Groupes finis

Jean-Pierre Serre

Cours à l'École Normale Supérieure de Jeunes Filles, 1978/1979

rédigé par Martine BUHLER et Catherine GOLDSTEIN
(Montrouge, 1979)

révisé et transcrit en LaTeX par
Nicolas BILLEREY, Olivier DODANE et Emmanuel REY
(Strasbourg – Paris, 2004)

Table des matières

1 Préliminaires **5**

1.1 Actions de groupes . . . 5

1.2 Sous-groupes normaux ; sous-groupes caractéristiques ; groupes simples . . 6

1.3 Filtrations et théorème de Jordan-Hölder . . . 7

2 Théorèmes de Sylow **10**

2.1 Définitions . . . 10

2.2 Existence des p-Sylow . . . 10

2.2.1 Première démonstration . . . 11

2.2.2 Seconde démonstration (Miller-Wielandt) . . . 11

2.3 Propriétés des p-Sylow . . . 12

2.4 Fusion . . . 13

3 Groupes résolubles et groupes nilpotents **16**

3.1 Groupes résolubles . . . 16

3.2 Suite centrale descendante . . . 19

3.3 Groupes nilpotents . . . 19

3.4 Groupes nilpotents finis . . . 21

3.5 Cas des groupes abéliens . . . 23

3.6 Sous-groupe de Frattini . . . 25

4 Cohomologie et extensions **28**

4.1 Définitions . . . 28

4.2 Extensions . . . 30

4.3 Groupes finis : un critère de nullité . . . 34

4.4 Extensions de groupes d'ordres premiers entre eux . . . 35

4.5 Relèvements d'homomorphismes . . . 37

5 Groupes résolubles et sous-groupes de Hall **39**
5.1 Π-sous-groupes 39
5.2 Préliminaires : sous-groupes permutables 40
5.3 Systèmes permutables de sous-groupes de Sylow 41
5.4 Démonstration du th. 5.1 42
5.5 Un critère de résolubilité 42
5.6 Démonstration du th. 5.3 43

6 Groupes de Frobenius **44**
6.1 Réunion des conjugués d'un sous-groupe 44
6.2 Groupes de Frobenius : définition 46
6.3 Structure de N 47
6.4 Structure de H 48

7 Transfert **51**
7.1 Définition 51
7.2 Calcul du transfert 52
7.3 Exemples d'utilisation du transfert 53
7.3.1 Premier exemple (Gauss) 53
7.3.2 Second exemple 54
7.4 Transfert dans un sous-groupe de Sylow 54
7.5 Application : groupes simples d'ordre impair inférieur à 2000 56
7.6 Application : groupes simples non abéliens d'ordre inférieur à 200 56

A Théorie des caractères **59**
A.1 Représentations et caractères 59
A.2 Relations d'orthogonalité 61
A.3 Caractères et fonctions centrales 63
A.4 Exemples de caractères 64
A.5 Propriétés d'intégralité 66
A.6 Application : théorème de Burnside 68
A.7 Démonstration du théorème de Frobenius 69

Bibliographie **72**

Index **73**

Chapitre 1

Préliminaires

Ce chapitre est essentiellement constitué de rappels sur la théorie générale des groupes. La lettre G désigne un groupe.

1.1 Actions de groupes

Définition 1.1 *On dit que le groupe G* opère à gauche *sur un ensemble X si l'on s'est donné une application*

$$\begin{cases} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g.x \end{cases}$$

vérifiant les conditions :

(1) $g.(g'.x) = (gg').x$ pour tout $x \in X$ et tout couple $(g, g') \in G \times G$.

(2) $1.x = x$ pour tout $x \in X$, où 1 est l'élément neutre de G.

Remarque. La donnée d'une action à gauche de G sur X équivaut à la donnée d'un homomorphisme τ de G dans le groupe $\mathcal{S}_X$ des permutations de X défini pour tout $g \in G$ et tout $x \in X$ par $\tau(g)(x) = g.x$.

On aurait une définition analogue pour les opérations à droite.

Le groupe G découpe alors X en *orbites* : deux éléments x et y de X sont dans la même orbite si et seulement s'il existe $g \in G$ tel que $x = g.y$. L'ensemble des orbites est le quotient de X par G et est noté $G\backslash X$ dans le cas d'une action à gauche (et X/G dans le cas d'une action à droite).

Définition 1.2 *On dit que G agit transitivement sur X si $G\backslash X$ est réduit à un élément.*

En particulier, le groupe G agit transitivement sur chaque orbite.

Définition 1.3 *Soit $x \in X$; on appelle* stabilisateur de x *(ou* fixateur *de x) et on note H_x le sous-groupe de G formé des éléments $g \in G$ qui fixent x (i.e. tels que $g.x = x$).*

Remarque. Si G opère transitivement sur X et si $x \in X$, on a une bijection de G/H_x sur X donnée par $gH_x \longmapsto g.x$, où G/H_x est l'ensemble des classes à gauche de G modulo H_x. Si $x' \in X$, il existe $g \in G$ tel que $x' = g.x$. Alors $H_{x'} = gH_xg^{-1}$. Donc changer de point de base revient à remplacer le stabilisateur de x par un de ses conjugués. Inversement, si H est un sous-groupe de G, alors G agit transitivement sur G/H et H stabilise la classe de 1. Ainsi la donnée de X sur lequel G opère transitivement revient à celle d'un sous-groupe de G, déterminé à conjugaison près.

Exemple. Soit X une droite affine définie sur un corps K et soit G le groupe des similitudes

$$G = \{x \mapsto ax + b,\ a \in K^*,\ b \in K\}\,.$$

Le groupe G opère transitivement sur X. Si $x \in X$, le stabilisateur de x est le groupe des homothéties centrées en x.

Application. Soit G un groupe *fini*, dont on note $|G|$ l'ordre. Soit X un ensemble où G opère. On a $X = \coprod_{i\in I} Gx_i$ où les Gx_i sont les orbites (2 à 2 disjointes) sous l'action de G, les x_i formant un système de représentants des éléments de $G\backslash X$. On a vu que Gx_i est en bijection avec G/H_{x_i}, donc $|Gx_i| = |G|.|H_{x_i}|^{-1}$. On en déduit $|X| = \sum_{i\in I} |G|.|H_{x_i}|^{-1}$ puis $|X|.|G|^{-1} = \sum_{i\in I} |H_{x_i}|^{-1}$.

Cas particulier. Le groupe G opère sur lui-même par automorphismes intérieurs ; on a une application :

$$\begin{cases} G & \longrightarrow & \mathcal{S}_G \\ x & \longmapsto & \mathrm{int}_x \end{cases}$$

où $\mathrm{int}_x(y) = xyx^{-1} = {}^x y$. Les orbites sont les classes de conjugaison. Le stabilisateur d'un élément x de G est l'ensemble des éléments de G qui commutent à x (on l'appelle *centralisateur* de x et on le note $C_G(x)$). On a $1 = \sum_{i\in I} |C_G(x_i)|^{-1}$ où $(x_i)_{i\in I}$ est un système de représentants des classes de conjugaison. Pour $x_i = 1$, on a $C_G(x_i) = G$ et donc $\sup_{i\in I} |C_G(x_i)| = |G|$.

Exercice.
(i) Si h est un entier $\geqslant 1$, montrer qu'il n'y a qu'un nombre fini de décompositions $1 = \sum_{i=1}^{h} \frac{1}{n_i}$ avec $n_i \in \mathbf{Z}$, $n_i \geqslant 1$. [Par exemple, si $h = 3$, les seuls n_i possibles sont $(3,3,3)$, $(2,4,4)$ et $(2,3,6)$.]

(ii) En déduire que, si un groupe fini G a un nombre de classes de conjugaison égal à h, l'ordre de G est majoré par une constante $N(h)$ ne dépendant que de h. (On peut prendre $N(h)$ de la forme ${c_1}^{{c_2}^h}$, où c_1, c_2 sont des constantes > 0. J'ignore si l'on peut faire beaucoup mieux.)

1.2 Sous-groupes normaux ; sous-groupes caractéristiques ; groupes simples

Définition 1.4 *On dit qu'un sous-groupe H de G est* normal *(ou* invariant*) si pour tout $x \in G$ et tout $h \in H$, on a $xhx^{-1} \in H$.*

Cela revient à dire que le sous-groupe H est stable par tout automorphisme intérieur. Une telle situation se décrit par une suite exacte :

$$\{1\} \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow \{1\} .$$

Remarque. Si H est un sous-groupe de G, il existe un plus grand sous-groupe de G dans lequel H est normal, à savoir l'ensemble des $g \in G$ tels que $gHg^{-1} = H$. On l'appelle le *normalisateur de H dans G*, et on le note $N_G(H)$. On dit qu'une partie de G *normalise* H si elle est contenue dans $N_G(H)$.

Définition 1.5 *On dit qu'un sous-groupe H de G est* caractéristique *s'il est stable par tout automorphisme de G.*

Un tel sous-groupe est normal.

Exemple. Le *centre* de G (ensemble des éléments qui commutent à tous les éléments de G) est un sous-groupe caractéristique. Il en est de même du *groupe dérivé* de G, ainsi des sous-groupes D^nG, C^iG et $\Phi(G)$ définis au chap. 3.

Définition 1.6 *On dit qu'un groupe G est* simple *lorsqu'il a exactement deux sous-groupes normaux : $\{1\}$ et G.*

Exemples.
(1) Les seuls groupes *abéliens* simples sont les groupes cycliques d'ordre premier, c'est-à-dire les groupes $\mathbf{Z}/p\mathbf{Z}$ avec p premier.

(2) Le groupe alterné $\mathcal{A}_n$ est simple si $n \geqslant 5$.

(3) Le groupe $\mathbf{PSL}_n(\mathbf{F}_q)$ est simple pour $n \geqslant 2$ sauf dans le cas $n = 2$ et $q = 2$ ou 3.

1.3 Filtrations et théorème de Jordan-Hölder

Définition 1.7 *Une* filtration *du groupe G est une suite finie $(G_i)_{0 \leqslant i \leqslant n}$ de sous-groupes telle que*

$$G_0 = \{1\} \subset G_1 \subset \cdots \subset G_i \subset \cdots \subset G_n = G$$

avec G_i normal dans G_{i+1}, pour $0 \leqslant i \leqslant n-1$.

On appelle gradué *de G (associé à la filtration $(G_i)_{0 \leqslant i \leqslant n}$) et on note* $\mathrm{gr}(G)$ *la suite des* $\mathrm{gr}_i(G) = G_i/G_{i-1}$, *pour $1 \leqslant i \leqslant n$.*

Définition 1.8 *Une filtration $(G_i)_{0 \leqslant i \leqslant n}$ de G est dite* de Jordan-Hölder *si G_i/G_{i-1} est simple pour tout $1 \leqslant i \leqslant n$.*

Proposition 1.1 *Si G est fini, G possède une suite de Jordan-Hölder.*

Si $G = \{1\}$, on a la suite de Jordan-Hölder triviale ($n = 0$). Si G est simple, on prend $n = 1$. Si G n'est pas simple, on raisonne par récurrence sur l'ordre de G. Soit $N \subset G$, N normal dans G d'ordre maximal. Alors G/N est simple, car sinon il existerait M normal dans G contenant strictement N et distinct de G. Comme $|N| < |G|$, on peut appliquer l'hypothèse de récurrence et si $(N_i)_{0 \leqslant i \leqslant n}$ est une suite de Jordan-Hölder pour N, alors $(N_0, \cdots, N_{n-1}, N, G)$ en est une pour G. $\square$

Remarque. Si G est infini, il peut ne pas posséder de suite de Jordan-Hölder : c'est par exemple le cas de $\mathbf{Z}$.

Théorème 1.2 (Jordan-Hölder) *Soit G un groupe fini et soit $(G_i)_{0\leqslant i\leqslant n}$ une suite de Jordan-Hölder de G. Le gradué de G, à permutation près des indices, ne dépend pas de la suite choisie.*

Il suffit de montrer que si S est un groupe simple fixé et si $n\,(G,(G_i),S)$ est le nombre de j tels que G_j/G_{j-1} est isomorphe à S, alors $n\,(G,(G_i),S)$ ne dépend pas de la suite (G_i).

On commence par une remarque : si H est un sous-groupe de G, une filtration (G_i) sur G induit une filtration (H_i) sur H définie par $H_i = G_i \cap H$. De même, si N est normal, on a une filtration sur G/N définie par $(G/N)_i = G_i/(G_i \cap N)$. La suite exacte

$$\{1\} \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow \{1\}$$

se conserve par filtration :

$$\{1\} \longrightarrow N_i/N_{i-1} \longrightarrow G_i/G_{i-1} \longrightarrow (G/N)_i/(G/N)_{i-1} \longrightarrow \{1\}$$

d'où finalement la suite exacte

$$\{1\} \longrightarrow \mathrm{gr}_i(N) \longrightarrow \mathrm{gr}_i(G) \longrightarrow \mathrm{gr}_i(G/N) \longrightarrow \{1\}.$$

Si la filtration initiale est de Jordan-Hölder, $\mathrm{gr}_i(G)$ est simple pour tout i, donc $\mathrm{gr}_i(N)$ est isomorphe à $\{1\}$ ou à $\mathrm{gr}_i(G)$. Par réindexation, on peut donc obtenir une filtration de Jordan-Hölder sur N et de même sur G/N.

Cette remarque permet de démontrer le théorème ; on a en effet deux possibilités : soit $\mathrm{gr}_i(N) = \{1\}$ et $\mathrm{gr}_i(G/N) = \mathrm{gr}_i(G)$, soit $\mathrm{gr}_i(N) = \mathrm{gr}_i(G)$ et $\mathrm{gr}_i(G/N) = \{1\}$. On en déduit une partition de $I = \{0,\dots,n\}$ en deux parties : $I_1 = \{i,\, \mathrm{gr}_i(N) = \{1\}\}$ et $I_2 = \{i,\, \mathrm{gr}_i(N) = \mathrm{gr}_i(G)\}$.

On raisonne alors par récurrence sur l'ordre de G. Si $G = \{1\}$, il n'y a pas de problème. Sinon, on peut toujours supposer que G n'est pas simple. Soit alors N un sous-groupe normal tel que $|N| < |G|$ et $|G/N| < |G|$. L'hypothèse de récurrence s'applique à N et G/N : $n\left(N,(N_i)_{i\in I_2},S\right)$ et $n\left(G/N,((G/N)_i)_{i\in I_1},S\right)$ sont indépendants de la filtration. Or

$$n\left(G,(G_i)_{i\in I},S\right) = n\left(N,(N_i)_{i\in I_2},S\right) + n\left(G/N,((G/N)_i)_{i\in I_1},S\right),$$

donc $n\left(G,(G_i)_{i\in I},S\right)$ est indépendant de la filtration choisie. □

Application. On retrouve ainsi l'unicité de la décomposition d'un entier en produit de facteurs premiers. En effet, si $n = p_1^{h_1}\cdots p_k^{h_k}$, on a pour $\mathbf{Z}/n\mathbf{Z}$ la filtration de Jordan-Hölder suivante :

$$\mathbf{Z}/n\mathbf{Z} \supset p_1\mathbf{Z}/n\mathbf{Z} \supset p_1^2\mathbf{Z}/n\mathbf{Z} \supset \cdots \supset p_1^{h_1}\mathbf{Z}/n\mathbf{Z} \supset \cdots$$

Donc $\mathbf{Z}/p_i\mathbf{Z}$ apparaît h_i fois dans le gradué, d'où l'unicité.

Exemples.
(1) Filtration de $\mathcal{S}_3$: $\mathcal{A}_3$ est normal dans $\mathcal{S}_3$ et $\mathcal{A}_3$ est cyclique d'ordre 3. D'où la filtration

$$\{1\} \subset \mathcal{A}_3 \subset \mathcal{S}_3.$$

(2) Filtration de $\mathcal{S}_4$: $\mathcal{A}_4$ est normal dans $\mathcal{S}_4$ avec $(\mathcal{S}_4 : \mathcal{A}_4) = 2$. Dans $\mathcal{A}_4$, il existe un sous-groupe normal D de type $(2,2)$: $D = \{1, \sigma_1, \sigma_2, \sigma_3\}$ avec

$$\begin{aligned} \sigma_1 &= (a,b)(c,d), \\ \sigma_2 &= (a,c)(b,d), \\ \sigma_3 &= (a,d)(b,c). \end{aligned}$$

On a donc la filtration

$$\{1\} \subset \{1, \sigma_i\} \subset D \subset \mathcal{A}_4 \subset \mathcal{S}_4.$$

L'ordre des quotients successifs est $2, 2, 3, 2$. Le choix de i étant arbitraire, il n'y a pas unicité de la filtration.

(3) Filtration de $\mathcal{S}_n$ pour $n \geqslant 5$: le groupe $\mathcal{A}_n$ étant simple, on a la filtration

$$\{1\} \subset \mathcal{A}_n \subset \mathcal{S}_n.$$

Chapitre 2

Théorèmes de Sylow

Soit p un nombre premier et soit G un groupe fini.

2.1 Définitions

Définition 2.1 *On dit que G est un* p-groupe *si l'ordre de G est une puissance de p. Si G est d'ordre $p^n m$ avec m premier à p, on dit qu'un sous-groupe H de G est un* p-Sylow *de G si H est d'ordre p^n.*

Remarques.
(1) Soit S un sous-groupe de G ; S est un p-Sylow de G si et seulement si S est un p-groupe et $(G : S)$ est premier à p.

(2) Tout conjugué d'un p-Sylow de G est un p-Sylow de G.

Exemple. Soit K un corps fini de caractéristique p à $q = p^f$ éléments. Soit $G = \mathbf{GL}_n(K)$ le groupe des matrices inversibles $n \times n$ à coefficients dans K. Ce groupe est isomorphe à $\mathbf{GL}(V)$ où V est un espace vectoriel sur K de dimension n. On remarque que l'ordre de G est le nombre de bases d'un espace vectoriel de dimension n sur K, soit :

$$|G| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1) = p^{fn(n-1)/2} m,$$

où $m = \prod_{i=1}^{n} (q^i - 1)$ est premier à q, donc à p.
Considérons d'autre part le groupe P constitué des matrices triangulaires supérieures à coefficients diagonaux égaux à 1. C'est un sous-groupe de G d'ordre $|P| = q^{n(n-1)/2} = p^{fn(n-1)/2}$. Donc P est un p-Sylow de G.

2.2 Existence des p-Sylow

Le but de cette section est de démontrer le premier théorème de Sylow :

Théorème 2.1 *Tout groupe fini possède au moins un p-Sylow.*

2.2.1 Première démonstration

Elle repose sur la proposition suivante :

Proposition 2.2 *Soit H un sous-groupe de G et soit S un p-Sylow de G. Alors il existe $g \in G$ tel que $H \cap gSg^{-1}$ soit un p-Sylow de H.*

Soit X l'ensemble des classes à gauche de G modulo S. Le groupe G (resp. H) agit sur X par translations. Les stabilisateurs des points de X sous G (resp. sous H) sont les conjugués de S (resp. les $H \cap gSg^{-1}$). Or $|X| \not\equiv 0 \pmod p$ car S est un p-Sylow de G. L'une des orbites $\mathcal{O}$ de X sous l'action de H a un nombre d'éléments premier à p (sinon $|X|$ serait divisible par p) ; soit $x \in \mathcal{O}$ et soit H_x le stabilisateur de x dans H. Le groupe H_x est un p-groupe, de la forme $H \cap gSg^{-1}$ (pour un certain g) et $(H : H_x) = |\mathcal{O}|$ est premier à p. Donc H_x est un p-Sylow de H de la forme $H \cap gSg^{-1}$. □

Corollaire 2.3 *Si G a des p-Sylow et si H est un sous-groupe de G, alors H a aussi des p-Sylow.*

Application. [Une première preuve du th. 2.1] Soit G un groupe fini d'ordre n. On peut plonger G dans le groupe symétrique $\mathcal{S}_n$. D'autre part, $\mathcal{S}_n$ se plonge dans $\mathbf{GL}_n(K)$ (où K est un corps fini de caractéristique p) : si $\sigma \in \mathcal{S}_n$ et si $(e_i)_{1 \leqslant i \leqslant n}$ est une base de K^n, on associe à σ la transformation linéaire f définie par $f(e_i) = e_{\sigma(i)}$. Donc G se plonge dans $\mathbf{GL}_n(K)$. D'après l'exemple du § 2.1, $\mathbf{GL}_n(K)$ possède un p-Sylow. Le corollaire ci-dessus permet de conclure.

2.2.2 Seconde démonstration (Miller-Wielandt)

On suppose que $|G| = p^n m$ avec m premier à p. On note X l'ensemble des parties de G à p^n éléments et s le nombre de p-Sylow de G.

Lemme 2.4 $|X| \equiv sm \pmod p$.

Le groupe G opère sur X par translations à gauche. Soit $X = \coprod_i X_i$ la décomposition de X en orbites sous l'action de G. Si $A_i \in X_i$, on a $X = \coprod_i GA_i$. On note G_i le stabilisateur de A_i. On rappelle que $|GA_i| = |G|/|G_i|$.
Remarque : $|G_i| \leqslant p^n$. Soit en effet $x \in A_i$. Si $g \in G_i$, alors gx appartient à A_i, donc peut prendre p^n valeurs. On a donc au plus p^n choix pour g. On distingue donc deux cas :
- Si $|G_i| < p^n$, alors $|GA_i|$ est divisible par p.
- Si $|G_i| = p^n$, alors G_i est un p-Sylow de G.

Réciproquement soit P un p-Sylow de G ; $Pg \in X$ pour tout $g \in G$ et le stabilisateur de Pg est P. De même, si P stabilise une partie A de X, alors $PA \subset A$ donc pour tout $a \in A$, on a $Pa \subset A$ donc $A = Pa$. (les deux ensembles ont mêmes cardinaux). Donc P stabilise exactement son orbite sous l'action de G (et le cardinal de cette orbite est $|G/P| = m$). Finalement

$$|X| = \sum_{i \,/\, |G_i| < p^n} |GA_i| \quad + \sum_{i \,/\, |G_i| = p^n} |GA_i|$$

soit

$$|X| \equiv 0 + sm \pmod p$$

d'où le résultat. $\square$

Ce lemme nous donne le th. 2.1. En effet, d'après ce lemme, la classe de s modulo p ne dépend que de l'ordre de G. Or $G' = \mathbf{Z}/|G|\mathbf{Z}$ a un unique p-Sylow (qui est isomorphe à $\mathbf{Z}/p^n\mathbf{Z}$). Donc $s \equiv 1 \pmod p$; en particulier, s est non nul. $\square$

Remarque. On a démontré en fait que le nombre de p-Sylow d'un groupe G est congru à 1 modulo p. On retrouvera cette propriété ultérieurement.

Corollaire 2.5 (Cauchy) *Si p divise l'ordre de G, alors G contient un élément d'ordre p.*

En effet, soit S un p-Sylow de G (il en existe d'après le th. 2.1) ; S n'est pas réduit à $\{1\}$ car p divise l'ordre de G. Soit $x \in S$ distinct de $\{1\}$. L'ordre de x est une puissance de p, soit p^m $(m \geqslant 1)$. Alors $x^{p^{m-1}}$ est d'ordre p. $\square$

2.3 Propriétés des p-Sylow

Théorème 2.6 (Second théorème de Sylow)

(1) Tout p-sous-groupe de G est contenu dans un p-Sylow de G.

(2) Les p-Sylow de G sont conjugués.

(3) Le nombre des p-Sylow est congru à 1 modulo p.

Lemme 2.7 *Soit X un ensemble fini sur lequel opère un p-groupe P et soit X^P l'ensemble des éléments de X fixés par P. Alors $|X| \equiv |X^P| \pmod p$.*

Les orbites à un élément de X sous l'action de P sont celles constituées d'un point de X^P. L'ensemble $X - X^P$ est donc réunion d'orbites non triviales, de cardinal divisible par p. $\square$

On peut alors démontrer les points (1) et (2) du th. 2.6 : soit S un p-Sylow de G et soit P un p-sous-groupe de G. On applique le lemme 2.7 à l'ensemble X des classes à gauche de G modulo S : $|X| \not\equiv 0 \pmod p$ donc $|X^P| \not\equiv 0 \pmod p$. En particulier, il existe $x \in X$ fixé par P. Le stabilisateur de x contient donc P et est un conjugué de S. Donc P est contenu dans un conjugué de S (c'est-à-dire dans un p-Sylow de G).
Pour le point (2), on applique (1) à $P = S'$ où S' est un p-Sylow de G. Il existe $g \in G$ tel que $S' \subset gSg^{-1}$, donc $S' = gSg^{-1}$. $\square$

Pour le point (3), on donne une nouvelle démonstration basée sur le lemme suivant :

Lemme 2.8 *Soient S et S' deux p-Sylow de G. Si S' normalise S, alors $S = S'$.*

Soit H le sous-groupe de G engendré par S et S'. Le groupe H normalise S qui est un p-Sylow de H. Donc S est le seul p-Sylow de H (les p-Sylow de H sont conjugués) ; or S' est un p-Sylow de H donc $S = S'$. $\square$

Montrons le point (3). Si X est l'ensemble des p-Sylow de G, alors S opère sur X par conjugaison et d'après le lemme 2.8, S est le seul élément de X fixé par S. On réapplique le lemme 2.7 (avec $P = S$) : $|X| \equiv 1 \pmod p$. $\square$

Corollaire 2.9 *Si S est un p-Sylow de G, alors $\big(G : N_G(S)\big) \equiv 1 \pmod p$.*

L'application f de $G/N_G(S)$ dans l'ensemble des p-Sylow de G, définie par $f(\bar{g}) = gSg^{-1}$ (où g est un représentant quelconque de $\bar{g}$) est bijective. $\square$

On a vu que pour tout sous-groupe H de G, il existe un p-Sylow de G dont l'intersection avec H est un p-Sylow de H. Ce n'est pas vrai pour tout p-Sylow de G. Mais si H est normal, on a :

Proposition 2.10 *Soit H un sous-groupe normal de G et soit S un p-Sylow de G. Alors*

(1) $S \cap H$ est un p-Sylow de H.

