$. D'après l'étape 1, deux conjugués distincts de H ont pour intersection $\{e\}$. Le résultat suit.

Étape 3. Conclusion.

Soit par l'absurde G un groupe fini simple dont tous les sous-groupes stricts sont abéliens. Soit H un sous-groupe maximal de G. Puisque la réunion des conjugués de H n'est pas égale à G, on dispose d'un sous-groupe maximal K de G qui n'est pas un conjugué de H. Un conjugué de H et un conjugué de K ont pour intersection $\{e\}$ d'après l'étape 1. La réunion des conjugués de H et des conjugués de K a donc pour cardinal :

$$2|G| + 1 - \frac{|G|}{|H|} - \frac{|G|}{|K|} \geq |G| + 1,$$

d'où la contradiction désirée.

Voici le résultat de Miller mentionné au début du paragraphe.

Théorème 18. *Soit n un élément de $\mathbb{N}^*$. Les assertions suivantes sont équivalentes.*

(i) Les entiers n et $\varphi(n)$ sont premiers entre eux.

(ii) Tout groupe d'ordre n est cylique.

Preuve de $(i) \Rightarrow (ii)$. On écarte le cas trivial $n = 1$. L'hypothèse signifie alors que $n = p_1 \dots p_r$ où les p_i sont premiers deux à deux distincts et où p_i ne divise pas $p_j - 1$ si $i \neq j$. On raisonne par récurrence sur r, le cas $r = 1$ étant trivial. Prenons G d'ordre $n = p_1 \dots p_r$, les p_i étant comme ci-dessus et le résultat étant établi à l'ordre $r - 1$. Il suffit de démontrer que G est abélien pour conclure : G contient un élément d'ordre p_i pour tout i (lemme de Cauchy), le produit de ces éléments est d'ordre n (car si deux éléments u et v d'un groupe commutent et ont des ordres finis m et n premiers entre eux, alors uv est d'ordre mn).

On raisonne par l'absurde en supposant G non abélien. Or, tout diviseur d de n vérifie : $d \wedge \varphi(d) = 1$, donc, par hypothèse de récurrence, tout sous-groupe de G est cyclique. On peut en particulier appliquer à G le théorème 17 et conclure que G n'est pas simple.

On dispose donc d'un sous-groupe normal non trivial N de G. D'après la proposition 14, G/N se plonge dans Aut (N). Mais si $m = |N|$, G/N est d'ordre n/m tandis que Aut (N), isomorphe au groupe multiplicatif $(\mathbb{Z}/m\mathbb{Z})^*$, est d'ordre $\varphi(m)$. Puisque n/m et $\varphi(m)$ sont premiers entre eux, le morphisme est trivial et N est central dans G. Ainsi, $Z(G)$ n'est pas nul et l'hypothèse de récurrence entraîne que $G/Z(G)$ est cyclique. Or, il est classique et facile de vérifier que $G/Z(G)$ n'est monogène que si G est abélien. [14] C'est la contradiction désirée.

Preuve de $(ii) \Rightarrow (i)$. L'hypothèse entraîne que soit n est divisible par le carré d'un nombre premier, soit n admet deux diviseurs premiers p et q tels que $q \equiv 1\ [p]$. Il suffit donc d'établir les deux points suivants.

1. Si p est un nombre premier, il existe un groupe d'ordre p^2 non cyclique. C'est clair en considérant $(\mathbb{Z}/p\mathbb{Z})^2$).

2. Si p et q sont deux nombres premiers distincts tels que $q \equiv 1\ [p]$, alors il existe un groupe non cylique de cardinal pq. Or, si tel est le cas, on dispose

14. Si g est un élément de G dont la classe dans $G/Z(G)$ engendre $G/Z(G)$, tout élément de G s'écrit $zg^n, z \in Z(G), n \in \mathbb{Z}$. On en déduit aisément que G est abélien.

d'un ssous-groupe cyclique C de ${\mathbb{F}_p}^*$ de cardinal q. En fait, le sous-groupe de $\mathrm{Aff}_1(\mathbb{F}_p)$ constitué des applications

$$x \longmapsto ax + b, \qquad a \in C, \quad b \in \mathbb{F}_p$$

est non abélien de cardinal pq. Cette méthode un peu ad-hoc peut être remplacée par un argument plus général (construction d'un produit semi-direct).

Exercice 71. ③ *a) Montrer que, si p est un nombre premier, le sous-groupe de $GL_3(\mathbb{F}_p)$ constitué des matrices triangulaires supérieures à termes diagonaux égaux à 1 est de cardinal p^3 et non abélien.*

b) Soient p et q deux nombres premiers tels que $q^2 \equiv 1\ [p]$. Construire un groupe de cardinal pq^2 non abélien.

Exercice 72. ⑤ *Déterminer les entiers n tels que tout groupe de cardinal n soit abélien.*