(2) L'image de S dans G/H est un p-Sylow de G/H (et on les obtient tous ainsi).

*(3) (**Frattini**) Si Q est un p-Sylow de H, alors $H.N_G(Q) = G$.*

(1) Evident.

(2) L'image de S dans G/H est isomorphe à $S/(H \cap S)$. Si p^a (resp. p^b) est la puissance de p maximale divisant l'ordre de H (resp. de G/H), p^{a+b} est la puissance maximale de p divisant l'ordre de G. Par suite, S a p^{a+b} éléments. De plus, $H \cap S$ a au plus p^a éléments donc $S/(H \cap S)$ au moins p^b et donc exactement p^b. Il s'ensuit que $S/(H \cap S)$ est un p-Sylow de G/H. D'autre part, on obtient tous les p-Sylow par conjugaison, d'où (2).

(3) Soit $g \in G$. On a $gQg^{-1} \subset gHg^{-1} = H$ (H est normal). Or gQg^{-1} est un p-Sylow de H, donc il existe $h \in H$ tel que $gQg^{-1} = hQh^{-1}$, donc $h^{-1}g \in N_G(Q)$ et donc $g \in H.N_G(Q)$. Ainsi $G \subset H.N_G(Q)$, donc $H.N_G(Q) = G$. $\square$

Corollaire 2.11 *Soit S un p-Sylow de G et soit H un sous-groupe de G contenant $N_G(S)$. Alors $N_G(H) = H$.*

H est normal dans $N_G(H)$ et contient S qui est donc un p-Sylow de H. On applique le point (3) de la proposition ci-dessus : $H.N_G(S) = N_G(H)$. Donc $N_G(H) \subset H$ d'où le résultat. $\square$

En particulier, si S est un p-Sylow de G, on a $N_G\big(N_G(S)\big) = N_G(S)$.

2.4 Fusion

Soit S un p-Sylow de G. On note N le normalisateur de S dans G. On se pose le problème de savoir si deux éléments de S conjugués dans G sont conjugués dans N. On a la :

Proposition 2.12 (Burnside) *Soient X et Y deux parties du centre de S, conjuguées dans G et soit $g \in G$ tel que $gXg^{-1} = Y$. Alors il existe $n \in N$ tel que $nxn^{-1} = gxg^{-1}$ pour tout $x \in X$. En particulier, $nXn^{-1} = Y$.*

On veut trouver $n \in N$ tel que $nxn^{-1} = gxg^{-1}$ pour tout $x \in X$ i.e. $g^{-1}nxn^{-1}g = x$ pour tout $x \in X$. Donc on cherche $n \in N$ tel que $g^{-1}n \in A = C_G(X)$ (le centralisateur de X). Or X est contenu dans le centre de S donc A contient S. De même, $Y = gXg^{-1}$ donc $g^{-1}Sg$ est contenu dans A. Les groupes S et $g^{-1}Sg$ sont des p-Sylow de A (il suffit de regarder leurs ordres) donc sont conjugués dans A : il existe $a \in A$ tel que $ag^{-1}Sga^{-1} = S$. Donc $n = ga^{-1}$ appartient à N et $g^{-1}n$ appartient à A. $\square$

Corollaire 2.13 *Soient x et y deux éléments du centre de S. S'ils sont conjugués dans G, ils sont conjugués dans N.*

Remarque. L'hypothèse « x et y appartiennent au centre de S » ne peut être supprimée : si l'on prend $G = \mathbf{GL}_3(\mathbf{Z}/p\mathbf{Z})$ et

$$S = \left\{ \begin{pmatrix} 1 & \times & \times \\ 0 & 1 & \times \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

alors

$$N = \left\{ \begin{pmatrix} \times & \times & \times \\ 0 & \times & \times \\ 0 & 0 & \times \end{pmatrix} \right\}$$

et les éléments

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

sont conjugués dans G et ne le sont pas dans N.

Disons que deux éléments x, y de S sont *localement conjugués* s'il existe un sous-groupe U de S les contenant tel que x et y soient conjugués dans $N_G(U)$.

Théorème 2.14 (Alperin) *La relation d'équivalence sur S engendrée par la relation « x et y sont localement conjugués » est la relation « x et y sont conjugués dans G ».*

En d'autres termes :

Théorème 2.15 *Si $x, y \in S$ sont conjugués dans G, il existe une suite $a_0, \ldots, a_n$ d'éléments de S telle que :*

(1) $a_0 = x$ et $a_n = y$.

(2) a_i est localement conjugué de a_{i+1} pour $0 \leqslant i \leqslant n-1$.

Cela résulte du théorème plus précis suivant :

Théorème 2.16 *Soit A une partie de S et soit $g \in G$ tel que $A^g \subset S$. Il existe alors un entier $n \geqslant 1$, des sous-groupes $U_1, \ldots, U_n$ de S et des éléments $g_1, \ldots, g_n$ de G avec :*

(1) $g = g_1 \cdots g_n$.

(2) $g_i \in N_G(U_i)$ pour $1 \leqslant i \leqslant n$.

(3) $A^{g_1 \cdots g_{i-1}} \subset U_i$ pour $1 \leqslant i \leqslant n$.

Remarque. Pour $i = 1$, (3) signifie que $A \subset U_1$. Noter que l'on a $A^{g_1 \cdots g_i} \subset U_i$ pour $1 \leqslant i \leqslant n$, comme on le voit en combinant (2) et (3). On a en particulier $A^g \subset U_n$.

Le théorème ci-dessus est un corollaire de celui-ci (prendre A réduit à un élément).

Démonstration. Soit T le sous-groupe de S engendré par A. On raisonne par récurrence sur *l'indice* $(S : T)$ de T dans S. Si cet indice est 1, on a $T = S$, d'où $S^g = S$ et $g \in N_G(S)$. On prend alors $n = 1$, $g_1 = g$ et $U_1 = S$.

Supposons donc $(S : T) > 1$, i.e. $T \neq S$. Le groupe $T_1 = N_S(T)$ est alors distinct de T. C'est un p-sous-groupe de $N_G(T)$. Choisissons un p-Sylow Σ de $N_G(T)$ contenant T_1. D'après le th. 2.6, il existe $u \in G$ tel que $\Sigma^u \subset S$. Posons d'autre part $V = T^g$; on a $V \subset S$ par hypothèse. Le groupe Σ^g est un p-Sylow de $N_G(V) = \big(N_G(T)\big)^g$.
Comme $N_S(V)$ est un p-sous-groupe de $N_G(V)$, il existe $w \in N_G(V)$ tel que $\big(N_S(V)\big)^w \subset \Sigma^g$. Posons $v = u^{-1}gw^{-1}$. On a $g = uvw$.

On va maintenant décomposer u et v :
(i) On a $T^u \subset \Sigma^u \subset S$. Comme l'indice de T_1 dans S est strictement inférieur à celui de T, l'hypothèse de récurrence montre qu'il existe des sous-groupes $U_1, \ldots, U_m$ de S et des éléments $u_1 \in N_G(U_1), \ldots, u_m \in N_G(U_m)$ avec $u = u_1 \cdots u_m$ et $T_1^{u_1 \cdots u_{i-1}} \subset U_i$ pour $1 \leqslant i \leqslant m$.
(ii) Posons $T_2 = N_S(V)$ et $T_3 = T_2^{v^{-1}} = T_2^{wg^{-1}u}$. Comme T_2^w est contenu dans Σ^g, on a $T_3 \subset \Sigma^{gg^{-1}u} = \Sigma^u$. Le groupe T_3 est contenu dans S, et $T_3^v = T_2$ aussi. Comme l'indice de T_3 est strictement inférieur à celui de T, on en déduit comme ci-dessus l'existence de sous-groupes $V_1, \ldots, V_r$ de S et d'éléments $v_j \in N_G(V_j)$, avec $v = v_1 \cdots v_r$ et $T_3^{v_1 \cdots v_{j-1}} \subset V_j$ pour $1 \leqslant j \leqslant r$.

Il reste à vérifier que les sous-groupes $U_1, \ldots, U_m, V_1, \ldots, V_r, V$ de S et la décomposition $g = u_1 \cdots u_m v_1 \cdots v_r w$ de g satisfont aux conditions du théorème.
On a

$$u_i \in N_G(U_i),\ v_j \in N_G(V_j),\ w \in N_G(V)$$

par construction, ainsi que $T^{u_1 \cdots u_{i-1}} \subset U_i$ $(1 \leqslant i \leqslant m)$ puisque T est contenu dans T_1. Il reste à voir que

$$T^{u_1 \cdots u_m v_1 \cdots v_{j-1}} \subset V_j$$

pour $1 \leqslant j \leqslant r$.
Or $T^{u_1 \cdots u_m} = T^u$ est contenu dans $T_3 = T_2^{wg^{-1}u}$; en effet, $V = T^g$ est normalisé par w^{-1} ; on a donc $T^{gw^{-1}} = V \subset N_S(V) = T_2$, d'où $T \subset T_2^{wg^{-1}}$ et $T^u \subset T_2^{wg^{-1}u}$.
On déduit de là que

$$T^{u_1 \cdots u_m v_1 \cdots v_{j-1}} = T^{uv_1 \cdots v_{j-1}} \subset T_3^{v_1 \cdots v_{j-1}} \subset V_j,$$

ce qui achève la démonstration. □

Chapitre 3

Groupes résolubles et groupes nilpotents

3.1 Groupes résolubles

Soit G un groupe et soient x, y deux éléments de G. L'élément $x^{-1}y^{-1}xy$ est appelé le *commutateur* de x et y. On le note (x, y). On a

$$xy = yx(x, y).$$

Si A et B sont deux sous-groupes de G, on note (A, B) le groupe engendré par les commutateurs (x, y) avec $x \in A$ et $y \in B$. Le groupe (G, G) est appelé le *groupe des commutateurs* de G ou encore le *groupe dérivé* de G et est noté $D(G)$. C'est un sous-groupe caractéristique de G. De sa définition résulte aussitôt la :

Proposition 3.1 *Soit H un sous-groupe de G. Les propriétés suivantes sont équivalentes :*

(1) H contient $D(G)$.

(2) H est normal et G/H est abélien.

En ce sens, $G/D(G)$ est le plus grand quotient abélien de G. On le note parfois G^{ab}.

On peut itérer le procédé et définir la suite des sous-groupes dérivés de G :

$$\begin{aligned} D^0G &= G, \\ D^nG &= (D^{n-1}G, D^{n-1}G) \quad \text{pour } n \geqslant 1. \end{aligned}$$

On a $G \supset D^1G \supset D^2G \supset \cdots$.

Définition 3.1 *Un groupe G est dit* résoluble *s'il existe un entier $n \geqslant 0$ tel que $D^nG = \{1\}$. On appelle alors* classe de résolubilité *de G et on note $cl(G)$ le plus petit entier n positif pour lequel $D^nG = \{1\}$.*

Ainsi, $cl(G) = 0$ équivaut à $G = \{1\}$ et $cl(G) \leqslant 1$ équivaut à dire que G est abélien.

Proposition 3.2 *Soit G un groupe et soit n un entier $\geqslant 1$. Les propriétés suivantes sont équivalentes :*

(1) G est résoluble de classe $\leqslant n$,

(2) Il existe une suite $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ de sous-groupes normaux de G tels que G_i/G_{i+1} soit abélien pour $0 \leqslant i \leqslant n-1$,

(2') Il existe une suite $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ de sous-groupes de G tels que G_i soit normal dans G_{i-1} et que G_{i-1}/G_i soit abélien, pour $1 \leqslant i \leqslant n$,

(3) Il existe un sous-groupe abélien A normal dans G tel que G/A soit résoluble de classe $\leqslant n-1$.

(1) $\Rightarrow$ (2) Posons $G_i = D^iG$ pour tout $i \geqslant 0$. Puisque $D(G)$ est stable par tout automorphisme (même non intérieur !) de G, D^iG est normal dans G pour tout i. La suite $(G_i)_{i\geqslant 0}$ ainsi définie vérifie donc (2).

(2) $\Rightarrow$ (2$'$) est trivial.

(2$'$) $\Rightarrow$ (1) Par récurrence sur k on voit que $D^kG \subset G_k$ pour tout k, d'où $D^nG = \{1\}$.

(1) $\Rightarrow$ (3) On prend $A = D^{n-1}G$.

(3) $\Rightarrow$ (1) D'après l'implication (1) $\Rightarrow$ (2), appliquée à G/A et à $n-1$, il existe une suite

$$A_0 = G \supset A_1 \cdots \supset A_{n-1} = A$$

de sous-groupes normaux de G telle que la suite des quotients

$$G/A \supset A_1/A \supset \cdots \supset A_{n-1}/A = \{1\}$$

vérifie la condition (2). Alors la suite

$$G \supset A_1 \supset \cdots \supset A_{n-1} \supset \{1\}$$

vérifie la condition (2) et l'implication (2) $\Rightarrow$ (1) appliquée à G et à n permet de conclure. $\square$

Remarque. Tout sous-groupe (et tout groupe quotient) d'un groupe résoluble de classe $\leqslant n$ est résoluble de classe $\leqslant n$.

Proposition 3.3 *Soit G un groupe fini et soit $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ une suite de Jordan-Hölder de G. Pour que G soit résoluble, il faut et il suffit que G_i/G_{i+1} soit cyclique d'ordre premier pour $0 \leqslant i \leqslant n-1$.*

Remarquons d'abord que si un groupe est simple et résoluble, alors son groupe dérivé, étant normal, est réduit à $\{1\}$; le groupe est donc abélien et, étant simple, est cyclique d'ordre premier. Le théorème en résulte. $\square$

Exemples.

(1) Les groupes $\mathcal{S}_n$ sont résolubles si et seulement si $n \leqslant 4$.

(2) Un groupe simple non abélien n'est pas résoluble.

(3) Soit V un espace vectoriel de dimension n sur un corps commutatif K et soit

$$V = V_0 \supset V_1 \supset \cdots \supset V_n = 0$$

un drapeau complet (i.e. une suite décroissante de sous-espaces vectoriels de V tels que $\mathrm{codim}(V_i) = i$). On pose

$$G = \{s \in \mathbf{GL}(V) \mid sV_i = V_i,\ 0 \leqslant i \leqslant n\}$$

(si on choisit dans V une base adaptée au drapeau, G peut être identifié au groupe des matrices triangulaires supérieures).
On définit alors une suite de sous-groupes $(B_i)_{0\leqslant i\leqslant n}$ de G par

$$B_i = \{s \in G \mid (s-1)V_j \subset V_{i+j},\ 0 \leqslant j \leqslant n-i\}.$$

En particulier, $B_0 = G$.

On va démontrer que $(B_j, B_k) \subset B_{j+k}$ pour $0 \leqslant j \leqslant n$ et $0 \leqslant k \leqslant n$ avec $0 \leqslant j+k \leqslant n$. Soient en effet $s \in B_j$, $t \in B_k$ et $x \in V_i$. Il existe $v_{i+k} \in V_{i+k}$ tel que

$$tx = x + v_{i+k},$$

puis

$$stx = sx + sv_{i+k} = x + w_{i+j} + v_{i+k} + t_{i+j+k}$$

(avec $w_{i+j} \in V_{i+j}$ et $t_{i+j+k} \in V_{i+j+k}$). De même

$$tsx = t(x + w_{i+j}) = x + v_{i+k} + w_{i+j} + t'_{i+j+k}$$

(avec $t'_{i+j+k} \in V_{i+j+k}$). Donc

$$stx \equiv tsx \pmod{V_{i+j+k}}$$

ou encore

$$s^{-1}t^{-1}stx \equiv x \pmod{V_{i+j+k}}$$

d'où le résultat. En particulier :
• $(B_0, B_i) \subset B_i$ pour $0 \leqslant i \leqslant n$, donc les B_i sont normaux dans $B_0 = G$.
• $(B_i, B_i) = D(B_i) \subset B_{2i} \subset B_{i+1}$ pour $1 \leqslant i \leqslant n$, donc les quotients B_i/B_{i+1} sont abéliens pour $1 \leqslant i \leqslant n-1$.
• Enfin, $B_0/B_1 = G/B_1$ s'identifie au groupe des matrices diagonales (abélien car K est commutatif). Donc la suite $B_0 = G \supset B_1 \supset \cdots \supset B_n = \{1\}$ vérifie la condition (2) et G est résoluble.

(4) On verra ultérieurement (th. 5.4) que tout groupe d'ordre $p^a q^b$ (où p et q sont premiers) est résoluble.

(5) Mentionnons aussi le (très difficile) théorème de Feit-Thompson[1] : tout groupe d'ordre impair est résoluble (ou encore : l'ordre d'un groupe simple non abélien est pair).

(6) Les groupes résolubles interviennent en théorie des corps. Soit K un corps de caractéristique 0 et soit $\overline{K}$ une clôture algébrique de K. On note K_{rad} le plus petit sous-corps de $\overline{K}$ contenant K tel que pour tout $x \in K_{rad}$ et tout entier $n \geqslant 1$, on ait $x^{1/n} \in K_{rad}$. On démontre qu'une extension galoisienne finie de K est contenue dans K_{rad} si et seulement si son groupe de Galois est résoluble (i.e. une équation est *résoluble par radicaux* si et seulement si son groupe de Galois est résoluble. C'est de là que provient la terminologie « résoluble »).

[1]Référence : W. Feit et J.G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. 13 (1963), 775 – 1029.

3.2 Suite centrale descendante

Soit G un groupe. On appelle *suite centrale descendante* de G la suite $(C^nG)_{n\geqslant 1}$ de sous-groupes de G définie par récurrence par :

$$\begin{aligned} C^1G &= G, \\ C^{n+1}G &= (G, C^nG) \quad \text{pour } n \geqslant 1. \end{aligned}$$

Pour tout $n \geqslant 1$, C^nG est un sous-groupe caractéristique de G.

Proposition 3.4 *On a $(C^iG, C^jG) \subset C^{i+j}G$ pour tout $i \geqslant 1$ et tout $j \geqslant 1$.*

On raisonne par récurrence sur i, la proposition étant claire pour $i = 1$ et tout $j \geqslant 1$. Soit $j \geqslant 1$; on a $(C^{i+1}G, C^jG) = \big((G, C^iG), C^jG\big)$. Or $\big((C^iG, C^jG), G\big) \subset (C^{i+j}G, G)$ (par hypothèse de récurrence), donc $\big((C^iG, C^jG), G\big) \subset C^{i+j+1}G$. De même $\big((C^jG, G), C^iG\big)$ est contenu dans $C^{i+j+1}G$. Le lemme suivant permet de conclure. □

Lemme 3.5 *Si X, Y et Z sont des sous-groupes normaux de G et si H est un sous-groupe de G contenant $\big((Y,Z),X\big)$ et $\big((Z,X),Y\big)$, alors H contient $\big((X,Y),Z\big)$.*

On utilise l'identité de Hall :

$$\big(x^y, (y,z)\big)\big(y^z, (z,x)\big)\big(z^x, (x,y)\big) = 1,$$

(où $x^y = y^{-1}xy$) qui s'obtient en développant les quarante-deux termes du membre de gauche. (cf. Bourbaki, A.I, § 6). □

Remarque. L'identité de Hall est l'analogue pour les groupes de l'identité de Jacobi :

$$\big[x, [y,z]\big] + \big[y, [z,x]\big] + \big[z, [x,y]\big] = 0$$

pour les algèbres de Lie. On peut l'utiliser pour associer à tout groupe G muni d'une filtration (G_i) satisfaisant à $(G_i, G_j) \subset G_{i+j}$ une algèbre de Lie $gr(G)$, à savoir

$$gr(G) = \bigoplus_i G_i/G_{i+1}.$$

Si $\xi \in G_i/G_{i+1}$ et $\eta \in G_j/G_{j+1}$, le crochet

$$[\xi, \eta] \in G_{i+j}/G_{i+j+1}$$

est par définition l'image du commutateur (x,y) où x (resp. y) est un représentant dans G_i (resp. G_j) de ξ (resp. η). Ceci s'applique notamment au cas où $G_i = C^iG$ (cf. aussi Bourbaki, Lie II, § 4, n$^\text{o}$ 4).

3.3 Groupes nilpotents

Définition 3.2 *Un groupe G est dit* nilpotent *s'il existe un entier n positif tel que $C^{n+1}G = \{1\}$. La* classe de nilpotence *de G est alors le plus petit tel entier n.*

En particulier :
– Le groupe G est abélien si et seulement s'il est nilpotent de classe $\leqslant 1$.
– Un produit fini de groupes nilpotents est nilpotent et la classe de nilpotence du produit est la borne supérieure des classes des groupes.
– Un sous-groupe (resp. un groupe quotient) d'un groupe nilpotent est nilpotent.

Proposition 3.6 *Tout groupe nilpotent est résoluble.*

En effet, pour tout $n \geqslant 0$, on a $D^n G \subset C^{2^n} G$. □

La réciproque est fausse : le groupe $\mathcal{S}_3$ est résoluble de classe 2. Regardons la suite centrale descendante de $\mathcal{S}_3$; on a $C^1\mathcal{S}_3 = \mathcal{S}_3$, $C^2\mathcal{S}_3 = \mathcal{C}_3$ (groupe cyclique d'ordre 3) puis $C^3\mathcal{S}_3 = \mathcal{C}_3$, etc. La suite est stationnaire et n'atteint pas $\{1\}$. Donc $\mathcal{S}_3$ n'est pas nilpotent.

On peut former des groupes nilpotents de la façon suivante :

Proposition 3.7 *Un groupe G est nilpotent de classe $\leqslant n+1$ si et seulement s'il est extension centrale d'un groupe Γ nilpotent de classe $\leqslant n$ (i.e. s'il existe une suite exacte $\{1\} \to A \to G \to \Gamma \to \{1\}$ où A est contenu dans le centre de G).*

Si G est nilpotent de classe $n+1$, alors $C^{n+2}G = \{1\}$ donc $C^{n+1}G$ est dans le centre de G. Posons $\Gamma = G/C^{n+1}G$; on a $C^{n+1}\Gamma = \{1\}$ donc Γ est nilpotent de classe $\leqslant n$.
Réciproquement, si une telle suite exacte existe et si $C^{n+1}\Gamma = \{1\}$, alors $C^{n+1}G \subset A$, donc $C^{n+1}G$ est contenu dans le centre de G, et $C^{n+2}G = \{1\}$. □

Corollaire 3.8 *Soit G un groupe nilpotent et soit H un sous-groupe de G distinct de G. Alors $N_G(H)$ est distinct de H.*

On raisonne par récurrence sur la classe de nilpotence n de G. Si $n = 1$, on a $N_G(H) = G$ (car G est abélien) donc $N_G(H) \neq H$.
Si $n \geqslant 2$, choisissons un sous-groupe central A de G tel que G/A soit nilpotent de classe $\leqslant n-1$. Alors $N_G(H)$ contient A. Si H ne contient pas A alors $N_G(H) \neq H$. Si H contient A, alors H/A est un sous-groupe propre de G/A et l'hypothèse de récurrence montre que $H/A \neq N_{G/A}(H/A)$. Comme $N_G(H)/A = N_{G/A}(H/A)$, on en déduit que $N_G(H)$ est distinct de H. □

Une autre caractérisation des groupes nilpotents est donnée par la

Proposition 3.9 *Un groupe G est nilpotent si et seulement s'il existe une filtration $(G_i)_{1\leqslant i\leqslant n+1}$ telle que $G_1 = G \supset G_2 \supset \cdots \supset G_{n+1} = \{1\}$ avec $(G, G_i) \subset G_{i+1}$ pour tout $1 \leqslant i \leqslant n$.*

Remarque. Une condition plus forte serait $(G_i, G_j) \subset G_{i+j}$.

Démonstration. Si une telle filtration existe, alors $C^kG \subset G_k$ pour tout $k \geqslant 1$, donc G est nilpotent. Réciproquement, si G est nilpotent, on prend $G_k = C^kG$. □

Exemple. Soit V un espace vectoriel de dimension finie n sur un corps K et soit

$$V = V_0 \supset V_1 \supset \cdots \supset V_n = 0$$

un drapeau complet de V. Reprenons l'exemple du § 3.1 et posons

$$B_j = \{g \in \mathbf{GL}(V) \mid (g-1)V_i \subset V_{i+j},\ i \geqslant 0\}.$$

Alors B_1 est nilpotent ; en effet $(B_i)_{i \geqslant 1}$ est une filtration telle que $B_1 \supset B_2 \supset \cdots \supset B_n = \{1\}$ et $(B_i, B_j) \subset B_{i+j}$ comme on l'a vu plus haut.

En application, on a le :

Théorème 3.10 (Kolchin) *Soit V un espace vectoriel de dimension finie sur un corps commutatif K et soit G un sous-groupe de $\mathbf{GL}(V)$. On suppose que tout élément g de G admet 1 comme unique valeur propre (i.e. $g-1$ est nilpotent). Alors il existe un drapeau complet de V tel que G soit contenu dans le groupe B_1 correspondant (cf. ci-dessus). En particulier, G est nilpotent.*

On raisonne par récurrence sur la dimension n de V, le cas $n = 0$ étant trivial. Supposons donc $n \geqslant 1$ et montrons qu'il existe $x \in V$ non nul tel que $gx = x$ pour tout $g \in G$. Le problème étant linéaire, on peut étendre les scalaires et supposer K algébriquement clos. Soit A_G le sous-espace vectoriel de $\mathrm{End}(V)$ engendré par G. C'est une sous-algèbre de $\mathrm{End}(V)$. Distinguons deux cas :
• V est un A_G-module réductible, i.e. il existe $V' \subset V$, stable par G, distinct de 0 et de V. L'hypothèse de récurrence s'applique à V' et fournit un x non nul dans V' tel que $gx = x$ pour tout $g \in G$.
• Si V est irréductible, on a $A_G = \mathrm{End}(V)$ d'après un théorème de Burnside (cf. Bourbaki, A. VIII, § 4, n° 3). Or si $a, a' \in A_G$, on a $n\mathrm{Tr}(aa') = \mathrm{Tr}(a)\mathrm{Tr}(a')$. En effet, c'est clair si $a, a' \in G$ car alors $\mathrm{Tr}(aa') = \mathrm{Tr}(a) = \mathrm{Tr}(a') = n$ et c'est donc vrai dans A_G par linéarité. Si $n > 1$, les éléments a et a' de matrices respectives

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

sont dans $\mathrm{End}(V)$ donc dans A_G. Or $\mathrm{Tr}(a) = \mathrm{Tr}(a') = 1$ et $\mathrm{Tr}(aa') = 0$, donc $\dim(V) = 1$ et tout x non nul de V convient.
Une fois l'existence de x prouvée, on note V_{n-1} la droite engendrée par x. L'hypothèse de récurrence, appliquée à V/V_{n-1} fournit un drapeau complet pour V/V_{n-1}, stable par G, d'où aussitôt un drapeau complet pour V, stable par G et il est clair que G est contenu dans le sous-groupe B_1 correspondant. □

3.4 Groupes nilpotents finis

Soit p un nombre premier.

Proposition 3.11 *Tout p-groupe est nilpotent.*

On va en donner deux démonstrations.
• Soit P un p-groupe ; alors P peut se plonger dans $\mathbf{GL}_n(\mathbf{Z}/p\mathbf{Z})$ pour un entier n suffisamment grand. Donc P est contenu dans un p-Sylow de $\mathbf{GL}_n(\mathbf{Z}/p\mathbf{Z})$, qui est conjugué, comme on l'a déjà vu, à l'ensemble B_1 des matrices triangulaires supérieures à éléments diagonaux égaux à 1. D'après l'exemple du § 3.3, B_1 est nilpotent, donc aussi P.

• On peut supposer $P \neq \{1\}$. Faisons opérer P sur lui-même par automorphismes intérieurs ; l'ensemble des points fixes est le centre $C(P)$ de P. Comme P est un p-groupe, on a d'après le lemme 2.7

$$|P| \equiv |C(P)| \pmod{p},$$

donc $C(P) \neq \{1\}$. Ainsi $P/C(P)$ est d'ordre strictement inférieur à celui de P. Une récurrence permet de conclure. □

Corollaire 3.12 *Soit G un groupe d'ordre p^n (avec p premier et $n \geqslant 1$). Alors :*

(1) Tout sous-groupe de G d'ordre p^{n-1} est normal.

(2) Si H est un sous-groupe de G, il existe une suite de sous-groupes $(H_i)_{1 \leqslant i \leqslant m}$ telle que $H = H_1 \subset H_2 \subset \cdots \subset H_m = G$ avec $(H_i : H_{i-1}) = p$ pour $2 \leqslant i \leqslant m$.

(3) Tout sous-groupe de G distinct de G est contenu dans un sous-groupe d'ordre p^{n-1}.

(1) Soit H un sous-groupe de G d'ordre p^{n-1}. Alors H est distinct de $N_G(H)$ car G est nilpotent. Donc l'ordre de $N_G(H)$ est p^n et H est normal dans G.

(2) On raisonne par récurrence sur l'ordre de G. Soit donc H un sous-groupe de G, qu'on peut supposer distinct de G. Soit H' un sous-groupe de G, distinct de G, contenant H, d'ordre maximal. Alors H' est distinct de $N_G(H')$, donc $N_G(H') = G$ et H' est normal dans G. En particulier, G/H' est un p-sous-groupe d'ordre p^k pour un certain entier $k \geqslant 1$. Si $k > 1$, il existe un sous-groupe de G/H', distinct de $\{1\}$ et de G/H', donc un sous-groupe de G, distinct de G contenant H' strictement, ce qui est absurde. Donc $k = 1$ et $(G : H') = p$. L'hypothèse de récurrence appliquée à H' donne le résultat.

(3) découle immédiatement de (2). □

Corollaire 3.13 *Tout produit fini de p-groupes est nilpotent.*

On va démontrer une réciproque.

Théorème 3.14 *Soit G un groupe fini. Les assertions suivantes sont équivalentes :*

(1) G est nilpotent.

(2) G est produit de p-groupes.

(3) Pour tout p premier, G a un unique p-Sylow.

(4) Soient p et p' deux nombres premiers distincts et soit S_p (resp. $S_{p'}$) un p-Sylow de G (resp. un p'-Sylow) ; alors S_p et $S_{p'}$ se centralisent mutuellement (i.e. tout élément de S_p commute à tout élément de $S_{p'}$).

(5) Deux éléments de G d'ordres premiers entre eux commutent.

(2) $\Rightarrow$ (1) C'est le cor. 3.13 ci-dessus.

(1) $\Rightarrow$ (3) Soit S un p-Sylow de G et soit N son normalisateur. Alors N est son propre normalisateur (cf. cor. 2.11). Puisque nous supposons G nilpotent, cela entraîne $N = G$, cf. cor. 3.8, donc S est normal. Les p-Sylow de G étant conjugués, G a un unique p-Sylow.

(3) $\Rightarrow$ (4) Pour tout nombre premier p, soit S_p l'unique p-Sylow de G : il est normal dans G. Si p et p' sont deux premiers distincts, $S_p \cap S_{p'}$ est réduit à $\{1\}$ car c'est à la fois un p-groupe et un p'-groupe. Or si $x \in S_p$ et $y \in S_{p'}$, on a $x^{-1}y^{-1}xy \in S_p \cap S_{p'}$, d'où $x^{-1}y^{-1}xy = 1$. Donc S_p et $S_{p'}$ se centralisent mutuellement.

(4) $\Rightarrow$ (2) Pour tout p premier, choisissons un p-Sylow de G qu'on note S_p. Le groupe engendré par les S_p (p décrivant l'ensemble des nombres premiers) est G tout entier (car son ordre est divisible par celui de G). Définissons alors une application

$$\varphi : \begin{cases} \prod_p S_p & \longrightarrow & G \\ (s_p)_p & \longmapsto & \prod_p s_p. \end{cases}$$

Par hypothèse, φ est un homomorphisme, car les S_p se centralisent mutuellement. D'autre part, φ est surjective, car G est engendré par les S_p. Enfin G et $\prod_p S_p$ ont même cardinal, donc φ est un isomorphisme, ce qui démontre (2).

(2) $\Rightarrow$ (5) Supposons que G soit un produit de p-groupes G_p. Soient x et y deux éléments de G d'ordres premiers entre eux. Alors $x = (x_p)_p$ et $y = (y_p)_p$ et pour tout p on a $x_p = 1$ ou $y_p = 1$. En effet, on a $x_p = 1$ si et seulement si p ne divise pas l'ordre de x. Donc $x^{-1}y^{-1}xy = (x_p^{-1}y_p^{-1}x_py_p)_p = (1)$, donc $xy = yx$.

(5) $\Rightarrow$ (4) C'est évident.

En résumé, nous avons montré les implications suivantes :

$$\begin{tikzcd} (1) \arrow[d, Rightarrow] & (2) \arrow[l, Rightarrow] \arrow[r, Rightarrow] & (5) \arrow[dl, Rightarrow] \\ (3) \arrow[r, Rightarrow] & (4) \arrow[u, Rightarrow] & \end{tikzcd}$$

Le théorème en résulte. □

3.5 Cas des groupes abéliens

Tout groupe abélien est nilpotent ; d'après le § 3.4, tout groupe abélien est produit de p-groupes abéliens. On peut alors poursuivre la décomposition grâce au

Théorème 3.15 *Tout p-groupe abélien est produit de groupes cycliques.*

Remarque. Si G est un p-groupe abélien fini, il existe un entier n tel que $p^n x = 0$ pour tout $x \in G$, et l'on peut considérer G comme un module sur $\mathbf{Z}/p^n\mathbf{Z}$ (pour n assez grand). Il suffit donc de démontrer le théorème suivant :

Théorème 3.16 *Tout module (non nécessairement fini) sur $\mathbf{Z}/p^n\mathbf{Z}$ est somme directe de modules monogènes (isomorphes à $\mathbf{Z}/p^i\mathbf{Z}$ pour $i \leqslant n$).*

Soit G un module sur $\mathbf{Z}/p^n\mathbf{Z}$ et soit V le module quotient G/pG : c'est un espace vectoriel sur $\mathbf{Z}/p\mathbf{Z}$. Notons G_i l'ensemble $\{x \in G \mid p^i x = 0\}$. Les G_i définissent une filtration de G :

$$G_0 = 0 \subset G_1 \subset \cdots \subset G_n = G.$$

Soit V_i l'image de G_i dans V, alors

$$V_0 = 0 \subset V_1 \subset \cdots \subset V_n = V.$$

On peut choisir une base S de V adaptée à cette décomposition (i.e. $S_i = S \cap V_i$ est une base de V_i).

Si $s \in S$, on note $i(s)$ le plus petit i pour lequel $s \in S_i$ et on choisit un représentant $\bar{s}$ de s dans $G_{i(s)}$. On a $p^{i(s)}\bar{s} = 0$. Soit $G' = \bigoplus_{s\in S} \mathbf{Z}/p^{i(s)}\mathbf{Z}$; on définit un homomorphisme φ de G' dans G de la façon suivante : si $(n_s)_{s\in S} \in G'$, on pose $\varphi\big((n_s)\big) = \sum_{s\in S} n_s\bar{s}$. On va montrer que φ est un isomorphisme.
• φ est surjectif : il suffit de prouver que le sous-groupe H de G engendré par les $\bar{s}$ est G tout entier. Or l'application projection de H dans V est surjective (par définition, $\bar{s}$ s'envoie sur s qui parcourt une base de V). Donc $H + pG = G$ ou encore $G = pG + H$. En itérant,

$$G = p(pG + H) = p^2G + H = \cdots = p^nG + H = H.$$

• φ est injectif : soit $(n_s) \in G'$ tel que $\sum_{s\in S} n_s\bar{s} = 0$ dans G. Montrons que n_s est divisible par p^i pour tout i (donc $n_s = 0$). En effet, montrons par récurrence sur i que $n_s \in p^i\left(\mathbf{Z}/p^{i(s)}\mathbf{Z}\right)$. Pour $i = 0$, il n'y a rien à démontrer. Si c'est vrai jusqu'à l'ordre k, on a $n_s \in p^k\left(\mathbf{Z}/p^{i(s)}\mathbf{Z}\right)$. En particulier $n_s = 0$ si $i(s) \leqslant k$. On regarde donc les s pour lesquels $i(s) \geqslant k+1$. Par hypothèse,

$$\sum_{i(s)\geqslant k+1} n_s\bar{s} = 0.$$

Posons $n_s = p^k m_s$ avec $m_s \in \mathbf{Z}/p^{i(s)}\mathbf{Z}$; on a

$$p^k \sum_{i(s)\geqslant k+1} m_s\bar{s} = 0,$$

c'est-à-dire

$$\sum_{i(s)\geqslant k+1} m_s\bar{s} \;\in\; G_k,$$

d'où, par projection,

$$\sum_{i(s)\geqslant k+1} m_s s \;\in\; V_k.$$

Vu le choix de S, on en déduit que $m_s \equiv 0 \pmod p$. Donc p^{k+1} divise n_s et on en déduit que n_s appartient à $p^{k+1}\big(\mathbf{Z}/p^{i(s)}\mathbf{Z}\big)$. □

Exercice. Si G est un module sur $\mathbf{Z}/p^n\mathbf{Z}$, tout sous-module de G isomorphe à $\mathbf{Z}/p^n\mathbf{Z}$ est facteur direct.

Application des 2-groupes : constructions par règle et compas. Soit K un corps de caractéristique quelconque et soit L une extension galoisienne de K dont le groupe de Galois G est un 2-groupe. D'après le cor. 3.12, il existe G' normal dans G, d'indice 2, donc un corps intermédiaire L', fixé par G', qui est une extension quadratique de K. Si on itère, L/K apparaît comme une tour d'extensions quadratiques.
Réciproquement, si L/K est une telle tour, l'extension galoisienne engendrée a pour groupe de Galois un 2-groupe. On a ainsi une caractérisation des extensions galoisiennes dont le groupe est un 2-groupe. Si la caractéristique de K est distincte de 2, une extension quadratique est de la forme $K\big[\sqrt{a}\,\big] \simeq K[X]/(X^2 - a)$ où $a \in K^* {-} K^{*2}$. (Si car$K = 2$ on remplace $X^2 - a$ par $X^2 + X + a$).
Ceci rejoint le problème des nombres constructibles par règle et compas : ce sont les

nombres (algébriques sur $\mathbf{Q}$) contenus dans une extension galoisienne de $\mathbf{Q}$ dont le groupe de Galois est un 2-groupe.

Exemple. $\sqrt[3]{2}$ ne marche pas, car $X^3 - 2$ est irréductible et le groupe de Galois associé à la plus petite extension possible contenant $\sqrt[3]{2}$ est $\mathcal{S}_3$ dont l'ordre n'est pas une puissance de 2.

3.6 Sous-groupe de Frattini

Soit G un groupe fini. On appelle *sous-groupe de Frattini* de G et on note $\Phi(G)$ l'intersection des sous-groupes maximaux[2] de G. C'est un sous-groupe caractéristique de G.

Un problème intéressant est de savoir à quelles conditions une partie S de G engendre le groupe G. On a la proposition suivante :

Proposition 3.17 *Soit S une partie de G et soit H le sous-groupe engendré par S. On a $H = G$ si et seulement si $H.\Phi(G) = G$, i.e. si S engendre $G/\Phi(G)$.*

En effet, si $H.\Phi(G) = G$ et $H \neq G$, il existe H' maximal contenant H et distinct de G ; $\Phi(G)$ est aussi contenu dans H' par définition : $G = H.\Phi(G)$ est donc contenu dans H', ce qui est absurde. $\square$

Théorème 3.18 *Le groupe $\Phi(G)$ est nilpotent.*

On va utiliser la caractérisation (3) du th. 3.14. Soit S un p-Sylow de $\Phi(G)$ (pour un p premier quelconque). On a vu dans l'étude des groupes de Sylow (prop. 2.10) que $G = \Phi(G).N_G(S)$. D'après la proposition ci-dessus, on a $N_G(S) = G$, donc S est normal dans G, donc dans $\Phi(G)$, donc est l'unique p-Sylow de $\Phi(G)$ qui est alors nilpotent. $\square$

Dans le cas où G est un p-groupe, on a une caractérisation simple de $\Phi(G)$:

Théorème 3.19 *Si G est un p-groupe, $\Phi(G)$ est le sous-groupe engendré par les commutateurs et les puissances p-ièmes de G, i.e. $\Phi(G) = (G,G).G^p$.*

Si G est d'ordre p^n, ses sous-groupes H maximaux sont d'ordre p^{n-1}, donc sont normaux, donc sont des noyaux d'homomorphismes surjectifs de G dans $G/H \simeq \mathbf{Z}/p\mathbf{Z}$ (et réciproquement un tel homomorphisme définit un sous-groupe maximal de G). Donc $\Phi(G)$ est l'intersection des noyaux d'homomorphismes surjectifs de G dans $\mathbf{Z}/p\mathbf{Z}$. Or un tel homomorphisme est trivial sur (G,G) et G^p. Donc $(G,G).G^p \subset \Phi(G)$.
Réciproquement $V = G/(G,G).G^p$ est un espace vectoriel sur $\mathbf{Z}/p\mathbf{Z}$, dans lequel 0 est intersection d'hyperplans. Or un hyperplan est le noyau d'un homomorphisme de V dans $\mathbf{Z}/p\mathbf{Z}$. Le groupe $(G,G).G^p$ contient donc $\Phi(G)$. Finalement $\Phi(G) = (G,G).G^p$. $\square$

Application. $G/\Phi(G)$ est donc le plus grand quotient de G qui soit abélien élémentaire (i.e. produit de groupes cycliques d'ordre p).

[2] Un sous-groupe H de G est dit *maximal* s'il est distinct de G et maximal pour cette propriété ; on dit alors que l'action de G sur G/H est *primitive*.

Corollaire 3.20 *Une partie S de G engendre G si et seulement si son image dans $G/(G,G).G^p$ engendre ce groupe.*

En effet, on a alors $\langle S\rangle.\Phi(G) = G$ donc $\langle S\rangle = G$. □

Ainsi le cardinal minimum d'une partie S génératrice de G est $\dim_{\mathbf{F}_p}\big(G/\Phi(G)\big)$ (dans le cas où G est un p-groupe).

Caractérisations par les sous-groupes à deux générateurs. On peut dans la même veine étudier si les propriétés de certains sous-groupes de G permettent de démontrer des propriétés analogues pour le groupe tout entier.

Proposition 3.21 *Soit G un groupe (resp. un groupe fini). Supposons que tout sous-groupe de G engendré par deux éléments soit commutatif (resp. nilpotent). Alors G est commutatif (resp. nilpotent).*

Soient $x, y \in G$. Le groupe $\langle x, y\rangle$ est commutatif, donc $xy = yx$. Pour les groupes nilpotents finis, on utilise la caractérisation (5) du th. 3.14. □

On peut se demander si un théorème analogue est vrai pour les groupes résolubles. On va d'abord définir la notion de *groupe simple minimal*. Soit G un groupe fini simple non abélien. On dit que G est *minimal* si tout sous-groupe de G distinct de G est résoluble.

Lemme 3.22 *Si G n'est pas résoluble, il existe un sous-groupe H de G et un sous-groupe normal K de H, tels que H/K soit simple minimal.*

Exemple. $G = \mathcal{A}_6$ est simple (non minimal) ; on peut prendre $H = \mathcal{A}_5$ et $K = \{1\}$.

Démonstration. Soit H un sous-groupe non résoluble minimal de G et soit K un sous-groupe normal de H, distinct de H, et maximal. Le groupe K est résoluble (car strictement contenu dans H). Le quotient H/K est simple (car K est maximal) et non abélien (sinon H serait résoluble) ; il est de plus minimal (tout sous-groupe s'obtient comme quotient par K d'un sous-groupe H' contenant K et contenu dans H, donc est résoluble).

On a alors une réponse partielle à notre question :

Proposition 3.23 *Les deux assertions suivantes sont équivalentes :*

(1) Tout groupe simple minimal peut être engendré par deux éléments.

(2) Tout groupe tel que ses sous-groupes engendrés par deux éléments soient résolubles est résoluble.

Supposons (2). Soit G simple minimal ; si $\langle x, y\rangle \neq G$ pour tout couple $(x, y) \in G\times G$, alors $\langle x, y\rangle$ est résoluble comme sous-groupe de G strict et d'après (2), G est aussi résoluble, ce qui est impossible.

Supposons (1). Si G n'est pas résoluble, il existe H et K comme dans le lemme 3.22. Le groupe H/K est simple minimal donc engendré par deux éléments $\bar{x}$ et $\bar{y}$. Soit H' le sous-groupe de H engendré par x et y (représentants respectifs de $\bar{x}$ et $\bar{y}$). C'est un groupe résoluble par hypothèse ; or H/K est l'image par projection de H' donc est aussi résoluble, ce qui est absurde. $\square$

On est donc ramené au problème suivant : trouver la liste de tous les groupes simples minimaux et chercher s'ils sont engendrés par deux éléments. Ce problème a été résolu par Thompson, qui a montré[3] que tout groupe simple minimal est isomorphe à l'un des suivants (que l'on peut engendrer par deux éléments) :
- $\mathbf{PSL}_2(\mathbf{F}_p)$, $p \geqslant 5$, $p \not\equiv \pm 1 \pmod 5$,
- $\mathbf{PSL}_2(\mathbf{F}_{2^p})$, p premier $\geqslant 3$,
- $\mathbf{PSL}_2(\mathbf{F}_{3^p})$, p premier $\geqslant 3$,
- $\mathbf{PSL}_3(\mathbf{F}_3)$,
- groupes de Suzuki $Sz(2^p)$, p premier $\geqslant 3$.

Signalons un problème : est-il vrai qu'un groupe simple non abélien qui est *minimal* au sens naïf (i.e. qui ne contient pas de sous-groupe propre non abélien qui soit simple) est minimal au sens défini plus haut ?[4]

[3] Références : J.G. Thompson, *Non solvable finite groups all of whose local subgroups are solvable, I, II, ..., VI*, Bull. A.M.S. 74 (1968), 383 – 437 ; Pac. J. Math. 33 (1970), 451 – 536 ; ... ; Pac. J. Math. 51 (1974), 573 – 630.

Il existe une démonstration indépendante du théorème de classification de Thompson : P. Flavell, *Finite groups in which two elements generate a solvable group*, Invent. math. 121 (1995), 279 – 285.

[4] Réponse : oui, d'après la classification des groupes simples.

Chapitre 4

Cohomologie et extensions

4.1 Définitions

Soient G un groupe (noté multiplicativement) et A un G-module (autrement dit un groupe abélien noté additivement sur lequel G opère par automorphismes). On note sa le transformé de l'élément $a \in A$ par l'élément $s \in G$. On a

$$\begin{aligned} (st)a &= s(ta), \\ 1a &= a, \\ s(a_1 + a_2) &= sa_1 + sa_2, \end{aligned}$$

si $s, t \in G$ et $a, a_1, a_2 \in A$.

Des exemples d'une telle situation sont donnés par :
(1) Action triviale d'un groupe G sur un groupe abélien A : $sa = a$ pour $s \in G$ et $a \in A$.

(2) Si L est une extension galoisienne du corps K, de groupe de Galois G, alors G opère par automorphismes sur L muni de l'addition ou L^* muni de la multiplication.

Définition 4.1 *Soit n un entier positif ou nul. On appelle* n-cochaîne, *ou* cochaîne de degré *n sur G à valeurs dans A toute fonction de n variables de G à valeurs dans A :*

$$f : \begin{cases} G \times G \times \cdots \times G & \longrightarrow \quad A \\ \quad (s_1, s_2, \ldots, s_n) & \longmapsto \quad f(s_1, s_2, \ldots, s_n). \end{cases}$$

L'ensemble des cochaînes, muni de l'addition induite par celle de A, forme un groupe abélien noté $C^n(G, A)$.

Exemples.
$n = 0$: par convention, une fonction de 0 variable à valeurs dans A est un élément de A. D'où $C^0(G, A) = A$. On note f_a l'élément de $C^0(G, A)$ correspondant à l'élément $a \in A$.

$n = 1$: $C^1(G, A) = \{f : G \to A\}$.

$n = 2$: $C^2(G, A) = \{f : G \times G \to A\}$.

Définition 4.2 *Si $f \in C^n(G,A)$, on appelle* cobord *de f et on note df l'élément de $C^{n+1}(G,A)$ défini par la formule :*

$$\begin{aligned} df(s_1,\ldots,s_n,s_{n+1}) &= s_1 f(s_2,\ldots,s_{n+1}) + \sum_{i=1}^{n} (-1)^i f(s_1,\ldots,s_{i-1},s_i s_{i+1},\ldots) \\ &\qquad + (-1)^{n+1} f(s_1,\ldots,s_n). \end{aligned}$$

Regardons ce qu'est d pour les petites valeurs de n.
• $d:\ C^0(G,A) \longrightarrow C^1(G,A)$. Soit $a \in A$; on cherche df_a. On a $df_a(s) = sa - a$. Noter que $df_a = 0$ si et seulement si a est fixé par G.
• $d:\ C^1(G,A) \longrightarrow C^2(G,A)$. Soit f une 1-cochaîne ; on a

$$df(s,t) = sf(t) - f(st) + f(s).$$

• $d:\ C^2(G,A) \longrightarrow C^3(G,A)$. Soit f une 2-cochaîne ; on a

$$df(u,v,w) = uf(v,w) - f(uv,w) + f(u,vw) - f(u,v).$$

Théorème 4.1 (Formule fondamentale) *On a $d \circ d = 0$. Autrement dit, le composé*

$$C^n(G,A) \xrightarrow{d} C^{n+1}(G,A) \xrightarrow{d} C^{n+2}(G,A)$$

est nul.

Nous allons faire la vérification seulement dans les cas $n=0$ et $n=1$, laissant en exercice la vérification générale.

Soit $a \in A$. On a $df_a(s) = sa - a$ d'où

$$\begin{aligned} d \circ d\,(f_a)(s,t) &= sdf_a(t) - df_a(st) + df_a(s) \\ &= s(ta-a) - (sta-a) + (sa-a) \\ &= 0. \end{aligned}$$

Regardons maintenant $f \in C^1(G,A)$:

$$\begin{aligned} d \circ d\,(f)(u,v,w) &= u\,df(v,w) - df(uv,w) + df(u,vw) - df(u,v) \\ &= u\big(vf(w) - f(vw) + f(v)\big) - \big(uvf(w) - f(uvw) + f(uv)\big) \\ &\qquad + \big(uf(vw) - f(uvw) + f(u)\big) - \big(uf(v) - f(uv) + f(u)\big) \\ &= 0. \end{aligned}$$

□

Définition 4.3 *Une n-cochaîne f est dite un* n-cocycle *si $df = 0$. Elle est dite un* n-cobord *s'il existe une $(n-1)$-cochaîne g telle que $f = dg$.*

D'après le th. 4.1, tout n-cobord est un n-cocycle. On note $Z^n(G,A)$ le groupe des n-cocycles et $B^n(G,A)$ le groupe des n-cobords.
On note $H^n(G,A)$ le groupe quotient $Z^n(G,A)/B^n(G,A)$ et on l'appelle le *n-ième groupe de cohomologie de G à valeurs dans A.*

Exemples.
(1) Pour $n = 0$, on convient que $B^0 = \{0\}$. En notant A^G le groupe des éléments de A fixés par G, on a vu que

$$df_a = 0 \Longleftrightarrow a \in A^G,$$

et donc $H^0(G, A) = A^G$.

(2) Pour $n = 1$, un élément de $Z^1(G, A)$ est une application f de G dans A telle que $df(s, t) = 0$ pour tous $s, t \in G$, ce qui donne

$$f(st) = sf(t) + f(s).$$

On dit que f est un *homomorphisme croisé*. Si l'action de G sur A est triviale, on a $sf(t) = f(t)$ et f est un homomorphisme de G dans A ; comme $B^1(G, A) = \{0\}$, on a alors

$$H^1(G, A) = \mathrm{Hom}(G, A),$$

où $\mathrm{Hom}(G, A)$ est le groupe des homomorphismes de groupes de G dans A.

(3) Pour $n = 2$, une 2-cochaîne f est un 2-cocycle si

$$uf(v, w) - f(uv, w) + f(u, vw) - f(u, v) = 0$$

pour tous $u, v, w \in G$. Une telle cochaîne s'appelle aussi un *système de facteurs*.

4.2 Extensions

Définition 4.4 *Soient A et G deux groupes. On dit que E est une* extension *de G par A si l'on a une suite exacte*

$$\{1\} \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow \{1\}$$

avec A normal dans E.

Remarque. Dans ce §, on suppose A commutatif.

Toute extension E de G par A définit une action de G sur A de la manière suivante : remarquons d'abord que E agit sur A par automorphismes intérieurs (puisque A est normal dans E) ; on a un homomorphisme

$$\begin{cases} E & \longrightarrow & \mathrm{Aut}(A) \\ e & \longmapsto & \mathrm{Int}(e)_{|A}, \end{cases}$$

qui passe au quotient G : en effet, si $s \in G$, on choisit $e \in E$ qui relève s ; alors $\mathrm{Int}(e)$ ne dépend pas du choix du relèvement de s ; changer e en e' au dessus de s revient en effet à le multiplier par un élément a de A, or a agit trivialement sur A par automorphismes intérieurs puisque A est abélien. Donc G agit sur A :

$$\begin{tikzcd} E \arrow[rr] \arrow[dr] & & \mathrm{Aut}(A) \\ & G \arrow[ur] & \end{tikzcd}$$

On va donc considérer A comme un G-module ; les lois de groupe étant écrites multiplicativement, la loi d'action de G sur A sera écrite ${}^s a$ pour $a \in A$ et $s \in G$. On va associer à toute extension de G par A une classe de cohomologie de $H^2(G, A)$ qui détermine cette extension à isomorphisme près. Et l'on verra que tout élément de $H^2(G, A)$ peut être obtenu ainsi, cf. th. 4.3.

Soit E une extension de G par A ; on a une surjection π de E sur G.

Définition 4.5 *Une* section *h de π est une application de G dans E telle que $\pi \circ h = \mathrm{Id}_G$.*

$$\begin{tikzcd} E \arrow[d, "\pi"'] \\ G \arrow[u, bend right, "h"'] \end{tikzcd}$$

Au-dessus de $s \in G$, on choisit un point dans la fibre $\pi^{-1}(s)$. Tout élément $e \in E$ s'écrit alors de manière unique $ah(x)$, avec $a \in A$ et $x \in G$ (en fait $x = \pi(e)$).

Cherchons à mettre sous la forme $ch(z)$ l'élément $ah(x)bh(y)$. On a

$$ah(x)bh(y) = ah(x)bh(x)^{-1}h(x)h(y).$$

L'action de $x \in G$ sur A est donnée par l'action de l'automorphisme intérieur d'un élément de E au-dessus de x, par exemple $h(x)$. Donc $h(x)bh(x)^{-1} = {}^x b$ (qui est dans A, puisque A est normal). Posons

$$h(x)h(y) = f_h(x, y)h(xy).$$

On a $f_h(x, y) \in A$ puisque $h(x)h(y)$ et $h(xy)$ ont même image dans G par π. On a finalement obtenu :

$$ah(x)bh(y) = a\,{}^x b f_h(x, y)h(xy)$$

avec $a\,{}^x b f_h(x, y) \in A$.

Nous allons maintenant voir comment f_h varie avec h. Soient donc h et h' deux sections de π ($h, h' : G \to E$). Alors $h(s)$ et $h'(s)$ diffèrent par un élément de A. Posons $h'(s) = l(s)h(s)$; l'application l est une 1-cochaîne de G à valeurs dans A. Calculons $f_{h'}$ à l'aide de l et de f_h. On a

$$h'(s)h'(t) = f_{h'}(s, t)h'(st) = f_{h'}(s, t)l(st)h(st),$$

mais

$$\begin{aligned} h'(s)h'(t) &= l(s)h(s)l(t)h(t) \\ &= l(s)h(s)l(t)h(s)^{-1}h(s)h(t) \\ &= l(s)\,{}^s l(t) f_h(s, t)h(st), \end{aligned}$$

d'où l'on tire

$$\begin{aligned} f_{h'}(s, t) &= l(s)\,{}^s l(t) f_h(s, t) l(st)^{-1} \\ &= f_h(s, t)\,{}^s l(t) l(s) l(st)^{-1}, \end{aligned}$$

car A est commutatif. Or, en notation multiplicative, on a

$$dl(s,t) = {}^{s}l(t)l(s)l(st)^{-1}.$$

D'où

$$f_{h'} = f_h\, dl.$$

Donc, quand h varie, f_h ne change que par multiplication par un cobord. On peut donc associer à E la classe de cohomologie de f_h dans $H^2(G, A)$; appelons e cette classe. Quand trouve-t-on $e = 0$? Cela signifie (en notation multiplicative) qu'il existe une section h telle que $f_h(s,t) = 1$ pour tous $s, t \in G$, i.e. que h est un homomorphisme.

Définition 4.6 *Une extension E de G par A est dite* triviale *s'il existe un homomorphisme $h : G \to E$ telle que $\pi \circ h = \mathrm{Id}_G$ (ou, de façon équivalente, si $e = 0$).*

Examinons une telle extension : tout élément de E s'écrit $ah(s)$ de manière unique et $ah(s)bh(t) = a\,{}^{s}bh(st)$. Donc on connaît E dès qu'on connaît A, G et l'action de G sur A. Le groupe E est isomorphe au groupe des couples (a, s) avec $a \in A$ et $s \in G$, muni de la loi

$$(a,s)(b,t) = (a\,{}^{s}b, st).$$

On appelle un tel E un *produit semi-direct* de G par A. On vient de voir : la classe nulle de $H^2(G, A)$ correspond à l'extension triviale de G par A, qui est le produit semi-direct de G par A défini par l'action de G sur A.

Théorème 4.2 *L'application f_h est un 2-cocycle de G à valeurs dans A.*

Il faut vérifier que f_h appartient au noyau de d, l'homomorphisme de cobord. L'écriture est ici multiplicative ; il faut donc voir que

$$df_h(u,v,w) = 1$$

pour tous $u, v, w \in G$; or df_h s'écrit

$$df_h(u,v,w) = {}^{u}f_h(v,w)f_h(u,vw)f_h(uv,w)^{-1}f_h(u,v)^{-1}.$$

Nous allons écrire $h(u)h(v)h(w)$ sous la forme $ah(uvw)$ avec $a \in A$ de deux manières différentes en utilisant l'associativité de la loi de groupe dans E.
On a

$$\big(h(u)h(v)\big)h(w) = f_h(u,v)f_h(uv,w)h(uvw)$$

et

$$h(u)\big(h(v)h(w)\big) = {}^{u}f_h(v,w)f_h(u,vw)h(uvw)$$

d'où

$${}^{u}f_h(v,w)f_h(u,vw) = f_h(u,v)f_h(uv,w)$$

ce qui est bien

$$df_h(u,v,w) = 1.$$ □

Nous allons enfin voir :

Théorème 4.3 *Toute classe de cohomologie de $H^2(G, A)$ correspond à une extension de G par A.*

On va reconstruire la situation précédente : soit $f \in Z^2(G, A)$. Définissons E ensemblistement par $E = A \times G$. On définit la loi de E par

$$(a, s)(b, t) = \big(a\,{}^s b f(s, t), st\big).$$

Tout d'abord E est un groupe :

• La loi est associative : le calcul fait ci-dessus pour voir que f_h est un 2-cocycle à partir de l'associativité de la loi de E se reprend à l'envers.

• Si $\varepsilon = f(1, 1)^{-1}$, alors l'élément $(\varepsilon, 1)$ est élément neutre. En effet,

$$(a, s)(\varepsilon, 1) = \big(a\,{}^s\varepsilon f(s, 1), s\big)$$

or f est un 2-cocycle donc $df = 1$ et

$$df(s, 1, 1) = {}^s f(1, 1) f(s, 1)^{-1} f(s, 1) f(s, 1)$$

donc

$$1 = df(s, 1, 1) = {}^s\varepsilon^{-1} f(s, 1)^{-1}$$

et $(\varepsilon, 1)$ est bien élément neutre.

• On fait de même le calcul de l'inverse.

On a un homomorphisme surjectif évident de E dans G :

$$\begin{cases} E & \longrightarrow & G \\ (a, s) & \longmapsto & s \end{cases}$$

et l'application

$$\begin{cases} A & \longrightarrow & E \\ a & \longmapsto & (a\varepsilon, 1) \end{cases}$$

est un homorphisme (car A est abélien) évidemment injectif.

Finalement on a bien :

$$\{1\} \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow \{1\}. \qquad \square$$

Interprétation de $H^1(G, A)$ en termes d'extensions. Soit E une extension triviale de G par A. Choisissons une section $h : G \to E$ qui soit un homomorphisme (ce qui identifie E au produit semi-direct $G.A$). Soit h' une autre section ; on peut écrire h' de façon unique comme $h' = l.h$, où l est une 1-cochaîne $G \to A$. On a $f_{h'} = f_h.dl = dl$ puisque $f_h = 1$. Pour que h' soit un homomorphisme, il faut et il suffit que $f_{h'} = 1$, i.e. que $dl = 1$, autrement dit que l soit un 1-cocycle.

D'autre part, si on conjugue h par un élément a de A, on obtient une section qui est un homomorphisme. Soit h' cette section. A quoi cela correspond-il en termes de l ? On a

$$h'(x) = ah(x)a^{-1} = l(x)h(x)$$

avec $l(x) = a\,{}^x a^{-1}$. Donc $l = df_a$ (où f_a est l'élément de $C^0(G, A)$ correspondant à a). Donc l doit être un cobord. D'où :

Théorème 4.4 *Les classes de conjugaison (par les éléments de A, ou de G) des sections de E qui sont des homomorphismes correspondent bijectivement aux éléments du groupe de cohomologie $H^1(G, A)$.*

[Noter que cette correspondance *dépend* du choix de h. Une façon plus intrinsèque de s'exprimer consiste à dire que l'ensemble des classes de sections-homomorphismes est un espace principal homogène (« torseur ») sous l'action de $H^1(G, A)$.]

Corollaire 4.5 *Pour que les sections de π qui sont des homomorphismes soient conjuguées, il faut et il suffit que $H^1(G, A) = \{0\}$.*

4.3 Groupes finis : un critère de nullité

Soit G un groupe à m éléments et soit A un G-module.

Théorème 4.6 *Soient $n \geqslant 1$ et $x \in H^n(G, A)$. On a $mx = 0$.*

Soit $f \in Z^n(G, A)$ un n-cocycle représentant x. Il faut construire $F \in C^{n-1}(G, A)$ tel que $dF = mf$.
Prenons $F_1(s_1, \ldots, s_{n-1}) = \sum_{s \in G} f(s_1, \ldots, s_{n-1}, s)$. Comme $f \in Z^n(G, A)$, on a $df = 0$. Or

$$\begin{aligned} df(s_1, \ldots, s_{n+1}) &= s_1 f(s_2, \ldots, s_{n+1}) - f(s_1 s_2, s_3, \ldots, s_{n+1}) + \cdots \\ &\quad + (-1)^n f(s_1, \ldots, s_n s_{n+1}) + (-1)^{n+1} f(s_1, \ldots, s_n) \\ &= 0. \end{aligned}$$

Donc

$$\begin{aligned} \sum_{s_{n+1} \in G} df(s_1, \ldots, s_{n+1}) &= s_1 F_1(s_2, \ldots, s_n) - F_1(s_1 s_2, \ldots, s_n) + \cdots \\ &\quad + (-1)^n F_1(s_1, \ldots, s_{n-1}) + (-1)^{n+1} m f(s_1, \ldots, s_n). \end{aligned}$$

On a utilisé le fait que si s_{n+1} parcourt G, $s_n s_{n+1}$ aussi (s_n étant fixé). On a ainsi obtenu

$$(-1)^n m f(s_1, \ldots, s_n) = dF_1(s_1, \ldots, s_n).$$

On pose donc $F = (-1)^n F_1$ qui vérifie $dF = mf$, d'où le résultat. $\square$

Corollaire 4.7 *Si l'application $a \mapsto ma$ est un automorphisme de A (m étant l'ordre de G) alors $H^n(G, A) = \{0\}$ pour tout $n \geqslant 1$.*

En effet, $x \mapsto mx$ est alors un automorphisme de $C^n(G, A)$ qui commute à d. Donc c'est un automorphisme de $H^n(G, A)$ par passage au quotient. Or c'est dans ce cas l'application nulle d'où $H^n(G, A) = \{0\}$. $\square$

Corollaire 4.8 *Si G et A sont finis d'ordres premiers entre eux alors $H^n(G, A) = \{0\}$ pour tout $n \geqslant 1$.*

En effet $a \mapsto ma$ est alors un automorphisme de A. $\square$

Corollaire 4.9 *Si G et A sont finis d'ordres premiers entre eux alors :*

(1) Toute extension E de G par A est triviale.

(2) Deux homomorphismes sections de $G \to E$ sont conjugués par un élément de A.

On a $H^n(G, A) = \{0\}$ si $n \geqslant 1$. Le cas $n = 2$ donne (1) et le cas $n = 1$ donne (2) d'après l'étude faite en 4.2. $\square$

4.4 Extensions de groupes d'ordres premiers entre eux

Nous allons étendre certains résultats sur les extensions d'un groupe G par un groupe A commutatif au cas où A est résoluble ou même quelconque.

Théorème 4.10 (Zassenhaus) *Soient A et G deux groupes finis d'ordres premiers entre eux et considérons une extension $\{1\} \to A \to E \to G \to \{1\}$. Alors :*

*(1) Il existe un sous-groupe de E (*supplémentaire de A*) qui se projette isomorphiquement sur G (E est produit semi-direct).*

(2) Si A ou G est résoluble, deux tels sous-groupes sont conjugués par un élément de A (ou de E, cela revient au même).

On raisonne par récurrence sur $|E|$; on peut supposer A et G distincts de $\{1\}$.

Premier cas : A est résoluble. On démontre d'abord le

Lemme 4.11 *Soit X un groupe résoluble non réduit à $\{1\}$. Il existe un nombre premier p et un p-sous-groupe Y de X distinct de $\{1\}$ tel que Y soit abélien élémentaire et caractéristique.*

On rappelle qu'un p-groupe abélien est dit *élémentaire* si ses éléments distincts de 1 sont d'ordre p et qu'un sous-groupe d'un groupe X est caractéristique s'il est stable par tout automorphisme de X.

Démonstration du lemme. Soient $D^i(X)$ les dérivés successifs de X. Comme X est résoluble, il existe i tel que $D^i(X)$ est distinct de $\{1\}$ et $D^{i+1}(X)$ est réduit à $\{1\}$. Alors $D^i(X)$ est un sous-groupe de X abélien et différent de $\{1\}$. De plus, il est caractéristique. Soit alors p divisant l'ordre de $D^i(X)$ et soit Y le groupe des éléments de $D^i(X)$ d'ordre divisant p. Alors Y est abélien, différent de $\{1\}$, caractéristique (un automorphisme de X transforme un élément d'ordre p en un autre de même ordre) et est un p-groupe élémentaire. $\square$

Retour à la démonstration du théorème. Appliquons le lemme avec $X = A$ et $Y = A'$ et remarquons que A' est normal dans E : un automorphisme intérieur de E restreint à A est un automorphisme de A (car A est normal dans E) et laisse donc A', qui est caractéristique, invariant.
Si $A = A'$, alors A est abélien et le théorème est connu. Sinon, comme A' est normal dans E, on peut passer au quotient par A' et on obtient la suite exacte

$$\{1\} \longrightarrow A/A' \longrightarrow E/A' \longrightarrow G \longrightarrow \{1\}\,.$$

La situation se décrit par le diagramme suivant :

$$\begin{tikzcd} & E \arrow[d] \\ & E/A' \arrow[d] \\ G \arrow[r] \arrow[uur, dotted] \arrow[ur, dotted] & E/A \end{tikzcd}$$

Comme E/A' est de cardinal strictement inférieur à celui de E, l'hypothèse de récurrence entraîne que G se relève en un sous-groupe G' de E/A'. Soit E' l'image réciproque de G' par la projection $E \to E/A'$. Alors on a la suite exacte

$$\{1\} \longrightarrow A' \longrightarrow E' \longrightarrow G' \longrightarrow \{1\}\ .$$

Or A' est abélien. D'après le § 4.3, on peut donc relever G' en un sous-groupe de E'. On obtient ainsi un relèvement de G dans E.

Montrons que deux tels relèvements G' et G'' sont conjugués par un élément de A. On a

$$E = A.G' \quad \text{et} \quad E = A.G''.$$

L'hypothèse de récurrence, appliquée à E/A', montre qu'il existe $a \in A$ tel que $aG'a^{-1}$ et G'' aient même image dans E/A'. Quitte à remplacer G' par $aG'a^{-1}$, on peut donc supposer que $A'.G' = A'.G''$. La conjugaison par un élément de A de G' et G'' résulte alors du cas abélien (cf. § 4.3), appliqué à $A'.G' = A'.G''$.

Deuxième cas : assertion (1) *dans le cas général.* Soit p premier divisant l'ordre de A et soit S un p-Sylow de A (cf. § 2.2). Soit E' le normalisateur dans E de S. D'après le § 2.3, on a $E = A.E'$. Soit $A' = E' \cap A$; A' est normal dans E' et l'on a la suite exacte

$$\{1\} \longrightarrow A' \longrightarrow E' \longrightarrow G \longrightarrow \{1\}\ .$$

Distinguons deux cas :
- Si $|E'| < |E|$, l'hypothèse de récurrence permet de relever G dans E', donc dans E.
- Si $|E'| = |E|$ alors S est normal dans E donc aussi dans A. On passe au quotient :

$$\{1\} \longrightarrow A/S \longrightarrow E/S \longrightarrow G \longrightarrow \{1\}$$

avec E/S de cardinal strictement inférieur à celui de E. Par l'hypothèse de récurrence, G se relève en G_1 de E/S. Soit E_1 l'image réciproque de G_1 par la projection $E \to E/S$. On a la suite exacte

$$\{1\} \longrightarrow S \longrightarrow E_1 \longrightarrow G \longrightarrow \{1\}.$$

Or S est un p-groupe donc est résoluble et l'on est ramené au premier cas.

Troisième cas : assertion (2) *lorsque G est résoluble.* Soient G et G' deux relèvements de G dans E. On a

$$E = A.G' \quad \text{et} \quad E = A.G''.$$

Soient p un nombre premier et I un sous-groupe abélien normal différent de $\{1\}$ de G (cf. lemme 4.11) et soit $\widetilde{I}$ son image réciproque dans E par la projection $E \to G$. Soient $I' = \widetilde{I} \cap G'$ et $I'' = \widetilde{I} \cap G''$. On a

$$A.I' = A.I'' \ (= \widetilde{I}).$$

Les groupes I' et I'' sont des p-Sylow de $\widetilde{I}$; il existe donc $x \in \widetilde{I}$ tel que $I'' = xI'x^{-1}$; si on écrit x sous la forme ay avec $a \in A$ et $y \in I'$, on a $I'' = aI'a^{-1}$. Quitte à remplacer I' par $aI'a^{-1}$, on peut donc supposer $I'' = I'$.

Soit N le normalisateur de $I' = I''$ dans E. On a $G' \subset N$ et $G'' \subset N$. Si N est distinct de E, l'hypothèse de récurrence appliquée à N montre que G' et G'' sont conjugués. Si $N = E$, autrement dit si I' est normal dans E, l'hypothèse de récurrence appliquée à E/I' montre qu'il existe $a \in A$ tel que $I'.aG'a^{-1} = I'.G''$. Puisque I' est normal et contenu à la fois dans G' et G'', cela entraîne

$$aG'a^{-1} = G'',$$

d'où le résultat. □

Remarque. L'hypothèse « A ou G est résoluble » faite dans (2) est automatiquement satisfaite d'après le théorème de Feit-Thompson (cf. § 3.1) disant que tout groupe d'ordre impair est résoluble.

4.5 Relèvements d'homomorphismes

Soient $\{1\} \to A \to E \xrightarrow{\pi} \Phi \to \{1\}$ une suite exacte , G un groupe et φ un homomorphisme de G dans Φ. Peut-on relever φ en un homomorphisme ψ de G dans E ?

$$\begin{tikzcd}
\{1\} \arrow[r] & A \arrow[r] & E \arrow[r, "\pi"] & \Phi \arrow[r] & \{1\} \\
 & & & G \arrow[u, "\varphi"'] \arrow[ul, dotted, "\psi"] &
\end{tikzcd}$$

La question équivaut à celle du relèvement de G dans une extension E_φ de G par A associée à φ, définie de la façon suivante :

$$E_\varphi = \{(g, e) \in G \times E \mid \varphi(g) = \pi(e)\}$$

muni de la loi de groupe habituelle pour le produit cartésien. Alors A se plonge dans E_φ par $a \mapsto (1, a)$ et E_φ se projette sur G par $(g, e) \mapsto g$.

$$\begin{tikzcd}
E_\varphi \arrow[r] \arrow[d] & E \arrow[d, "\pi"] \\
G \arrow[r, "\varphi"] & \Phi
\end{tikzcd}$$

On a la suite exacte

$$\{1\} \longrightarrow A \longrightarrow E_\varphi \longrightarrow G \longrightarrow \{1\} .$$

(on dit parfois que E_φ est *l'image réciproque* (« pull-back ») de l'extension E par l'homomorphisme φ).

Voyons l'équivalence des deux problèmes. Soit ψ un relèvement de φ. Alors l'ensemble $G_\psi = \{(g, \psi(g)),\ g \in G\}$ est un sous-groupe de E_φ qui est un relèvement de G.
Soit maintenant G' un relèvement de G. Alors G' est formé de couples (g, e) avec $g \in G$ et $e \in E$, chaque $g \in G$ apparaissant dans un et un seul couple. Alors ψ défini par $\psi(g) = e$ est un homomorphisme qui relève φ.
De plus, deux relèvements ψ' et ψ'' sont conjugués par $a \in A$ si et seulement si $G_{\psi'}$ et $G_{\psi''}$ sont conjugués par $(1, a) \in E_\varphi$. Le § 4.4 donne alors le

Théorème 4.12 *Soit $\{1\} \to A \to E \to \Phi \to \{1\}$ une suite exacte et soit φ un homomorphisme d'un groupe G dans le groupe Φ. Supposons G et A finis d'ordres premiers entre eux. Alors :*

(1) Il existe un homomorphisme ψ de G dans E qui relève φ.

(2) Si G ou A est résoluble, deux tels homomorphismes sont conjugués par un élément de A.

Application. On se donne un homomorphisme $\varphi : G \to \mathbf{GL}_n(\mathbf{Z}/p\mathbf{Z})$ où p ne divise pas l'ordre de G. On va voir qu'*on peut relever φ en $\varphi_\alpha : G \to \mathbf{GL}_n(\mathbf{Z}/p^\alpha\mathbf{Z})$ pour tout $\alpha \geqslant 1$.*

Commençons par relever φ en φ_2. On a la suite exacte

$$\{1\} \longrightarrow A \longrightarrow \mathbf{GL}_n(\mathbf{Z}/p^2\mathbf{Z}) \longrightarrow \mathbf{GL}_n(\mathbf{Z}/p\mathbf{Z}) \longrightarrow \{1\}$$

où A est formé des matrices de la forme $1 + pX$ avec X matrice $n \times n$ modulo p et où l'application de $\mathbf{GL}_n(\mathbf{Z}/p^2\mathbf{Z})$ dans $\mathbf{GL}_n(\mathbf{Z}/p\mathbf{Z})$ est la réduction modulo p. Le groupe A est alors isomorphe à $\mathbf{M}_n(\mathbf{Z}/p\mathbf{Z})$ qui est un p-groupe abélien. On peut donc appliquer le théorème précédent et relever φ en φ_2 de manière essentiellement unique.
Le même argument permet de relever φ_α en $\varphi_{\alpha+1}$. On a la suite exacte

$$\begin{tikzcd}
\{1\} \arrow[r] & A \arrow[r] & \mathbf{GL}_n(\mathbf{Z}/p^{\alpha+1}\mathbf{Z}) \arrow[r] & \mathbf{GL}_n(\mathbf{Z}/p^\alpha\mathbf{Z}) \arrow[r] & \{1\} . \\
& & G \arrow[u, "\varphi_{\alpha+1}"] \arrow[ur, "\varphi_\alpha"'] & &
\end{tikzcd}$$

On peut passer à la limite projective : comme $\varprojlim (\mathbf{Z}/p^\alpha\mathbf{Z}) = \mathbf{Z}_p$, on obtient une représentation

$$\varphi_\infty : \ G \longrightarrow \mathbf{GL}_n(\mathbf{Z}_p) \hookrightarrow \mathbf{GL}_n(\mathbf{Q}_p) .$$

Or $\mathbf{Q}_p$ est de caractéristique 0 : ainsi, à partir d'une représentation en caractéristique p, on en obtient une en caractérisque 0.

Chapitre 5

Groupes résolubles et sous-groupes de Hall

Nous allons essayer de généraliser les théorèmes de Sylow. Le problème était alors le suivant : soit G un groupe d'ordre $\prod_p p^{\alpha(p)}$ (où p est premier), existe-t-il, pour tout nombre premier p, un sous-groupe de G d'ordre $p^{\alpha(p)}$?
On peut se demander si, plus généralement, pour tout n divisant l'ordre de G, on peut trouver un sous-groupe de G d'ordre n. C'est vrai si G est nilpotent, mais faux sans hypothèse sur G ; même « G résoluble » est insuffisant : le groupe $\mathcal{A}_4$, d'ordre 12 est résoluble et n'a pas de sous-groupe d'ordre 6. On va donc faire des hypothèses plus restrictives sur n.

5.1 Π-sous-groupes

Soit Π un ensemble de nombres premiers et soit Π' son complémentaire. Si $n \in \mathbf{N}$, on écrit $n = n_\Pi n_{\Pi'}$, avec n_Π (resp. $n_{\Pi'}$) divisible uniquement par des éléments de Π (resp. Π'). Un groupe G est appelé un Π-*groupe* si tous les facteurs premiers de l'ordre de G appartiennent à Π.
Le problème consiste en la recherche des Π-sous-groupes d'un groupe donné et de ses Π-sous-groupes maximaux tels qu'ils sont définis ci-dessous.

Définition 5.1 *Soit G un groupe et soit Π un ensemble de nombres premiers. On appelle* Π-Sylow *ou* Π-sous-groupe de Hall *de G un sous-groupe H tel que $|H| = |G|_\Pi$.*

Remarque. Si $\Pi = \{p\}$, un Π-Sylow de G est un p-Sylow de G.

Théorème 5.1 (P. Hall) *Soient G un groupe résoluble et Π un ensemble de nombres premiers. Alors :*

(1) G possède des Π-Sylow.

(2) Soient S_Π un Π-Sylow de G et H un Π-sous-groupe de G. Alors H est contenu dans un conjugué de S_Π.

La démonstration de ce théorème sera donnée au § 5.4.

Corollaire 5.2 *Deux Π-Sylow d'un groupe résoluble sont conjugués.*

L'hypothèse « résoluble » est essentielle :

Théorème 5.3 *Si pour tout ensemble Π de nombres premiers, G possède un Π-Sylow, alors G est résoluble.*

La démonstration sera donnée au § 5.6.

Théorème 5.4 (Burnside) *Soient p et q deux nombres premiers. Tout groupe d'ordre $p^a q^b$ $(a, b \in \mathbf{N})$ est résoluble.*

En effet, la question de l'existence de Π-Sylow ne se pose vraiment que si $\Pi = \{p\}$ ou $\{q\}$ ou $\{p, q\}$. Les théorèmes de Sylow (cf. § 2.2) répondent dans les deux premiers cas et G lui-même convient dans le troisième. Le th. 5.3 assure alors que G est résoluble. □

En fait le théorème de Burnside sera démontré en annexe (cf. th. A.21) par la théorie des caractères et il sera utilisé dans la démonstration du th. 5.3.

5.2 Préliminaires : sous-groupes permutables

Nous allons démontrer quelques lemmes sur les produits de sous-groupes.
Soient A et B deux sous-groupes d'un groupe G. Notons $A.B$ l'ensemble des produits ab, où $a \in A$ et $b \in B$.

Lemme 5.5 *Il y a équivalence entre :*

(1) $A.B = B.A$.

(2) $A.B$ *est un sous-groupe de* G.

(1) ⇒ (2) car si $A.B = B.A$, on a $A.B.A.B \subset A.A.B.B \subset A.B$ et $(A.B)^{-1} \subset B.A = A.B$ et $A.B$ est un sous-groupe de G.

(2) ⇒ (1) Si $A.B$ est un sous-groupe de G, on a $A.B = (A.B)^{-1} = B.A$. □

On dit que deux groupes A et B sont *permutables* si $A.B = B.A$.

Lemme 5.6 *Soient $A_1, \ldots, A_n$ des sous-groupes de G deux à deux permutables. Alors $A_1 \ldots A_n$ est un sous-groupe de G.*

La démonstration se fait par récurrence sur n. Le lemme 5.5 donne le cas $n = 2$. D'après l'hypothèse de récurrence, $A_1 \ldots A_{n-1}$ est un groupe. Il est permutable avec A_n car $A_1 \ldots A_{n-1}.A_n = A_1 \ldots A_n.A_{n-1}$, d'où après $(n-1)$ opérations $A_1 \ldots A_{n-1}.A_n = A_n.A_1 \ldots A_{n-1}$. D'après le lemme 5.5, $A_1 \ldots A_n$ est un sous-groupe de G. □

Lemme 5.7 *Il y a équivalence entre :*

(1) $A.B = G$.

(1') $B.A = G$.

(2) G *opère transitivement sur* $G/A \times G/B$.

De plus, si G est fini, ces propriétés sont équivalentes à chacune des suivantes :

(3) $(G : A \cap B) = (G : A).(G : B)$.

(3') $(G : A \cap B) \geqslant (G : A).(G : B)$.

En effet :
(1) $\Leftrightarrow$ (1′) car si $A.B = G$, $A.B$ est un sous-groupe et d'après le lemme 5.5, on a $A.B = B.A$, donc $B.A = G$.

(1) $\Rightarrow$ (2) Il s'agit de prouver que pour tous $g_1, g_2 \in G$, il existe $g \in G$ tel que $g \in g_1 A$ et $g \in g_2 B$. Or par hypothèse, il existe $a \in A$ et $b \in B$ tels que $g_1^{-1} g_2 = ab$, d'où $g_1 a = g_2 b^{-1}$ et l'élément $g = g_1 a = g_2 b^{-1}$ convient.

(2) $\Rightarrow$ (1) Le groupe G opère transitivement sur $G/A \times G/B$. Prenons donc, pour tout $g_1 \in G$, un élément $g \in G$ tel que $g \in 1.A$ et $g \in g_1.B$. Cela entraine $g_1 \in A.B$, i.e. $A.B = G$.

Soit maintenant G un groupe fini. Montrons (2) $\Leftrightarrow$ (3). Soit $\dot{1}$ l'image de l'élément unité de G dans G/A (resp. G/B). Le stablisateur de $(\dot{1}, \dot{1})$ par l'action de G sur $G/A \times G/B$ est $A \cap B$. Le nombre n d'éléments de l'orbite de $(\dot{1}, \dot{1})$ est donc l'indice $(G : A \cap B)$ de $A \cap B$ dans G. Or

$$\begin{aligned} G \text{ opère transitivement sur } G/A \times G/B \quad & \Longleftrightarrow \quad n = |G/A| \times |G/B| \\ & \Longleftrightarrow \quad n = (G : A)(G : B) \\ & \Longleftrightarrow \quad (G : A \cap B) = (G : A)(G : B), \end{aligned}$$

ce qui est bien l'équivalence entre (2) et (3).

(3′) $\Leftrightarrow$ (3) car $(G : A \cap B)$ est le cardinal de l'orbite de $(1, 1)$, cardinal majoré par celui de $G/A \times G/B$, qui est $(G : A)(G : B)$. □

Lemme 5.8 *Les propriétés du lemme 5.7 sont vraies si les indices de A et B dans G sont premiers entre eux.*

En effet, $(G : A \cap B)$ est divisible par $(G : A)$ et $(G : B)$ donc par leur produit, ce qui prouve (3′) du lemme précédent. □

5.3 Systèmes permutables de sous-groupes de Sylow

Soit G un groupe. Pour tout nombre premier p, choisissons un p-Sylow H_p de G. Nous dirons que le système $\{H_p\}$ est *permutable* si les H_p sont deux à deux permutables au sens du § 5.2. Dans ce cas, si Π est un ensemble de nombres premiers, le groupe $H_\Pi = \prod_{p \in \Pi} H_p$ est un Π-sous-groupe de G.

Théorème 5.9 *Si G est résoluble, G possède un système permutable de sous-groupes de Sylow.*

La démonstration se fait par récurrence sur l'ordre de G. On suppose $G \neq \{1\}$; d'après le lemme 4.11, il existe alors un nombre premier p_0 et un p_0-sous-groupe normal A de G distinct de $\{1\}$. D'après l'hypothèse de récurrence, le groupe G/A possède un système permutable $\{H'_p\}$ de p-Sylow. Soit $H' = \prod_{p \neq p_0} H'_p$; c'est un sous-groupe de G/A d'ordre $\prod_{p\neq p_0} |H'_p|$. Soit G' son image réciproque dans G, on a une suite exacte :

$$\{1\} \longrightarrow A \longrightarrow G' \longrightarrow H' \longrightarrow \{1\} .$$

Comme A et H' sont d'ordres premiers entre eux, il existe un sous-groupe H de G qui relève H' (cf. §4.4). Si $p \neq p_0$, posons H_p le sous-groupe de H qui relève H'_p ; les H_p sont des p-Sylow de G deux à deux permutables. Pour $p = p_0$, définissons H_p comme l'image réciproque de H'_{p_0} dans G. C'est un p_0-Sylow de G qui permute aux H_p $(p \neq p_0)$. Le système $\{H_p\}$ répond donc à la question. □

5.4 Démonstration du th. 5.1

L'assertion (1) sur l'existence de Π-Sylow résulte du th. 5.9 et du lemme 5.6.

Prouvons l'assertion (2) par récurrence sur l'ordre de G. Prenons comme au § 5.3 un p_0-sous-groupe normal A de G distinct de $\{1\}$. Soient H' et S'_Π les images respectives de H et S_Π dans $G' = G/A$. D'après l'hypothèse de récurrence H' est contenu dans un conjugué de S'_Π. Quitte à remplacer H' par un de ses conjugués, on peut donc supposer $H' \subset S'_\Pi$. Il faut maintenant examiner deux cas :

• $p_0 \in \Pi$. Alors $A \subset S_\Pi$ car S_Π contient un p_0-Sylow S_0 de G et comme A est normal, $A \subset S_0$ (cf. les théorèmes de Sylow). L'inclusion $H' \subset S'_\Pi$ donne alors $H \subset S_\Pi$.

• $p_0 \notin \Pi$. Alors les ordres de A et S_Π sont premiers entre eux et on a $A \cap H = \{1\}$, et $A \cap S_\Pi = \{1\}$. Les projections $H \to H'$ et $S_\Pi \to S'_\Pi$ sont des isomorphismes. Soit $\widetilde{H}$ le sous-groupe de S_Π qui se projette sur H' ; dans $A.H$ les groupes H et $\widetilde{H}$ sont des relèvements de H' ; ils sont donc conjugués (voir le § 4.4, th. 4.10). □

5.5 Un critère de résolubilité

Théorème 5.10 (Wielandt) *Soit G un groupe fini et soient H_1, H_2, H_3 trois sous-groupes de G. Si les H_i sont résolubles et si leurs indices sont premiers entre eux deux à deux, alors G est résoluble.*

La démonstration se fait par récurrence sur l'ordre de G. Remarquons tout d'abord que $G = H_1.H_2$. En effet, les indices $(G : H_1)$ et $(G : H_2)$ sont premiers entre eux, donc comme chacun d'eux divise $(G : H_1 \cap H_2)$, on a $(G : H_1 \cap H_2) \geqslant (G : H_1)(G : H_2)$ et d'après le lemme 5.7, on a $G = H_1.H_2$.

On peut supposer que $H_1 \neq \{1\}$. D'après le lemme 4.11, il existe un nombre premier p et un p-sous-groupe normal A de H_1 différent de $\{1\}$. On peut supposer que p ne divise pas $(G : H_2)$. Alors H_2 contient un p-Sylow de G , donc un conjugué de A. Comme $G = H_1.H_2$, tout conjugué de A est de la forme $h_2^{-1}h_1^{-1}Ah_1h_2$ avec $h_i \in H_i$ $(i = 1, 2)$ et comme A est normal dans H_1, et qu'un de ses conjugués est contenu dans H_2, tous ses conjugués sont dans H_2.

Soit $\widetilde{A}$ le sous-groupe de G engendré par les conjugués de A. Alors $\widetilde{A}$ est normal dans G et contenu dans H_2, donc $\widetilde{A}$ est résoluble. Soit H'_i l'image de H_i dans $G' = G/\widetilde{A}$. Les indices $(G' : H'_i)$ sont premiers entre eux deux à deux (car $(G' : H'_i)$ divise $(G : H_i)$) et les H'_i sont résolubles. L'hypothèse de récurrence montre alors que G' est résoluble ; donc G est résoluble. □

5.6 Démonstration du th. 5.3

Soit p un nombre premier et soit G un groupe. On appelle *p-complément* de G tout sous-groupe H de G qui est un p'-Sylow où p' est l'ensemble des nombres premiers différents de p.

Nous allons démontrer le th. 5.3 sous la forme apparemment plus forte suivante :

Théorème 5.11 *Si, pour tout nombre premier p, le groupe G a un p-complément, alors G est résoluble.*

On raisonne par récurrence sur $|G|$. On distingue deux cas.
• Le nombre des facteurs premiers de $|G|$ est $\leqslant 2$, autrement dit $|G|$ est de la forme $p^a q^b$, où p et q sont premiers. D'après un théorème de Burnside, (démontré grâce à la théorie des caractères, cf. § A.6), G est résoluble.
• Le nombre des facteurs de l'ordre de G est supérieur ou égal à 3. Soient p_i $(i = 1, 2, 3)$ de tels facteurs et H_i $(i = 1, 2, 3)$ un p_i-complément de G. Alors les indices $(G : H_i)$ pour $i = 1, 2, 3$ sont premiers entre eux deux à deux.
De plus, H_i possède un p-complément pour tout nombre premier p. En effet, si $p = p_i$, alors H_i est son propre p_i-complément. Sinon, soit H_p un p-complément pour G ; comme $(G : H_i)$ et $(G : H_p)$ sont premiers entre eux, le lemme 5.8 montre que

$$(G : H_i \cap H_p) = (G : H_i)(G : H_p),$$

d'où $(H_i : H_i \cap H_p)$ est la plus grande puissance de p divisant l'ordre de H_i. Comme $H_i \cap H_p$ est un p'-groupe, $H_i \cap H_p$ est un p-complément de H_i. D'après l'hypothèse de récurrence, H_i est résoluble. Mais alors G satisfait aux hypothèses du th. 5.10, donc G est résoluble. □

Chapitre 6

Groupes de Frobenius

6.1 Réunion des conjugués d'un sous-groupe

Théorème 6.1 (Jordan) *Soit G un groupe fini et soit H un sous-groupe de G distinct de G ; alors $\bigcup_{g\in G}(gHg^{-1}) \neq G$. De façon plus précise, on a :*

$$\Big|\bigcup_{g\in G} gHg^{-1}\Big| \leqslant |G| - \left(\frac{|G|}{|H|} - 1\right).$$

On sait évidemment que 1 appartient à $H \cap (gHg^{-1})$ pour tout $g \in G$. On raisonne sur $G - \{1\}$. On a

$$\bigcup_{g\in G}(gHg^{-1} - \{1\}) = \bigcup_{g\in G/H}(gHg^{-1} - \{1\})$$

d'où

$$\Big|\bigcup_{g\in G}(gHg^{-1} - \{1\})\Big| \leqslant \frac{|G|}{|H|}(|H| - 1)$$

puis

$$\Big|\bigcup_{g\in G} gHg^{-1}\Big| \leqslant |G| - \frac{|G|}{|H|} + 1. \qquad \square$$

On va voir que cette propriété reste vraie sans supposer que G est fini, pourvu que $(G : H) < \infty$. On utilise un lemme :

Lemme 6.2 *Soit G un groupe et soit H un sous-groupe de G d'indice fini n. Il existe un sous-groupe N normal dans G et contenu dans H, tel que l'indice $(G : N)$ divise $n!$.*

En effet, le groupe G agit sur $X = G/H$ qui a n éléments. On obtient ainsi un homomorphisme φ de G dans le groupe $\mathcal{S}_X$ des permutations de X qui est de cardinal $n!$. Le groupe $N = \ker\varphi$ répond à la question. $\square$

Si l'on applique le th. 6.1 à G/N et H/N, on constate que la réunion des conjugués de H ne remplit pas G modulo N donc, *a fortiori*, que $\bigcup_{g\in G} gHg^{-1} \neq G$. $\square$

Remarque. Le cas $G = SO_3(\mathbf{R})$ et $H = \mathbf{S}_1$ montre que l'hypothèse $(G : H) < \infty$ ne peut être supprimée.

Mentionnons deux reformulations du th. 6.1 :

Théorème 6.1' *Si un sous-groupe H de G rencontre toutes les classes de conjugaison de G, on a $H = G$.*

(C'est un critère souvent utilisé en théorie des nombres, G étant un groupe de Galois.)

Théorème 6.1" *Si G opère transitivement sur un ensemble X, et si $|X| \geqslant 2$, il existe un élément de G qui opère sans point fixe.*

En effet, si H est le fixateur d'un point de X, on choisit un élément qui n'appartient à aucun conjugué de H. □

Voici deux applications du théorème ci-dessus :

Tout corps fini est commutatif (théorème de Wedderburn). En effet, soit D un corps fini et soit F son centre. On sait que $(D : F)$ est un carré n^2 et que tout $x \in D$ est contenu dans un sous-corps L commutatif, contenant F et tel que $(L : F) = n$. Comme deux tels sous-corps sont isomorphes, le théorème de Skolem-Noether montre qu'ils sont conjugués. Si L est l'un d'eux et si l'on pose $G = D^*$ et $H = L^*$, on a $G = \bigcup gHg^{-1}$, d'où $G = H$, $n = 1$ et D est commutatif.

Racine d'une équation modulo p. Soit $f = X^n + a_1X^{n-1} + \cdots + a_n$ un polynôme à coefficients dans $\mathbf{Z}$, irréductible sur $\mathbf{Q}$. Si p est un nombre premier, notons f_p la réduction de f modulo p ; c'est un élément de $\mathbf{F}_p[X]$. Notons $\mathcal{P}_f$ l'ensemble des p tels que f_p ait une racines (au moins) dans $\mathbf{F}_p$. On va voir que la densité de $\mathcal{P}_f$ est strictement inférieure à 1 dès que $n \geqslant 2$. [On dit que $\mathcal{P}$ a une densité égale à ρ si

$$\frac{|\{p \leqslant x,\ p \in \mathcal{P}\}|}{|\{p \leqslant x\}|} \longrightarrow \rho \quad \text{pour } x \to +\infty.]$$

Soit $X = \{x_1, \ldots, x_n\}$ l'ensemble des racines de f dans une extension de $\mathbf{Q}$ et soit G le groupe de Galois de f. Ce groupe opère transitivement sur X ; on a $X \simeq G/H$ où H est le fixateur de x_1. On démontre (théorème de Chebotarev-Frobenius) que la densité de $\mathcal{P}_f$ existe, et est égale à

$$\frac{1}{|G|}\Big|\bigcup_{g\in G} gHg^{-1}\Big|.$$

Vu le théorème ci-dessus, cette densité est < 1.

Corollaire. Si $n \geqslant 2$, il existe une infinité de p tels que f_p n'ait aucune racine dans $\mathbf{F}_p$.

Pour plus de détails, voir J.-P Serre, *On a theorem of Jordan*, Bull. A.M.S 40 (2003), 429 – 440.

6.2 Groupes de Frobenius : définition

On va désormais s'intéresser aux couples (G, H) tels que

$$\Big|\bigcup_{g\in G} gHg^{-1}\Big| = |G| - \left(\frac{|G|}{|H|} - 1\right).$$

Cela signifie que $(gHg^{-1}-\{1\})$ et $(hHh^{-1}-\{1\})$ sont disjoints si g et h ne sont pas congrus modulo H, ou encore que H et gHg^{-1} sont d'intersection réduite à $\{1\}$ si $g \notin H$. On dit que H « ne rencontre pas ses conjugués ».
On s'intéresse au cas où H est un sous-groupe propre de G. Soit $X = G/H$. Une propriété équivalente est que tout élément de G (distinct de 1) a au plus un point fixe dans X si on fait agir G sur X, ou encore : tout élément de G qui fixe deux points est l'identité.

Exemple. Soit G le groupe des transformations h de la forme $h(x) = ax + b$, où a et b sont dans un corps fini $\mathbf{F}$, avec $a \neq 0$. Soit H le sous-groupe $\{x \mapsto ax\}$. Si N est le sous-groupe de G des translations, N est normal dans G, et G est le produit semi-direct de H par N. Alors (G, H) est un exemple de la situation précédente.

On va voir si cette propriété peut se généraliser.

Définition 6.1 *Un groupe G est dit* de Frobenius *s'il possède un sous-groupe H distinct de $\{1\}$ et de G tel que $\big|\bigcup_{g\in G} gHg^{-1}\big| = |G| - (|G|/|H| - 1)$. On parle dans ce cas pour (G, H) de* couple de Frobenius.

Exemples.
(1) Soient N et H deux groupes finis, où H agit sur N : à tout $h \in H$, on associe $\sigma_h : N \to N$ défini par $\sigma_h(n) = hnh^{-1}$. On a $\sigma_{h_1h_2} = \sigma_{h_1} \circ \sigma_{h_2}$ pour tous $h_1, h_2 \in H$. Soit G le produit semi-direct correspondant. Cherchons à quelle condition (G, H) est de Frobenius. Il faut et il suffit que $H \cap nHn^{-1} = \{1\}$ pour tout $n \in N-\{1\}$. En effet, soit $h \in H \cap nHn^{-1}$; alors h s'écrit $nh'n^{-1}$ avec $h' \in H$. On quotiente modulo N, ce qui fournit $h = h'$ $(G/N \simeq H)$. Donc $h = nhn^{-1}$ soit encore $n = h^{-1}nh = \sigma_{h^{-1}}(n)$. Donc n est fixé par $\sigma_{h^{-1}}$. Si $h \neq 1$, alors nécessairement $n = 1$.
Une condition nécessaire et suffisante pour que (G, H) soit de Frobenius est qu'il n'existe pas de couple (h, n) avec $h \neq 1$ et $n \neq 1$ tel que $\sigma_h(n) = n$, ou encore que H opère librement sur $N-\{1\}$. On a $\bigcup_{g\in G} gHg^{-1} = \{1\} \cup (G-N)$ d'où $G-\bigcup_{g\in G} gHg^{-1} = N-\{1\}$ (en effet $\bigcup_{g\in G} gHg^{-1} \subset \{1\}\cup(G-N)$ et il suffit de compter les éléments pour conclure).
(2) Soit p un nombre premier et soit $\mathbf{F}$ un corps fini contenant une racine ξ p-ième de l'unité. Soit N l'ensemble des matrices $p \times p$ triangulaires supérieures à éléments diagonaux égaux à 1. C'est un groupe. Soit H le groupe cyclique engendré par

$$\begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & \xi & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \xi^{p-2} & 0 \\ 0 & \dots & \dots & 0 & \xi^{p-1} \end{pmatrix}.$$

Alors H normalise N. Le groupe $G = N.H$ est le groupe des matrices triangulaires supérieures avec des ξ^k sur la diagonale. On vérifie que l'action de H est sans point fixe.

Ces exemples sont en fait caractéristiques ; on a en effet le

Théorème 6.3 (Frobenius) *Soit (G, H) un couple de Frobenius. Alors l'ensemble N des éléments de G non conjugués à un élément de H (ou égaux à 1) est un sous-groupe normal et on a $G = N.H$.*

Le point clé de la démonstration est que N est effectivement un sous-groupe : il repose sur la théorie des caractères ; nous le démontrerons plus tard (cf. Annexe, th. A.22). Le groupe N est alors normal (car invariant par conjugaison). D'autre part :

$$\Big|\bigcup_{g\in G} gHg^{-1}\Big| = |G| - \big((G:H) - 1\big),$$

donc $|N| = (G : H)$. Enfin $N \cap H = \{1\}$, d'où $G = N.H$. □

On démontre (nous ne le ferons pas) qu'un groupe G ne peut être un groupe de Frobenius que « d'une seule manière » : si (G, H_1) et (G, H_2) sont des couples de Frobenius, alors H_1 est conjugué de H_2. En particulier le sous-groupe normal N est unique.

On cherche maintenant à classer les groupes de Frobenius en étudiant la structure de N et celle de H.

6.3 Structure de N

On suppose que N et H sont distincts de $\{1\}$ et qu'ils interviennent dans le groupe de Frobenius G. Choisissons $x \in H$ d'ordre premier p. L'élément x définit un automorphisme de N d'ordre p sans point fixe $\neq 1$. D'où : N intervient dans un groupe de Frobenius si et seulement s'il possède un automorphisme σ d'ordre premier et sans point fixe distinct de 1.

Proposition 6.4 *Soit σ un automorphisme d'ordre p (non nécessairement premier) d'un groupe fini N sans point fixe autre que 1. Alors :*

(1) L'application $x \mapsto x^{-1}\sigma(x)$ (de N dans N) est bijective.

(2) Pour tout $x \in N$, on a $x\sigma(x)\sigma^2(x)\cdots\sigma^{p-1}(x) = 1$.

(3) Si x et $\sigma(x)$ sont conjugués dans N alors $x = 1$.

(1) Comme N est fini, il suffit de montrer que l'application est injective. Supposons $x^{-1}\sigma(x) = y^{-1}\sigma(y)$ avec $x, y \in N$. Alors $yx^{-1} = \sigma(yx^{-1})$ donc l'élément yx^{-1} est fixé par σ donc est égal à 1.

(3) Soit $x \in N$ et supposons qu'il existe $a \in N$ tel que $\sigma(x) = axa^{-1}$. D'après (1), il existe $b \in N$ tel que $a^{-1} = b^{-1}\sigma(b)$. Alors $\sigma(x) = \sigma^{-1}(b)bxb^{-1}\sigma(b)$ donc $\sigma(bxb^{-1}) = bxb^{-1}$, ce qui implique $bxb^{-1} = 1$ puis $x = 1$.

(2) Soit $a = x\sigma(x)\sigma^2(x)\cdots\sigma^{p-1}(x)$. On a

$$\sigma(a) = \sigma(x)\sigma^2(x)\cdots\sigma^{p-1}(x)x = x^{-1}ax,$$

donc $a = 1$ d'après (3). □

Corollaire 6.5 *Si l est un nombre premier, il existe un l-Sylow de N stable par σ.*

Soit S un l-Sylow de N. Le groupe $\sigma(S)$ est aussi un l-Sylow de N, donc il existe $a \in N$ tel que $aSa^{-1} = \sigma(S)$. On écrit $a^{-1} = b^{-1}\sigma(b)$, d'où $\sigma(b^{-1})bSb^{-1}\sigma(b) = \sigma(S)$, soit $bSb^{-1} = \sigma(b)\sigma(S)\sigma(b^{-1}) = \sigma(bSb^{-1})$. Donc bSb^{-1} est un l-Sylow de N stable par σ. □

Corollaire 6.6 *Si $a \in N$, l'automorphisme $\sigma_a : x \mapsto a\sigma(x)a^{-1}$ est conjugué à σ dans* $\mathrm{Aut}(G)$ *; en particulier, il est d'ordre p et sans point fixe.*

D'après 6.4 (1), il existe $b \in G$ tel que $a = b^{-1}\sigma(b)$; alors $\sigma_a(x) = b^{-1}\sigma(bxb^{-1})b$, donc $b\sigma_a(x)b^{-1} = \sigma(bxb^{-1})$ i.e. le diagramme suivant est commutatif :

$$\begin{tikzcd} N \arrow[r, "\sigma_a"] \arrow[d, "\text{conjugaison par } b^{-1}"'] & N \arrow[d, "\text{conjugaison par } b^{-1}"] \\ N \arrow[r, "\sigma"'] & N \end{tikzcd}$$

Ceci donne immédiatement le résultat. □

Exemples.
(1) Si $p = 2$, on a $x\sigma(x) = 1$ pour tout $x \in N$, donc $\sigma(x) = x^{-1}$. Comme σ est un automorphisme, N est abélien.

(2) Pour le cas $p = 3$ (Burnside), posons $\sigma(x) = x'$ et $\sigma^2(x) = x''$. La prop. 6.4 (2) appliquée à σ et σ^2 donne $xx'x'' = 1$ et $xx''x' = 1$, donc x' et x'' commutent ; pour les autres c'est évident, donc x, x' et x'' commutent. De même x et $ax'a^{-1}$ commutent pour tout a, ainsi que x et $ax''a^{-1}$. Donc x' et x'' commutent à tout conjugué de x. Or $x = (x'x'')^{-1}$ donc N la propriété suivante : deux éléments conjugués commutent, donc aussi x et (x, y). Finalement $\big(x, (x, y)\big) = 1$ pour tous $x, y \in N$. Le groupe dérivé de N est contenu dans le centre de N ; cela entraîne que N est nilpotent de classe au plus 2.

(3) Le cas $p = 5$ a été traité par Higman : le groupe N est alors nilpotent de classe au plus 6 (c'est la meilleure borne possible).

Thompson a généralisé ces résultats par le

Théorème 6.7 (Thompson) *N est nilpotent.*

Pour une démonstration, cf. [6, Kap. V, Haupsatz 8.14]. En ce qui concerne la classe de N, Higman a conjecturé que si p est l'ordre de G, la classe de N est $\leqslant \frac{p^2-1}{4}$.

6.4 Structure de H

Nous dirons que H a la propriété $\mathcal{F}$ s'il existe un groupe G contenant H et distinct de H tel que le couple (G, H) soit un couple de Frobenius. D'après les théorèmes de Frobenius et de Thompson, cela revient à dire qu'il existe un groupe nilpotent $N \neq \{1\}$ sur lequel H opère *sans point fixe* (i.e. librement sur $N - \{1\}$).

Exemple. Soit $\mathbf{F}$ un corps fini de caractéristique l et soit H un sous-groupe de $\mathbf{SL}_2(\mathbf{F})$ d'ordre premier à l. Si l'on prend pour N le $\mathbf{F}$-espace vectoriel $\mathbf{F}^2$, on vérifie facilement que H opère librement sur $N - \{0\}$. Donc H a la propriété $\mathcal{F}$. (Ceci s'applique notamment au groupe icosaédral binaire d'ordre 120, groupe qui n'est pas résoluble.)

Théorème 6.8 *Soit H un groupe fini. Les propriétés suivantes sont équivalentes :*

(1) H a la propriété $\mathcal{F}$ (i.e. H intervient dans un couple de Frobenius).

(2) Il existe un corps K et une représentation linéaire $\rho : H \to \mathbf{GL}_n(K)$, avec $n \geqslant 1$, telle que ρ soit « sans point fixe »(i.e. H opère librement sur $K^n - \{0\}$).

(3) Pour tout corps K dont la caractéristique ne divise pas $|H|$, il existe une représentation linéaire $\rho : H \to \mathbf{GL}_n(K)$ sans point fixe.

(4) On peut faire opérer H linéairement et librement sur une sphère $\mathbf{S}_{n-1}$.

[Noter que (2) et (3) entraînent que ρ est fidèle.]

Avant de donner la démonstration, faisons quelques remarques sur la propriété suivante d'un corps K, notée (2_K) : il existe une représentation $H \to \mathbf{GL}_n(K)$ sans point fixe (avec $n \geqslant 1$).

(a) *Cette propriété ne dépend que de la caractéristique p de K.*
En effet, si elle est satisfaite par K et si x est un vecteur non nul de K^n, les transformés par H de x engendrent un espace vectoriel de dimension finie N sur le corps premier K_0 (i.e. $\mathbf{F}_p$ ou $\mathbf{Q}$), d'où une représentation $H \to \mathbf{GL}_N(K_0)$ sans point fixe. Par extension des scalaires, on en déduit une pour tout corps contenant K_0.

(b) *Si (2_K) est vraie, la caractéristique p de K est, soit 0, soit un nombre premier ne divisant pas $|H|$.*
En effet, si H opère librement sur $\mathbf{F}_p^n - \{0\}$, l'ordre de H divise $p^n - 1$ et n'est donc pas divisible par p.

(c) *La propriété (2_K) en caractéristique 0 entraîne la propriété analogue en toute caractéristique p ne divisant pas $|H|$.*
En effet, d'après (a), il existe un $\mathbf{Q}$-espace vectoriel V de dimension finie $\geqslant 1$ où H opère sans point fixe. Soit $x \in V$ non nul et soit L le $\mathbf{Z}$-réseau de V engendré par les transformés de x par H. Le groupe H opère sans point fixe sur L. Il opère aussi sur le $\mathbf{F}_p$-espace vectoriel $V_p = L/pL$. Montrons que cette action est sans point fixe, dès lors que p ne divise pas l'ordre de H. Si $s \in H$ est d'ordre m, l'automorphisme s_V de V défini par s est tel que $s_V^m = 1$, et il n'admet pas 1 pour valeur propre. On a donc

$$1 + s_V + s_V^2 + \cdots + s_V^{m-1} = 0.$$

A fortiori, la même équation vaut dans V_p et elle entraîne (vu que m est premier à p) que $sx \neq x$ pour tout $x \in V_p$ non nul. D'où la propriété (2_K) pour $\mathbf{F}_p$.

(d) *La propriété (2_K) en caractéristique $p \neq 0$ entraîne la propriété analogue en caractéristique 0.*
Soit en effet $\rho_p : H \to \mathbf{GL}_n(\mathbf{Z}/p\mathbf{Z})$ une représentation linéaire de H sans point fixe. D'après (b), p ne divise pas $|H|$. D'après ce qu'on a vu au chapitre 4, on peut relever ρ_p en un homomorphisme $\rho_{p^\infty} : H \to \mathbf{GL}_n(\mathbf{Z}_p)$, où $\mathbf{Z}_p = \varprojlim \mathbf{Z}/p^\nu\mathbf{Z}$ est l'anneau des entiers p-adiques. Comme $\mathbf{Z}_p \subset \mathbf{Q}_p$, on obtient ainsi une représentation linéaire $H \to \mathbf{GL}_n(\mathbf{Q}_p)$ de caractéristique nulle. Cette représentation est sans point fixe. En effet, si $x = (x_1, \ldots, x_n)$ est un vecteur fixe non nul, on peut supposer (quitte à multiplier x par un scalaire) que les x_i appartiennent à $\mathbf{Z}_p$ et que l'un d'eux n'est pas divisible par p. La réduction modulo p des x_i donne alors un vecteur non nul de $\mathbf{F}_p^n$ fixe par H, contrairement à l'hypothèse.

Ceci fait, la démonstration du théorème est immédiate. En effet, il résulte de (a), (b), (c) et (d) que (2_K) est indépendante de K. D'où l'équivalence (2) $\Leftrightarrow$ (3) du théorème. Prouvons maintenant :

(1) $\Rightarrow$ (2) Si H opère sans point fixe sur le groupe nilpotent $N \neq \{1\}$, le centre C de N n'est pas réduit à $\{1\}$. Si p est un facteur premier de $|C|$, le groupe $\mathcal{C}_p$ des éléments $x \in N$ tels que $x^p = 1$ est un $\mathbf{F}_p$-espace vectoriel non nul où H opère sans point fixe.

(3) $\Rightarrow$ (1) On choisit pour K un corps fini. On obtient ainsi une action sans point fixe de H sur un groupe abélien élémentaire.

(4) $\Rightarrow$ (2) On prend $K = \mathbf{R}$.

(3) $\Rightarrow$ (4) On prend $K = \mathbf{R}$. On obtient une représentation linéaire $\rho : H \to \mathbf{GL}_n(\mathbf{R})$ sans point fixe. Comme H est fini, il existe sur $\mathbf{R}^n$ une forme quadratique définie positive invariante par H (prendre la somme des transformés par H de la forme quadratique standard $\sum x_i^2$) : quitte à conjuguer ρ, on peut donc supposer que $\rho(H)$ est contenu dans le groupe orthogonal $\mathbf{O}_n(\mathbf{R})$, donc laisse stable la sphère $\mathbf{S}_{n-1}$ d'équation

$$\sum_{i=1}^{n} x_i^2 = 1.$$

Ceci achève la démonstration du théorème. $\square$

Remarques.
(1) On peut classer les groupes H ayant la propriété $\mathcal{F}$, cf. [12].

(2) Dans (4), on ne peut pas supprimer la condition que H opère linéairement sur $\mathbf{S}_{n-1}$. Exemple : $\mathbf{SL}_2(\mathbf{F}_p)$ pour $p \geqslant 7$.

Exercice. Soit H un groupe ayant la propriété $\mathcal{F}$. Montrer que :
(i) Tout sous-groupe abélien de H est cyclique.

(ii) Si p et q sont premiers, tout sous-groupe d'ordre pq de H est cyclique.

Inversement, si H est résoluble et si (i) et (ii) sont vérifiées, alors H a la propriété $\mathcal{F}$ (théorème de Vincent). Par contre, on peut montrer que le groupe $\mathbf{SL}_2(\mathbf{F}_{17})$ a les propriétés (i) et (ii), mais pas la propriété $\mathcal{F}$.

Chapitre 7

Transfert

7.1 Définition

Soient G un groupe et H un sous-groupe de G d'indice fini. Soit $X = G/H$ l'ensemble des classes à gauche selon H. Pour tout $x \in X$, on choisit un représentant $\bar{x}$ de x dans G. Le groupe G agit sur X. Si $s \in G$ et $x \in X$, l'élément $s\bar{x}$ de G a pour image sx dans X. Si $\overline{sx}$ désigne le représentant de sx, il existe donc $h_{s,x} \in H$ tel que $s\bar{x} = \overline{sx}\, h_{s,x}$. On pose :

$$\mathrm{Ver}(s) = \prod_{x \in X} h_{s,x} \pmod{(H,H)},$$

où le produit est calculé dans le groupe $H^{ab} = H/(H,H)$.

Théorème 7.1 (Schur) *L'application* Ver : $G \to H^{ab}$ *définie ci-dessus est un homomorphisme et ne dépend pas du choix du système de représentants* $\{\bar{x}\}_{x \in X}$.

On commence par montrer que l'application Ver est bien définie. Soit donc $\{\bar{x}'\}_{x\in X}$ un autre système de représentants ; calculons $\mathrm{Ver}'(s)$ le produit relatif aux $\bar{x}'$. L'élément $\bar{x}' \in X$ a pour image x dans X ; il existe donc $h_x \in H$ tel que $\bar{x}' = \bar{x}\, h_x$.
On a :

$$\begin{aligned} s\,\bar{x}' &= s\,\bar{x}\,h_x \\ &= \overline{sx}\,h_{s,x}\,h_x \\ &= \overline{sx}\,h_{sx}\,h_{sx}^{-1}\,h_{s,x}\,h_x \\ &= (\overline{sx})'\,h_{sx}^{-1}\,h_{s,x}\,h_x, \end{aligned}$$

d'où

$$\begin{aligned} \mathrm{Ver}'(s) &= \prod h_{sx}^{-1}\,h_{s,x}\,h_x \pmod{(H,H)} \\ &= \left(\prod h_{sx}\right)^{-1} \prod h_{s,x} \prod h_x \pmod{(H,H)}, \end{aligned}$$

car H^{ab} est abélien[1]. Or $\prod h_{sx} = \prod h_x$ car sx parcourt X quand x parcourt X, d'où :

$$\mathrm{Ver}'(s) = \prod h_{s,x} = \mathrm{Ver}(s) \pmod{(H,H)},$$

et l'application Ver est bien définie.
Montrons à présent qu'il s'agit d'un homomorphisme. Soient $s, t \in G$, on a :

$$\begin{aligned} st\,\bar{x} &= s\,\overline{tx}\,h_{t,x} \\ &= \overline{stx}\,h_{s,tx}\,h_{t,x}, \end{aligned}$$

[1]Afin d'éviter les lourdeurs d'écriture, il est sous-entendu que les produits sont étendus aux $x \in X$.

d'où :

$$\begin{aligned}\mathrm{Ver}(st) &= \prod h_{s,tx}\, h_{t,x} \pmod{(H,H)}\\ &= \prod h_{s,tx} \prod h_{t,x} \pmod{(H,H)},\end{aligned}$$

car H^{ab} est abélien. Or $\prod h_{s,tx} = \prod h_{s,x}$ car tx parcourt X quand x parcourt X.
D'où $\mathrm{Ver}(st) = \prod h_{s,x} \prod h_{t,x} = \mathrm{Ver}(s)\mathrm{Ver}(t) \pmod{(H,H)}$. □

Comme H^{ab} est abélien, l'homomorphisme Ver se factorise en un homomorphisme de G^{ab} dans H^{ab} (que nous noterons encore Ver), appelé *transfert*.

Remarque. Le transfert est *fonctoriel* pour les isomorphismes : si σ est un isomorphisme du couple (G, H) sur le couple (G', H'), le diagramme

$$\begin{tikzcd} G^{ab} \arrow[r, "\sigma"] \arrow[d, "\mathrm{Ver}"'] & G'^{ab} \arrow[d, "\mathrm{Ver}"] \\ H^{ab} \arrow[r, "\sigma"] & H'^{ab} \end{tikzcd}$$

est commutatif (il suffit de constater que si $\{\bar{x}\}$ est un système de représentants de G/H alors $\{\sigma(\bar{x})\}$ en est un pour G'/H').
En particulier, si l'on prend $G = G'$, $H = H'$ et $\sigma(x) = gxg^{-1}$, avec $g \in N_G(H)$, ceci montre que l'image de l'homomorphisme Ver : $G^{ab} \to H^{ab}$ est contenue dans l'ensemble des éléments de H^{ab} fixés par $N_G(H)$.

7.2 Calcul du transfert

Soit H un sous-groupe d'indice fini de G et soit $X = G/H$. L'élément $s \in G$ opère sur X ; soit C le sous-groupe cyclique de G engendré par s. Alors C découpe X en orbites O_α. Soient $f_\alpha = |O_\alpha|$ et $x_\alpha \in O_\alpha$. On a $s^{f_\alpha} x_\alpha = x_\alpha$. Si g_α est un représentant de x_α, on a donc :

$$s^{f_\alpha} g_\alpha = g_\alpha h_\alpha, \text{ avec } h_\alpha \in H.$$

Proposition 7.2 *On a* $\mathrm{Ver}(s) = \prod_\alpha h_\alpha = \prod_\alpha g_\alpha^{-1} s^{f_\alpha} g_\alpha \pmod{(H,H)}$.

On prend pour système de représentants de X les éléments $s^i g_\alpha$, avec $0 \leqslant i < f_\alpha$. Si le représentant de $x \in X$ est de la forme $s^{f_\alpha - 1} g_\alpha$, l'élément $h_{s,x}$ correspondant de H est h_α ; les autres $h_{s,x}$ sont égaux à 1. La proposition en résulte. □

Corollaire 7.3 *Soit φ un homomorphisme de H^{ab} dans un groupe A. On suppose que $\varphi(h) = \varphi(h')$ lorsque les éléments $h, h' \in H$ sont conjugués dans G. Alors*

$$\varphi\big(\mathrm{Ver}(h)\big) = \varphi(h)^n,$$

pour tout $h \in H$, où $n = (G : H)$.

En effet, on a $\varphi\big(\mathrm{Ver}(h)\big) = \prod_\alpha \varphi(g_\alpha^{-1} h^{f_\alpha} g_\alpha)$. Or les éléments $g_\alpha^{-1} h^{f_\alpha} g_\alpha$ et h^{f_α} sont conjugués dans G, donc on a :

$$\varphi\big(\mathrm{Ver}(h)\big) = \textstyle\prod_\alpha \varphi(h^{f_\alpha}) = \prod_\alpha \varphi(h)^{f_\alpha}.$$

Le résultat se déduit alors de la relation $\sum_\alpha f_\alpha = \sum_\alpha |O_\alpha| = |X| = n$. □

Comme $H \subset G$, on a un morphisme naturel $H^{ab} \to G^{ab}$.

Corollaire 7.4 *L'homomorphisme composé* $G^{ab} \xrightarrow{\mathrm{Ver}} H^{ab} \longrightarrow G^{ab}$ *est* $s \mapsto s^n$.

C'est immédiat par la proposition, car

$$g_\alpha^{-1} s^{f_\alpha} g_\alpha = s^{f_\alpha} \pmod{(G,G)} \quad \text{et} \quad \textstyle\sum_\alpha f_\alpha = |X| = n. \qquad \square$$

Corollaire 7.5 *Si* G *est abélien, alors* $\mathrm{Ver} : G \to H$ *est donné par* $s \mapsto s^n$.

7.3 Exemples d'utilisation du transfert

7.3.1 Premier exemple (Gauss)

On fixe un nombre premier $p \neq 2$.

Soit $G = \mathbf{F}_p^*$ et soit $H = \{\pm 1\}$. Alors l'indice de H dans G est $(p-1)/2$ et le transfert est donné par $\mathrm{Ver}(x) = x^{(p-1)/2}$ pour $x \in \mathbf{F}_p^*$. Or c'est aussi le *symbole de Legendre* $\left(\frac{x}{p}\right)$. Ceci nous donne alors un moyen de calculer $\left(\frac{x}{p}\right)$.
On choisit le système de représentants de $X = G/H$ donné par $S = \{1, 2, \dots, (p-1)/2\}$. Soit $x \in G$ et soit $s \in S$. Si $xs \in S$, alors le $h_{s,x}$ correspondant vaut 1 ; sinon c'est -1. On pose donc :

$$\varepsilon(x,s) = \begin{cases} 1 & \text{si } xs \in S, \\ -1 & \text{si } xs \notin S. \end{cases}$$

On a $\mathrm{Ver}(x) = \prod_{s \in S} \varepsilon(x,s)$ (*lemme de Gauss*).

Calculons par exemple $\left(\frac{2}{p}\right)$ pour $p \neq 2$. On a $p = 1 + 2m$ et :

$$\begin{aligned} \left(\tfrac{2}{p}\right) &= (-1)^{m/2} && \text{si } m \text{ est pair}, \\ \left(\tfrac{2}{p}\right) &= (-1)^{(m+1)/2} && \text{si } m \text{ est impair}. \end{aligned}$$

D'où :

$$\begin{aligned} p \equiv 1 \pmod 8 &\Longrightarrow \left(\tfrac{2}{p}\right) = +1, \\ p \equiv 3 \pmod 8 &\Longrightarrow \left(\tfrac{2}{p}\right) = -1, \\ p \equiv 5 \pmod 8 &\Longrightarrow \left(\tfrac{2}{p}\right) = -1, \\ p \equiv 7 \pmod 8 &\Longrightarrow \left(\tfrac{2}{p}\right) = +1, \end{aligned}$$

ce qui se résume par : $\left(\frac{2}{p}\right) = 1 \Longleftrightarrow p \equiv \pm 1 \pmod 8$.

7.3.2 Second exemple

Proposition 7.6 *Si G est un groupe sans torsion contenant un sous-groupe H d'indice fini isomorphe à $\mathbf{Z}$, alors G lui-même est isomorphe à $\mathbf{Z}$.*

Quitte à remplacer H par l'intersection de ses conjugués, on peut supposer H normal dans G. Le groupe G agit sur H, d'où un homomorphisme $\varepsilon : G \to \mathrm{Aut}(H) = \{\pm 1\}$. Soit G' le noyau de ε ; alors $H \subset G'$ car H, étant abélien, agit trivialement sur lui-même par automorphismes intérieurs (H est même contenu dans le centre de G' car celui-ci agit trivialement sur H). Donc le transfert $\mathrm{Ver} : G'^{ab} \to H^{ab} = \mathbf{Z}$ est égal à $x \mapsto x^n$ où $n = (G' : H)$. Soit Φ le noyau de $\mathrm{Ver} : G' \to H^{ab}$, alors $\Phi \cap H = \{1\}$ car H est isomorphe à $\mathbf{Z}$, donc Φ est fini et même $\Phi = \{1\}$ puisque G est sans torsion. Donc G' est isomorphe à $\mathbf{Z}$. Si G est isomorphe à G', on a fini.
Sinon, on a $(G : G') = 2$, $G' \simeq \mathbf{Z}$ et G/G' opère sur G' par $y \mapsto y^{\pm 1}$. Soit donc $x \in G - G'$ tel que, pour un certain $y \in G'$, on ait $xyx^{-1} = y^{-1}$. Alors $x^2 \in G'$ car l'indice de G' dans G est 2. Prenons alors $y = x^2$, il vient $xx^2x^{-1} = x^{-2}$ d'où $x^2 = x^{-2}$ donc $x = 1$ car G est sans torsion. Donc G est isomorphe à $\mathbf{Z}$. □

Remarque. On a un résultat analogue (mais bien moins élémentaire) pour les groupes libres non abéliens (Stallings-Swan[2]).

7.4 Transfert dans un sous-groupe de Sylow

Théorème 7.7 *Soient H un p-Sylow d'un groupe G et $\varphi : H \to A$ un homomorphisme à valeurs dans un p-groupe abélien A. Alors :*

(1) Pour qu'il existe un prolongement de φ en un homomorphisme de G dans A, il faut et il suffit que, pour tous $h, h' \in H$ conjugués dans G, on ait $\varphi(h) = \varphi(h')$.

(2) Si cette condition est vérifiée, alors le prolongement est unique et donné par : $s \mapsto \varphi\big(\mathrm{Ver}(s)\big)^{1/n}$, où $n = (G : H)$, ce qui a bien un sens car n est premier à p.

(1) La condition est nécessaire car si $\widetilde{\varphi}$ est un prolongement de φ à G, alors pour $h \in H$ et $g \in G$ avec $g^{-1}hg \in H$, on a

$$\varphi(g^{-1}hg) = \widetilde{\varphi}(g)^{-1}\varphi(h)\widetilde{\varphi}(g) = \varphi(h)$$

car A est abélien.
La condition est suffisante car, n étant premier à p et A étant un p-groupe, $\varphi\big(\mathrm{Ver}(s)\big)^{1/n}$ a un sens (pour tout $a \in A$, il existe $b \in A$ unique tel que $b^n = a$) et l'application $s \mapsto \varphi\big(\mathrm{Ver}(s)\big)^{1/n}$ convient d'après le cor. 7.3.

(2) Ce prolongement est unique car φ est nécessairement égal à 1 sur les p'-Sylow de G lorsque $p' \neq p$. □

Théorème 7.8 *Soient H un p-Sylow abélien de G et N son normalisateur dans G. Alors l'image de l'homomorphisme $\mathrm{Ver} : G^{ab} \to H^{ab} = H$ est l'ensemble des éléments de H fixés par N (i.e. les éléments de H qui sont dans le centre de N).*

[2]Références : J.R. Stallings, *On torsion-free groups with infinitely many ends*, Ann. Math. 88 (1968), 312 – 334. R. Swan, *Groups of cohomological dimension one*, J. Algebra 12 (1969), 585 – 610.

Par la remarque faite à la fin du § 7.1, on a déjà l'inclusion de l'image de Ver dans $H^N = \{h \in H |\ xhx^{-1} = h, \forall\, x \in N\}$.
Montrons l'égalité. On a $N \supset H$ et $(N : H)$ est premier à p car H est un p-Sylow. On définit l'homomorphisme $\varphi : H \to H^N$ par $\varphi(h) = \big(\prod_{x\in N/H} xhx^{-1}\big)^{1/(N:H)}$.
On a bien $\prod_{x\in N/H} xhx^{-1} \in H^N$ car si $x' \in N$, on a :

$$x'\big(\prod_{x\in N/H} xhx^{-1}\big)x'^{-1} = \prod_{x\in N/H} x'xhx^{-1}x'^{-1} = \prod_{x\in N/H} xhx^{-1}.$$

De plus, comme H est abélien, si $h, h' \in H$ sont conjugués dans G, ils le sont dans N (cf. § 2.4) et on a alors $\varphi(h) = \varphi(h')$. D'après le cor. 7.3, on a

$$\varphi\big(\mathrm{Ver}(h)\big) = \varphi(h)^n,$$

pour $h \in H$, où n est l'indice de H dans G. Or, pour $h \in H^N$, on a $\varphi(h) = h$ et comme $\mathrm{Ver}(h) \in H^N$, on a, pour $h \in H^N$:

$$\mathrm{Ver}(h) = \varphi\big(\mathrm{Ver}(h)\big) = \varphi(h)^n,$$

i.e. $\mathrm{Ver}(h) = h^n$ si $h \in H^N$.
Comme H^N est un p-groupe et que n est premier à p, on obtient tous les éléments de H^N par les puissances n-ièmes d'éléments de H^N. Donc $\mathrm{Im}\,(\mathrm{Ver}) = H^N$. □

Théorème 7.9 *Soit H un p-Sylow de G. Supposons que H soit abélien différent de $\{1\}$ et que G n'ait pas de quotient cyclique d'ordre p. Soit N le normalisateur de H dans G. Alors :*

(1) L'ensemble H^N des éléments de H fixés par N est réduit à $\{1\}$.

(2) Si r est le rang de H (nombre minimum de générateurs), il existe un nombre premier l, distinct de p, qui divise à la fois $(N : H)$ et $\prod_{i=1}^{r}(p^i - 1)$.

(1) Si $H^N \neq \{1\}$, on a alors un homomorphisme non trivial $\mathrm{Ver} : G \to H^N$, où H^N est un p-groupe, d'où l'on tire un quotient cyclique d'ordre p de G.

Pour (2), soit H_p le sous-groupe de H formé des éléments x tels que $x^p = 1$; c'est un $\mathbf{F}_p$-espace vectoriel de dimension r $\big($puisque $H = \prod_{i=1}^{r}(\mathbf{Z}/p^{n_i}\mathbf{Z})\big)$. L'action de N sur H_p est non triviale par (1) ; elle définit un sous-groupe Φ de $\mathrm{Aut}(H_p) \simeq \mathbf{GL}_r(\mathbf{Z}/p\mathbf{Z})$. Si l est un facteur premier de l'ordre de Φ alors l divise l'ordre de N/H car Φ est un quotient de N/H (en effet, Φ est défini par l'action de N sur H, qui est en fait une action de N/H car H étant abélien, il agit trivialement sur lui-même). On a $l \neq p$, car p ne divise pas l'ordre de N/H ; comme Φ est un sous-groupe de $\mathbf{GL}_r(\mathbf{Z}/p\mathbf{Z})$, l divise l'ordre de $\mathbf{GL}_r(\mathbf{Z}/p\mathbf{Z})$, qui est $p^{r(r-1)/2}\prod_{i=1}^{r}(p^i - 1)$. D'où (2). □

Corollaire 7.10 *Si $p = 2$, le sous-groupe H n'est pas cyclique.*

En effet, on a alors $r \geqslant 2$ par le th. 7.9, mais on peut en donner une démonstration directe : si H est un 2-Sylow cyclique, soit h un générateur de H. Le groupe agit sur lui-même par translations. L'élément h découpe alors G en $|G/H|$ orbites. On envoie G dans $\{\pm 1\}$ en associant à $x \in G$ la signature de la permutation que x effectue sur G par l'action de translations. Or h est formé d'un nombre impair (i.e. précisément $|G/H|$) de cycles de la forme $(x, hx, \ldots, h^{2^n-1}x)$, où $|H| = 2^n$. Chacun de ces cycles est de signature (-1), donc la signature de h est (-1). On vient d'exhiber un homomorphisme non trivial de G dans $\{\pm 1\}$, d'où contradiction. □

Remarque. Le th. 7.9 montre que $N_G(H) \neq H$ quand celui-ci est un p-Sylow abélien d'un groupe sans quotient cyclique d'ordre p (sinon $H^N = H \neq \{1\}$).

7.5 Application : groupes simples d'ordre impair inférieur à 2000

En fait, on va montrer qu'il n'existe pas de groupe G d'ordre impair, avec $1 < |G| < 2000$, tel que $G = (G, G)$.
D'après le théorème de Burnside (cf. Annexe, th. A.21), il y a au moins trois facteurs premiers dans $|G|$; si p^α est le plus petit de ces facteurs, on a $p^{3\alpha} < 2000$, ce qui donne 5 cas possibles : $p^\alpha = 3, 5, 7, 9$ ou 11.

Cas $p^\alpha = 3$: le groupe G a un 3-Sylow d'ordre 3, donc cyclique, donc abélien. Soit N son normalisateur. D'après le th. 7.9, il existe l premier distinct de 3 qui divise à la fois $|N|$ et $(p-1) = 2$. Or $|N|$ est impair, c'est impossible.

Cas $p^\alpha = 5$: il s'exclut par un raisonnement analogue.

Cas $p^\alpha = 9$: on remarque de même que le 3-Sylow est d'ordre 3^2, donc abélien. Et le même raisonnement (dans les deux cas possibles : $r = 1$ ou $r = 2$) exclut ce cas.

Cas $p^\alpha = 7$: par le même théorème, on doit avoir l premier divisant $|N|$ (impair) et $p - 1 = 6$. Donc 3 divise $|G|$. Comme les cas précédents excluent $p^\alpha = 3$ ou 9, on a : 3^3 divise $|G|$. Par le théorème de Burnside, on a q premier, distinct de 3 et de 7, divisant l'ordre de G. Donc $|G| \geqslant 3^3.7.q^\beta$ et $q^\beta \geqslant 11$ (car si $q = 5$, un cas déjà vu montre que $\beta \geqslant 2$). Or c'est impossible, car $3^3.7.11 > 2000$.

Cas $p^\alpha = 11$: le th. 7.9, appliqué au 11-Sylow, montre qu'il existe l divisant $|N|$ et $p - 1 = 10$. D'après un cas précédent, on a alors $|G| \geqslant 11.5^2.q^\beta$ et $q^\beta \geqslant 13$, ce qui est impossible. $\square$

7.6 Application : groupes simples non abéliens d'ordre inférieur à 200

Dans ce §, on suppose $|G| \leqslant 200$.

Proposition 7.11

(1) On suppose $G = (G, G)$ *et* $G \neq \{1\}$*. Alors l'ordre de* G *est* $60, 120, 168$ *ou* 180*.*
(2) Si G *est simple non abélien, alors l'ordre de* G *est* 60 *ou* 168 *et* G *est isomorphe à* $\mathcal{A}_5$ *ou* $\mathbf{PSL}_2(\mathbf{F}_7)$*.*

(1) D'après le § précédent, l'ordre de G est pair et il est même divisible par 4 d'après le cor. 7.10 qui affirme la non-existence de 2-Sylow cycliques.
Cas où le 2*-Sylow* H *est d'ordre* 4. C'est alors $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Soit $N = N_G(H)$; N agit non trivialement sur H (puisque $H^N = \{1\}$, cf. th. 7.9), d'où un homomorphisme non trivial $N \to \mathrm{Aut}(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})$ (qui est d'ordre 6). Si N s'envoie sur un sous-groupe d'ordre 2 de $\mathrm{Aut} H$, alors $H^N \simeq \mathbf{Z}/2\mathbf{Z}$ (il suffit pour le voir d'examiner les automorphismes de $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$). Donc 3 divise l'ordre de N, donc aussi l'ordre de G. D'où cinq possibilités :
• $|G| = 4.3.13$: soit H un 13-Sylow et soit N son normalisateur. Alors $(G : N)$ est le nombre des 13-Sylow de G donc $(G : N) \equiv 1 \pmod{13}$; comme $(G : N)$ divise 4.3 cela implique $(G : N) = 1$ et donc H est normal : c'est impossible.
• $|G| = 4.3.11$: soit N le normalisateur d'un 11-Sylow H ; alors $(G : N)$ divise 4.3 et $(G : N) \equiv 1 \pmod{11}$, donc ou $(G : N) = 1$ et c'est impossible, ou $(G : N) = 12$ et alors $N = H$ puis $H^N = H$ (puisque H est abélien) et c'est impossible (cf. § 7.4).

• $|G| = 4.3.7$: soit N le normalisateur d'un 7-Sylow H. Alors $(G : N)$ divise 12 et $(G : N) \equiv 1 \pmod 7$; donc $(G : N) = 1$: c'est impossible.
• Restent les cas $|G| = 4.3.5 = 60$ ou $|G| = 4.3^2.5 = 180$ (les autres cas sont éliminés car sinon $|G| > 200$).
Cas où le 2*-Sylow* H *est d'ordre* 8. On a deux cas possibles : $|G| = 8.3.5$ ou $|G| = 8.3.7$, les autres cas donnent un ordre de G trop grand. De même, le cas $|H| > 8$ est éliminé pour des raisons d'ordre. Ceci donne l'assertion (1).

(2) Etudions les cas $|G| = 4.3^2.5$ et $|G| = 8.3.5$: soit H un 5-Sylow et soit N son normalisateur ; alors $(G : N) \equiv 1 \pmod 5$ et $(G : N)$ divise 4.3^2 dans un cas, 8.3 dans l'autre. Dans les deux cas, la seule possibilité est $(G : N) = 6$. Soit X l'ensemble des 5-Sylow de G. Le groupe G s'envoie dans le groupe des permutations de X, c'est-à-dire $\mathcal{S}_6$. Comme G est simple, il s'envoie dans $\mathcal{A}_6$. Or $\mathcal{A}_6$ est d'ordre 360 et G d'ordre 180 ou 120. Le groupe $\mathcal{A}_6$ ne peut avoir de sous-groupe d'indice m avec $1 < m < 6$ (ici ce serait 3 ou 2) sinon $\mathcal{A}_6$ se plongerait dans $\mathcal{S}_m$, ce qui est impossible puisque $|\mathcal{A}_6| > |\mathcal{S}_m|$.
Les seuls ordres possibles de groupes simples non abéliens inférieurs à 200 sont donc $4.3.5 = 60$ et $8.3.7 = 168$.

Structure des groupes simples d'ordre 60 *et* 168.

Ordre 60 : soit H un 2-Sylow de G ; alors H ne peut pas être cyclique (cor. 7.10) et donc (th. 7.9) 3 divise $|N|$ (N normalisateur de H). Donc 12 divise $|N|$ et $N \neq G$ donc $|N| = 12$. Ainsi G/N est d'ordre 5 et on a un homomorphisme non trivial de G dans $\mathcal{S}_5$. Comme G est simple, cela donne un plongement de G dans $\mathcal{A}_5$ et pour des raisons d'ordre, on a $G = \mathcal{A}_5$.

Ordre 168 : soit H un 7-Sylow de G et soit N son normalisateur. Alors $(G : N)$ divise 8.3 et $(G : N) \equiv 1 \pmod 7$. Comme $N \neq G$, on a $(G : N) = 8$. Donc $|N| = 21$. Considérons la suite exacte $\{1\} \to H \to N \to N/H \to \{1\}$. Comme l'ordre de H est premier à celui de N/H, le groupe N est produit semi-direct de N/H et de H (cf. th. 4.10). Le groupe N a donc deux générateurs : α (générateur de H) avec $\alpha^7 = 1$ et β (générateur de N/H) avec $\beta^3 = 1$. L'automorphisme $x \mapsto \beta x \beta^{-1}$ de H est d'ordre 3 ; c'est donc, soit $x \mapsto x^2$, soit $x \mapsto x^{-2}$. Quitte à remplacer β par β^{-1}, on peut supposer que c'est $x \mapsto x^2$. On a alors $\beta\alpha\beta^{-1} = \alpha^2$.
Soit X l'ensemble des 7-Sylow de G. Alors H opère sur X et fixe lui-même comme élément de X ; appelons cet élément ∞. On a $X = \{\infty\} \cup X_0$ avec $|X_0| = 7$. Le groupe H opère librement sur X_0 (car H est cyclique d'ordre 7). L'élément β opère sur X et fixe ∞ car $\beta \in N$. Comme $\beta^3 = 1$, il existe $x_0 \in X_0$ tel que $\beta x_0 = x_0$. Alors

$$X = \{x_0, \alpha x_0, \ldots, \alpha^6 x_0, \infty\}.$$

On identifie X à $\mathbf{P}_1(\mathbf{F}_7)$ en indexant $\alpha^i x_0$ par i.
L'élément α opère sur $\mathbf{P}_1(\mathbf{F}_7)$ par : $\alpha(i) = i + 1$ si $i < 6$, $\alpha(6) = 0$ et $\alpha(\infty) = \infty$. L'élément β opère par : $\beta(\infty) = \infty$, $\beta(0) = 0$; de plus $\beta\alpha = \alpha^2\beta$ d'où $\beta(i+1) = \beta(i)+2$ et $\beta(i) = 2i$ pour tout i. Ainsi α agit sur $\mathbf{P}_1(\mathbf{F}_7)$ comme une translation et β comme une homothétie. Soit C le sous-groupe cyclique de N engendré par β et soit M son normalisateur dans G. Comme C est un 3-Sylow cyclique de G, 2 divise $|M|$ (cf. th. 7.9). Le groupe M agit de façon non triviale sur C (cf. § 7.4) et donc il existe γ tel que $\gamma C \gamma^{-1} = C$ et $\gamma\beta\gamma^{-1} = \beta^{-1}$. Comme $\gamma \notin C$ et $\gamma \neq \alpha^n$ (car $\alpha \notin M$), γ peut être choisi d'ordre 2^n.

L'élément γ transforme une orbite de C en une orbite de C donc $\gamma(\{0,\infty\}) = \{0,\infty\}$. Or γ opère sans point fixe sur X, car sinon il serait conjugué à un élément de N, ce qui est impossible puisque $|N|$ est impair. Donc $\gamma(0) = \infty$ et $\gamma(\infty) = 0$. Comme γ^2 fixe ∞, on a $\gamma^2 \in N$. Comme γ est d'ordre pair, on a $\gamma^2 = 1$. Donc γ permute les deux orbites $\{1,2,4\}$ et $\{3,6,5\}$. Posons $\gamma(1) = \lambda$. Alors λ est égal à $3, 6$ ou 5. Comme $\gamma\beta = \beta^{-1}\gamma$, on a $\gamma(2i) \equiv \gamma(i)/2 \pmod 7$. D'où $\gamma(i) = \lambda/i$ et γ est une homographie. D'où $\gamma \in \mathbf{PGL}_2(\mathbf{F}_7)$. Comme $-\lambda$ est un carré, on a

$$\gamma(i) = \frac{-\mu}{\mu^{-1}i}$$

avec $\mu^2 = -\lambda$. Le déterminant de la matrice

$$\begin{pmatrix} 0 & -\mu \\ \mu^{-1} & 0 \end{pmatrix}$$

étant égal à 1, on a $\gamma \in \mathbf{PSL}_2(\mathbf{F}_7)$.
Or α, β et γ engendrent G. En effet, soit G' le sous-groupe de G engendré par ces éléments. Alors G' contient N et γ (d'ordre pair). Si $G' \neq G$, alors G' est d'indice 2 ou 4 et G s'envoie dans $\mathcal{A}_4$ ou $\mathcal{A}_2$, ce qui est impossible. Donc $G = G'$. On a un homomorphisme injectif $G \to \mathbf{PSL}_2(\mathbf{F}_7)$. Comme ces deux groupes ont le même ordre, c'est un isomorphisme. $\square$

Annexe A

Théorie des caractères

A.1 Représentations et caractères

Soient G un groupe, K un corps et V un espace vectoriel de dimension finie n sur le corps K. A partir du th. A.2, on suppose que $K = \mathbf{C}$ et que G est *fini*.

Définition A.1 *On appelle* représentation linéaire *de G dans V la donnée d'un homomorphisme ρ de G dans $\mathbf{GL}(V)$. La dimension de V est appelée le* degré *de la représentation.*

Remarques.
(1) On définit ainsi une opération de G sur V par $s.x = \rho(s)(x)$ pour $x \in V$ et $s \in G$.

(2) Si ρ est donné, V est appelé *espace de représentation* de G ou simplement *représentation* de G ; on écrit souvent ρ_V au lieu de ρ.

Si V_1 et V_2 sont des représentations de G associées aux homomorphismes ρ_1 et ρ_2, on peut définir :
• La somme directe $V_1 \oplus V_2$ de V_1 et V_2 : c'est la représentation $\rho : G \to \mathbf{GL}(V_1 \oplus V_2)$ telle que $\rho(s) = \rho_1(s) \oplus \rho_2(s)$. Si on choisit une base de $V = V_1 \oplus V_2$ associée à la décomposition en somme directe, la matrice associée dans cette base à $\rho(s)$ est la matrice :

$$\begin{pmatrix} A_1(s) & 0 \\ 0 & A_2(s) \end{pmatrix}$$

où $A_i(s)$ est la matrice associée à $\rho_i(s)$ dans la base de V_i correspondante.
• Le produit tensoriel $V_1 \otimes V_2$: $\rho(s)(x \otimes y) = \rho_1(s)(x) \otimes \rho_2(s)(y)$ pour tout $x \in V_1$ et tout $y \in V_2$.
• Le dual V_1^* de V_1 : $\rho(s).l(x) = l\big(\rho_1(s^{-1}).x\big)$ pour tout $l \in V_1^*$ et tout $x \in V_1$.
• $\mathrm{Hom}(V_1, V_2)$ que l'on peut identifier à $V_1^* \otimes V_2$: $\rho(s).h(x) = \rho_2(s)h\big(\rho_1(s)^{-1}.x\big)$ pour tout $x \in V_1$.
etc...

Caractère d'une représentation

Soit V un espace vectoriel muni d'une base $(e_i)_{1 \leqslant i \leqslant n}$ et ρ une application linéaire de V dans lui-même de matrice $a = (a_{ij})$. On note $\mathrm{Tr}(\rho) = \sum_i a_{ii}$ la trace de la matrice a

(elle est indépendante de la base choisie).
Si, maintenant V est une représentation d'un groupe fini G, on définit une fonction χ_V sur G à valeurs dans K par

$$\chi_V(s) = \mathrm{Tr}\big(\rho_V(s)\big)$$

où ρ_V est l'homomorphisme associé à la représentation V. La fonction χ_V est appelée le *caractère* de la représentation V.

Remarque. On a $\chi_V(1) = \dim V$.

Propriétés A.1

- χ_V *est une fonction centrale* $\big($i.e. $\chi_V(sts^{-1}) = \chi_V(t)$ si $s,t \in G\big)$,
- $\chi_{V_1 \oplus V_2} = \chi_{V_1} + \chi_{V_2}$,
- $\chi_{V_1 \otimes V_2} = \chi_{V_1}\chi_{V_2}$,
- $\chi_{V^*}(s) = \chi_V(s^{-1})$ *pour tout* $s \in G$,
- $\chi_{\mathrm{Hom}(V_1,V_2)}(s) = \chi_{V_1}(s^{-1})\chi_{V_2}(s)$ *pour tout* $s \in G$.

On suppose désormais que $K = \mathbf{C}$ *et que le groupe* G *est fini.* Soit V une représentation de G. On pose :

$$V^G = \{x \in V \mid s.x = x, \forall\, s \in G\}$$

$$\text{et} \quad \pi(x) = \frac{1}{|G|}\sum_{s \in G} s.x \quad \text{pour } x \in V.$$

On a $\pi(x) \in V^G$ et $\pi(x) = x$ si $x \in V^G$. Cela montre que π est un projecteur de V sur V^G. L'application π commute aux éléments de G : $\pi(s.x) = s.\pi(x)$ pour tout $s \in G$; on a donc

$$V = V^G \oplus \ker \pi.$$

Dans une base associée à cette décomposition, la matrice de π s'écrit :

$$\begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix}$$

d'où :

Théorème A.2 $\dim V^G = \mathrm{Tr}(\pi) = \dfrac{1}{|G|}\displaystyle\sum_{s \in G} \chi_V(s).$

Corollaire A.3 *Soit* $0 \to V' \to V \xrightarrow{f} V'' \to 0$ *une suite exacte de représentations de* G*. Alors tout élément de* V''^G *est image d'un élément de* V^G*.*

Soit $x'' \in V''^G$. La suite étant exacte, f est surjective et il existe $x \in V$ tel que $f(x) = x''$. Alors $\pi(x) \in V^G$ et $f\big(\pi(x)\big) = \pi\big(f(x)\big) = f(x) = x''$. □

Corollaire A.4 *Si* V' *est un sous-espace vectoriel de* V*, stable sous l'action de* G*, il existe un supplémentaire de* V' *dans* V *stable aussi sous l'action de* G*.*

Considérons la suite exacte :

$$0 \longrightarrow \mathrm{Hom}(V'', V') \longrightarrow \mathrm{Hom}(V'', V) \longrightarrow \mathrm{Hom}(V'', V'') \longrightarrow 0$$

où $V'' = V/V'$. Soit $x = \mathrm{Id}_{V''} \in \mathrm{Hom}(V'', V'')$; x est invariant sous l'action de G donc, d'après le cor. A.3, il existe $\varphi : V'' \to V$ invariant sous l'action de G et s'envoyant sur x. Donc φ commute avec G :

$$(s^{-1}.\varphi)(v) = \varphi(v) = s^{-1}.\varphi(sv)$$

si $v \in V''$ et $s \in G$. Donc $s.\varphi(v) = \varphi(s.v)$.
L'homomorphisme φ est une section (car $p \circ \varphi = x$ où $x = \mathrm{Id}_{V''}$ et $p : V \to V''$ projection) donc $V = V' \oplus \mathrm{Im}\,\varphi$ et $\mathrm{Im}\,\varphi$ est stable sous l'action de G. □

Définition A.2 *Soit $\rho : G \to \mathbf{GL}(V)$ une représentation linéaire de G. On dit qu'elle est* irréductible *si $V \neq 0$ et si aucun sous-espace vectoriel de V n'est stable par G, à part 0 et V.*

On a alors le

Théorème A.5 *Toute représentation est somme directe de représentations irréductibles.*

On raisonne par récurrence sur la dimension de la représentation V.
C'est évident si $\dim V \leqslant 1$. Sinon, ou bien V est irréductible, ou bien il existe un sous-espace vectoriel propre $\neq 0$ de V stable sous l'action de G donc, d'après le cor. A.4, il existe une décomposition en somme directe $V = V' \oplus V''$ avec $\dim V' < \dim V$ et $\dim V'' < \dim V$ et où V et V' sont stables par G. On applique l'hypothèse de récurrence à V' et V'' : ils sont sommes directes de représentations irréductibles donc aussi V. □

Remarque. Il n'y a pas unicité de la décomposition : si par exemple G opère trivialement sur V, décomposer V en somme directe de représentations irréductibles revient simplement à écrire V comme somme directe de droites, ce qui peut se faire de bien des façons (si $\dim V \geqslant 2$).

A.2 Relations d'orthogonalité

Théorème A.6 (lemme de Schur) *Soient $\rho_1 : G \to \mathbf{GL}(V_1)$ et $\rho_2 : G \to \mathbf{GL}(V_2)$ deux représentations irréductibles de G et soit f un homomorphisme de V_1 dans V_2 tel que $\rho_2(s) \circ f = f \circ \rho_1(s)$ pour tout $s \in G$. Alors :*

(1) Si V_1 et V_2 ne sont pas isomorphes, on a $f = 0$.

(2) Si $V_1 = V_2$ et $\rho_1 = \rho_2$, alors f est une homothétie.

(1) Si $x \in \ker f$, on a $f\big(\rho_1(s)\big).x = \big(\rho_2(s) \circ f\big).x = 0$ pour tout $s \in G$. Donc $\ker f$ est stable par G. Comme V_1 est irréductible, $\ker f = 0$ ou $\ker f = V_1$. Dans le premier cas f est injective, dans le second elle est nulle. De même $\mathrm{Im}\, f$ est stable sous G, donc $\mathrm{Im}\, f = 0$ ou V_2. Donc si $f \neq 0$, on a $\ker f = 0$ et $\mathrm{Im}\, f = V_2$: f est un isomorphisme de V_1 sur V_2, d'où (1).

(2) Soient maintenant $V_1 = V_2$ et $\rho = \rho_1 = \rho_2$. Soit $\lambda \in \mathbf{C}$ une valeur propre de f. Posons $f' = f - \lambda$; f' n'est pas injective. D'autre part $\rho(s) \circ f' = \rho(s) \circ (f - \lambda) = f' \circ \rho(s)$. Donc, d'après la première partie de la démonstration, $f' = 0$: f est une homothétie. □

Orthogonalité des caractères

Soient f et g des fonctions sur G. On pose :

$$\langle f, g\rangle = \frac{1}{|G|}\sum_{s\in G} f(s)g(s^{-1}).$$

C'est un produit scalaire.

Remarque. Si g est un *caractère*, on a $g(s^{-1}) = \overline{g(s)}$, de sorte que $\langle f, g\rangle$ se récrit comme un produit hermitien :

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

Théorème A.7 (orthogonalité des caractères) *Soient V et V' deux représentations irréductibles de caractères χ et χ'. Alors :*

$$\langle \chi, \chi'\rangle = \begin{cases} 1 & \text{si } V = V' \text{ et } \chi = \chi', \\ 0 & \text{si } V \text{ et } V' \text{ ne sont pas isomorphes.} \end{cases}$$

• Considérons $W = \mathrm{Hom}(V, V)$; c'est une représentation de G. Soit $\varphi \in W$; alors φ est fixé par G si et seulement si $\varphi \circ s = s \circ \varphi$ pour tout $s \in G$. Soit W^G l'ensemble des G-endomorphismes de V (endomorphismes fixés par G). D'après le lemme de Schur, on a $\dim W^G = 1$, donc

$$1 = \frac{1}{|G|}\sum_{s\in G} \chi_W(s),$$

d'après le th. A.2. Or $\chi_W(s) = \chi(s)\chi(s^{-1})$ donc $\langle \chi, \chi\rangle = 1$.

• Si V et V' ne sont pas isomorphes et si l'on pose $W = \mathrm{Hom}(V, V')$ et W^G l'ensemble des G-homomorphismes de V dans V', le lemme de Schur implique que $\dim W^G = 0$, d'où $\langle \chi, \chi'\rangle = 0$. □

Corollaire A.8 *Les caractères des différentes représentations irréductibles de G sont $\mathbf{C}$-linéairement indépendants (on les appelle les caractères irréductibles de G).*

Ceci va nous permettre de montrer que les caractères « caractérisent » les représentations de G.

Théorème A.9 *Soit V une représentation de G, de caractère χ_V, et soit $V = \bigoplus_{i=1}^{p} V_i$ une décomposition de V en somme directe de représentations irréductibles V_i (de caractères associés χ_{V_i}). Alors si W est irréductible de caractère χ_W, le nombre des V_i isomorphes à W est égal à $\langle \chi_V, \chi_W\rangle$.*

On a :

$$\begin{aligned} \chi_V &= \sum_{i=1}^{p} \chi_{V_i}, \\ \langle \chi_V, \chi_W\rangle &= \sum_{i=1}^{p} \langle \chi_{V_i}, \chi_W\rangle. \end{aligned}$$

Or d'après le théorème précédent, $\langle \chi_{V_i}, \chi_W\rangle$ vaut 1 ou 0 selon que V_i est ou n'est pas isomorphe à W. D'où le théorème. □

Corollaire A.10

• *Le nombre des V_i isomorphes à W ne dépend pas de la décomposition choisie* (en ce sens, il y a unicité de la décomposition).
• *Deux représentations de même caractère sont isomorphes.*
• *Si $(W_i)_{1\leqslant i\leqslant n}$ sont les représentations irréductibles de G, toute représentation V de G est isomorphe à une somme $\bigoplus n_i W_i$ (avec la convention : $n_i W_i = W_i \oplus \cdots \oplus W_i$, n_i fois) où $n_i = \langle \chi_V, \chi_{W_i} \rangle$.*

A.3 Caractères et fonctions centrales

On va maintenant chercher le nombre h de représentations irréductibles (à isomorphismes près), c'est-à-dire le nombre des caractères irréductibles.
Soit $\mathcal{C}$ le $\mathbf{C}$-espace vectoriel des fonctions centrales sur G (c'est-à-dire l'ensemble des fonctions constantes sur chaque classe de conjugaison de G). La dimension de $\mathcal{C}$ est égale au nombre de classes de conjugaison de G.

Théorème A.11 *Les caractères irréductibles $(\chi_1, \ldots, \chi_h)$ de G forment une base de $\mathcal{C}$ (en particulier, h est le nombre de classes de conjugaison de G).*

Pour démontrer ce théorème, on va utiliser le :

Lemme A.12 *Soit V une représentation irréductible de caractère χ et soit n la dimension de V (i.e. $n = \chi(1)$). Soit $f \in \mathcal{C}$ et soit π_f l'endomorphisme de V défini par :*

$$\pi_f = \sum_{s\in G} f(s^{-1})\rho_V(s).$$

Alors π_f est une homothétie de rapport $\lambda = \dfrac{1}{n}\displaystyle\sum_{s\in G} f(s^{-1})\chi(s) = \dfrac{|G|}{n}\langle f, \chi\rangle$.

Si $t \in G$, on a $\pi_f.t = \sum_{s\in G} f(s^{-1})\rho_V(st) = \sum_{s\in G} f(u^{-1})\rho_V(tu)$ (avec $u = t^{-1}st$), puisque f est centrale. Donc $\pi_f.t = t.\pi_f$. D'après le th. A.6, π_f est une homothétie et

$$\mathrm{Tr}(\pi_f) = n\lambda = \sum_{s\in G} f(s^{-1})\chi(s),$$

d'où $\lambda = \dfrac{|G|}{n}\langle f, \chi\rangle$. □

On en déduit la démonstration du th. A.11 : si les (χ_i) ne forment pas une base de $\mathcal{C}$, il existe $f \in \mathcal{C}$ non nulle et orthogonale aux χ_i. Donc par le lemme ci-dessus π_f est nulle pour toute représentation irréductible, donc (par décomposition en somme directe) pour toute représentation. On va calculer π_f pour une représentation particulière : soit V un espace de dimension $|G|$, muni d'une base $(e_s)_{s\in G}$. Soit ρ l'opération de G sur V définie par :

$$\rho(s).e_t = e_{st}.$$

La représentation ainsi définie est dite *représentation régulière* de G (son caractère se note r_G et on a $r_G(s) = 0$ si $s \neq 1$ et $r_G(1) = |G|$). Calculons π_f pour cette représentation. On a $\pi_f = \sum_{s\in G} f(s^{-1})\rho(s)$ donc $\pi_f(e_1) = \sum_{s\in G} f(s^{-1})e_s$ (car $e_{1.s} = e_s$). Si π_f est nulle, alors $f(s^{-1}) = 0$ pour tout $s \in G$ donc f est nulle (les $(e_s)_{s\in G}$ forment une base) ce qui contredit l'hypothèse. $\square$

Remarque. Chaque représentation irréductible W est contenue n fois dans la représentation régulière (avec $n = \dim W$). En effet, si χ est le caractère de W, on a :

$$\langle r_G, \chi\rangle = \frac{1}{|G|}\sum_{s\in G} r_G(s^{-1})\chi(s) = \chi(1) = \dim W.$$

Donc $r_G = \sum_{i=1}^{h} \chi_i(1)\chi_i$ avec χ_i irréductible. En particulier,

$$r_G(1) = |G| = \sum_{i=1}^{h} \chi_i(1)\chi_i(1)$$

d'où

$$|G| = \sum_{i=1}^{h} n_i^2$$

avec $n_i = \chi_i(1)$.

A.4 Exemples de caractères

On va déterminer les caractères irréductibles des groupes $\mathcal{A}_n$ ou $\mathcal{S}_n$ pour $n \leqslant 4$.

(1) Dans le cas trivial $\mathcal{S}_1 = \mathcal{A}_1 = \mathcal{A}_2 = \{1\}$, il y a un seul caractère irréductible : $\chi = 1$.

(2) Dans le cas où le groupe est $\mathcal{S}_2 = \{1, s\}$ (avec $s^2 = 1$), tout caractère irréductible est de degré 1 (par exemple car $|\mathcal{S}_2| = 2 = \sum n_i^2$ où n_i est le degré de χ_i irréductible). On a deux caractères irréductibles :

	1	s
χ_1	1	1
χ_2	1	-1

(3) Le groupe $\mathcal{A}_3 = \{1, t, t^2 \mid t^3 = 1\}$ est cyclique d'ordre 3. On a $|\mathcal{A}_3| = 3 = \sum n_i^2$ d'où trois représentations irréductibles de degré 1. Elles sont données par leurs caractères :

	1	t	t^2
χ_1	1	1	1
χ_2	1	ρ	ρ^2
χ_3	1	ρ^2	ρ

où ρ est une racine cubique de l'unité $\neq 1$.

(4) Le groupe symétrique $\mathcal{S}_3$ est le groupe diédral $\mathcal{D}_3$. On a trois classes de conjugaison $1, s, t$ avec $s^2 = 1, t^3 = 1$ et $sts^{-1} = t^{-1}$. Deux caractères irréductibles de degré 1 sont donnés par 1 et la signature. D'autre part $\chi_1 + \chi_2 + n_3\chi_3 = r_{\mathcal{S}_3}$ et $\sum n_i^2 = |\mathcal{S}_3| = 6 = 2 + n_3^2$ donc $n_3 = 2$ et χ_3 est de degré 2.
Ensuite,

$$(\chi_1 + \chi_2 + 2\chi_3)(s) = r_{\mathcal{S}_3}(s) = 0,$$

donc $\chi_3(s) = 0$, et de même

$$(\chi_1 + \chi_2 + 2\chi_3)(t) = r_{\mathcal{S}_3}(t) = 0,$$

donc $\chi_3(t) = -1$. On a donc :

	1	s	t
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

On peut trouver χ_3 directement en réalisant $\mathcal{S}_3$ comme groupe de symétries d'un triangle équilatéral. Alors s s'interprète comme symétrie par rapport à une droite, de matrice $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ donc de trace nulle, et t comme rotation d'angle $\frac{2\pi}{3}$ dont la trace est $2\cos(\frac{2\pi}{3}) = -1$.

(5) Le groupe $\mathcal{A}_4$ est d'ordre 12. On a quatre classes de conjugaison de représentants $1, s, t, t'$ où s est d'ordre 2 ($s = (a, b)(c, d)$), t d'ordre 3 ($t = (a, b, c)$) et $t' = t^2$. On a déjà les trois représentations du quotient d'ordre 3 de $\mathcal{A}_4$. Puis $\chi_1 + \chi_2 + \chi_3 + n_4\chi_4 = r_{\mathcal{A}_4}$ et $\sum n_i^2 = |\mathcal{A}_4| = 12$. D'où la table de caractères :

	1	s	t	t'
χ_1	1	1	1	1
χ_2	1	1	ρ	ρ^2
χ_3	1	1	ρ^2	ρ
χ_4	3	-1	0	0

On peut trouver χ_4 directement en regardant $\mathcal{A}_4$ comme un groupe de symétries d'un tétraèdre regulier. Alors s s'interprète comme la symétrie par rapport à une droite joignant les milieux de deux côtés opposés : sa matrice est

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

dans une base convenable, donc sa trace est -1. D'autre part, t s'interprète comme permutation circulaire donc sa trace est nulle.
Un autre argument permet de retrouver ce résultat : si W est une représentation irréductible de dimension 1 et si V est irréductible, alors $V \otimes W$ est irréductible. En particulier, $\chi_4\chi_2$ est irréductible et donc égal à χ_4 (pour des raisons de degré). D'où $\chi_4(t) = \chi_4(t') = 0$.

Exercice. On peut donner de même la table des caractères du groupe $\mathcal{S}_4$. Il y a cinq classes de conjugaison $1, \sigma, s, t, \tau$ avec $\sigma = (a, b)$, $s = (a, b)(c, d)$, $t = (a, b, c)$ et $\tau = (a, b, c, d)$. On trouve :

	1	σ	s	t	τ
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	2	-1	0
χ_4	3	1	-1	0	-1
χ_5	3	-1	-1	0	1

A.5 Propriétés d'intégralité

Soit G un groupe fini, soit ρ une représentation de G et soit χ son caractère.

Proposition A.13 *Les valeurs de χ sont des entiers algébriques.*

[On rappelle qu'un nombre complexe x est un *entier algébrique* s'il existe un entier $n > 0$ et des éléments $a_0, \ldots, a_{n-1} \in \mathbf{Z}$ tels que :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

L'ensemble des entiers algébriques forme un sous-anneau de $\mathbf{C}$.]

Démonstration. Le groupe G étant fini, il existe un entier $p > 0$ tel que $s^p = 1$ pour tout $s \in G$. Donc $\rho(s^p) = \rho(s)^p = 1$ pour tout s. Si λ est une valeur propre de $\rho(s)$, alors λ^p est une valeur propre de $\rho(s)^p$, donc $\lambda^p = 1$. Toute valeur propre de $\rho(s)$ est un entier algébrique, or $\chi(s)$ est la trace de $\rho(s)$ donc la somme des valeurs propres de $\rho(s)$: c'est aussi un entier algébrique. $\square$

Remarque. Pour tout $s \in G$, $\rho(s)$ est diagonisable. En effet, ρ est une application de G dans $\mathbf{GL}_n(\mathbf{C})$ et la matrice de $\rho(s)$, pour tout $s \in G$, est semblable à une matrice de Jordan J_s, décomposable en blocs de la forme :

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

Alors $\rho(s)^p$ est semblable à une matrice décomposable en blocs

$$\begin{pmatrix} \lambda^p & p & \cdots & \times \\ & \ddots & \ddots & \vdots \\ & & \ddots & p \\ & & & \lambda^p \end{pmatrix}.$$

Or $\rho(s)^p = 1$, ceci n'est possible que si J_s est en fait diagonale, d'où le résultat.

[Variante : appliquer le th. A.5 au groupe cyclique engendré par s.]

On va montrer comment la connaissance des caractères d'un groupe donne des renseignements sur ce groupe. Tout d'abord :

Proposition A.14 *Soit G un groupe distinct de $\{1\}$. Alors G est simple si et seulement si, pour tout $s \in G - \{1\}$ et tout caractère χ irréductible et distinct de 1, on a :*

$$\chi(s) \neq \chi(1).$$

Soient $(\lambda_i)_{1 \leqslant i \leqslant n}$ les valeurs propres de $\rho(s)$. On sait que les λ_i sont des racines de l'unité, donc que $|\lambda_i| = 1$. Comme $\chi(s) = \lambda_1 + \cdots + \lambda_n$ et $\chi(1) = n$, on a $\chi(s) = \chi(1) = n$ si et

seulement si $\lambda_i = 1$ pour tout i[1]. Donc $\chi(s) = n$ si et seulement si $s \in \ker\rho$.
Supposons maintenant que G soit simple. Alors $\ker\rho$ est un sous-groupe normal de G, c'est donc $\{1\}$ ou G. Donc si $\chi(s) = \chi(1)$ pour un $s \in G-\{1\}$ alors $\rho = \mathrm{Id}$ et donc $\chi = 1$.
Réciproquement, si G n'est pas simple, soit N un sous-groupe normal non trivial de G. Soit χ' un caractère non trivial de G/N associé à la représentation ρ'. Alors

$$G \longrightarrow G/N \xrightarrow{\rho'} \mathbf{GL}_n(\mathbf{C})$$

définit une représentation ρ de G de caractère $\chi \neq 1$ et telle qu'il existe $s \in G-\{1\}$ avec $\chi(s) = \chi(1)$. □

On va maintenant généraliser la prop. A.13 :

Théorème A.15 *Soit ρ une représentation irréductible d'un groupe G, de caractère associé χ. Soit f une fonction centrale sur G, dont les valeurs sont des entiers algébriques. Posons $n = \chi(1)$. Alors $n^{-1}\sum_{s\in G} f(s)\chi(s)$ est un entier algébrique.*

Il suffit de démontrer le théorème pour les fonctions valant 1 sur une classe de conjugaison et 0 ailleurs. Soit $s \in G$; notons $Cl(s)$ la classe de conjugaison de s et $c(s)$ le cardinal de $Cl(s)$. Soit f_s la fonction définie sur G, valant 1 sur $Cl(s)$ et 0 ailleurs. On a :

$$\frac{1}{n}\sum_{t\in G} f_s(t)\chi(t) = \frac{1}{n}\sum_{t\in Cl(s)} \chi(t) = \frac{c(s)\chi(s)}{n}$$

car χ est centrale. Il suffit donc de démontrer le :

Théorème A.16 *Avec les hypothèses du th. A.15 et les notations ci-dessus, $\frac{c(s)\chi(s)}{n}$ est un entier algébrique pour tout $s \in G$.*

Soit X l'ensemble des fonctions centrales sur G à valeurs dans $\mathbf{Z}$. C'est un $\mathbf{Z}$-module libre, engendré par les f_s. Il y a sur X une structure d'anneau naturelle, la *convolution*, définie par $f, g \mapsto f * g$ avec

$$f * g\,(s) = \sum_{uv=s} f(u)g(v).$$

On vérifie que l'anneau X est associatif et commutatif, et a pour élément unité la « fonction de Dirac » f_1.
Si $f \in X$, on lui associe l'endomorphisme $\rho(f) = \sum f(s)\rho(s)$. D'après le lemme A.12, $\rho(f)$ est une homothétie, i.e. appartient à $\mathbf{C}$. On obtient ainsi une application $\widetilde{\rho} : X \to \mathbf{C}$, qui est un homorphisme d'anneaux (en vertu de la formule $\rho(f*f') = \rho(f).\rho(f')$). L'image $\widetilde{\rho}(X)$ de X est donc un sous-anneau de $\mathbf{C}$ qui est un $\mathbf{Z}$-module de type fini. On déduit de là, par un argument standard, que les éléments de cet anneau sont des entiers algébriques. Comme $\frac{c(s)\chi(s)}{n}$ est égal à $\widetilde{\rho}(f_s)$, le théorème en résulte. □

Corollaire A.17 *Le degré de la représentation ρ divise l'ordre du groupe.*

En effet, soit $n = \chi(1)$ et soit f définie sur G par $f(s) = \chi(s^{-1})$. Alors f vérifie les hypothèses du th. A.15, donc $n^{-1}\sum_{s\in G}\chi(s^{-1})\chi(s)$ est un entier algébrique. Or $n^{-1}\sum_{s\in G}\chi(s^{-1})\chi(s) = |G|/n$ donc est dans $\mathbf{Q}$. Les seuls éléments de $\mathbf{Q}$ qui soient entiers sur $\mathbf{Z}$ sont les éléments de $\mathbf{Z}$, donc n divise $|G|$. □

[1] On utilise le résultat élémentaire suivant : si $\alpha_1, \ldots, \alpha_n \in \mathbf{C}$ sont de module 1, et si $|\alpha_1 + \cdots + \alpha_n| = n$, alors $\alpha_1 = \cdots = \alpha_n$.

Corollaire A.18 *Soit χ un caractère irréductible de degré n d'un groupe G et soit $s \in G$. Si $c(s)$ et n sont premiers entre eux, alors $\frac{\chi(s)}{n}$ est un entier algébrique. De plus, si $\chi(s) \neq 0$, alors $\rho(s)$ (associé à $\chi(s)$) est une homothétie.*

Si $c(s)$ et n sont premiers entre eux, il existe, d'après le théorème de Bézout, deux éléments $a, b \in \mathbf{Z}$ tels que $ac(s) + bn = 1$. Donc :

$$\frac{\chi(s)}{n} = \frac{ac(s)\chi(s)}{n} + b\chi(s).$$

Or $\chi(s)$ est un entier algébrique par la prop. A.13 et $\frac{c(s)\chi(s)}{n}$ aussi par le th. A.16. Cela démontre la première assertion du corollaire. Pour la seconde, nous utiliserons le :

Lemme A.19 *Soient $\lambda_1, \ldots, \lambda_n$ des racines de l'unité. Si $(\lambda_1 + \cdots + \lambda_n)/n$ est un entier algébrique, alors, soit $\lambda_1 + \cdots + \lambda_n = 0$, soit tous les λ_i sont égaux.*

Démonstration du lemme. Si λ est une racine de l'unité, son équation intégrale minimale est de la forme $x^p - 1 = 0$, donc tout conjugué de λ est aussi racine de l'unité [rappel : si $z \in \mathbf{C}$ est un nombre algébrique, on appelle conjugué de z toute racine de l'équation minimale de z]. Soit $z = (\lambda_1 + \cdots + \lambda_n)/n$; alors z est un entier algébrique par hypothèse et tout conjugué z' de z s'écrit $(\lambda'_1 + \cdots + \lambda'_n)/n$ où les λ'_i sont des racines de l'unité. Donc $|z'| \leqslant 1$. Notons Z le produit de tous les conjugués de z. Alors $|Z| \leqslant 1$. D'autre part Z est rationnel (c'est le terme constant, au signe près, du polynôme minimal de z). Enfin Z est entier algébrique (comme produit d'entiers algébriques) donc $Z \in \mathbf{Z}$. Si $Z = 0$, l'un des conjugués de z est nul donc $z = 0$; si $|Z| = 1$, tous les conjugués de z ont 1 comme module, donc $|z| = 1$ et tous les λ_i sont égaux, puisque leur somme est de module n (cf. note 1 à la prop. A.14). □

Revenons à la seconde assertion du corollaire. Soient (λ_i) les valeurs propres de $\rho(s)$; ce sont des racines de l'unité et $\chi(s) = \mathrm{Tr}(\rho(s)) = \sum \lambda_i$. On conclut avec le lemme. □

A.6 Application : théorème de Burnside

On reprend les notations du § précédent.

Théorème A.20 *Soient s un élément de $G - \{1\}$ et p un nombre premier. Supposons que $c(s)$ (= nombre d'éléments de G conjugués à s) soit une puissance de p. Alors il existe un sous-groupe normal N de G, distinct de G, tel que l'image de s dans G/N appartienne au centre de G/N.*

Soit r_G le caractère de la représentation régulière (cf. § A.3). On a $r_G(s) = 0$ car $s \neq 1$. D'autre part, $r_G = \sum n_\chi \chi$ (où l'on somme sur l'ensemble des caractères irréductibles) avec $n_\chi = \chi(1)$. Donc $\sum \chi(1)\chi(s) = 0$ ou encore $1 + \sum_{\chi \neq 1} \chi(1)\chi(s) = 0$ et donc $\sum_{\chi \neq 1} \frac{\chi(1)\chi(s)}{p} = -\frac{1}{p}$; or $-\frac{1}{p}$ n'est pas un entier algébrique. Donc il existe un caractère χ irréductible et distinct de 1 tel que $\frac{\chi(1)\chi(s)}{p}$ ne soit pas un entier algébrique. En particulier, $\chi(s) \neq 0$ et p ne divise pas $\chi(1)$, donc $c(s)$ et $\chi(1)$ sont premiers entre eux. D'après le cor. A.18, si ρ est la représentation de G attachée à χ, $\rho(s)$ est une homothétie. Soit alors $N = \ker \rho$; le groupe N est un sous-groupe de G, normal et distinct de G. D'autre part,

G/N s'identifie à l'image de ρ dans $\mathbf{GL}_n(\mathbf{C})$, or s s'envoie par ρ sur une homothétie, donc dans le centre de G/N. $\square$

On va en déduire le :

Théorème A.21 (Burnside) *Tout groupe G d'ordre $p^\alpha q^\beta$ (où p et q sont des nombres premiers) est résoluble.*

On suppose α et β non nuls (sinon G est nilpotent). On va démontrer le théorème par récurrence sur $|G|$.
Il existe $s \in G-\{1\}$ tel que q ne divise pas $c(s)$. En effet, $G = \{1\} \cup \{Cl(s)\}$ où les $Cl(s)$ sont les classes de conjugaison autres que 1. Donc $|G| = 1 + \sum |Cl(s)| = 1 + \sum c(s)$. Comme q divise $|G|$, il existe s tel que q ne divise pas $c(s)$. Or $c(s)$ divise $|G|$, donc $c(s)$ est une puissance de p. D'après ce qui précède, il existe un sous-groupe normal N de G, distinct de G, tel que l'image de s dans G/N soit dans le centre de G/N. Si $N \neq \{1\}$, l'hypothèse de récurrence appliquée à N et à G/N montre qu'ils sont résolubles ; donc G est résoluble. Si $N = \{1\}$, le centre C de G est non trivial puisqu'il contient s ; on peut appliquer l'hypothèse de récurrence à C et à G/C : G est résoluble. $\square$

A.7 Démonstration du théorème de Frobenius

Soient G un groupe fini et H un sous-groupe de G « ne rencontrant pas ses conjugués », c'est-à-dire tel que :

$$H \cap gHg^{-1} = \{1\}$$

pour tout $g \in G-H$, cf. § 6.2.

Théorème A.22 (Frobenius) *Soit $N = \{1\} \cup \{G - \bigcup_{g \in H} gHg^{-1}\}$. Alors N est un sous-groupe normal de G ; de plus G est produit semi-direct de H par N.*

La démonstration consiste à montrer que les représentations linéaires de H se prolongent à G tout entier. Tout d'abord :

Lemme A.23 *Soit f une fonction centrale sur H. Il existe une fonction centrale $\widetilde{f}$ sur G, et une seule, qui satisfait aux deux propriétés suivantes :*

(1) $\widetilde{f}$ prolonge f (i.e. $\widetilde{f}(h) = f(h)$ si $h \in H$),

(2) $\widetilde{f}(x) = f(1)$ si $x \in N$ (i.e. $\widetilde{f}$ est constante sur N).

C'est immédiat : si $x \notin N$, on écrit x sous la forme ghg^{-1}, avec $g \in G$, $h \in H$, et l'on pose $\widetilde{f}(x) = f(h)$; cela ne dépend pas du choix de g, h car si $g'h'g'^{-1} = ghg^{-1}$, on a $g'^{-1}ghg^{-1}g' = h'$, donc $h = h' = 1$ ou bien $g'^{-1}g \in H$; donc h et h' sont conjugués dans H, et, comme f est centrale, on a $f(h) = f(h')$. $\square$

Dans l'énoncé suivant, on utilise la notation $\langle \alpha, \beta \rangle_G$ pour désigner le produit scalaire $\frac{1}{|G|} \sum_{s \in G} \alpha(s^{-1})\beta(s)$ relatif au groupe G. De même $\langle \alpha, \beta \rangle_H$ désigne le produit scalaire relatif à H. Si F est une fonction sur G, on note F_H sa restriction à H.

Lemme A.24 *Soient f et $\widetilde{f}$ comme dans le lemme précédent, et soit θ une fonction centrale sur G. On a*

$$\langle \widetilde{f}, \theta \rangle_G = \langle f, \theta_H \rangle_H + f(1)\langle 1, \theta \rangle_G - f(1)\langle 1, \theta_H \rangle_H. \tag{A.1}$$

Démontrons cette égalité. Elle est vraie pour $f = 1$ car alors $\widetilde{f} = 1$. Par linéarité, il suffit donc de vérifier (A.1) pour les fonctions f telles que $f(1) = 0$. Soit alors $\mathcal{R}$ un système de représentants des classes à gauche modulo H : les différents conjugués de H sont les rHr^{-1} pour r décrivant $\mathcal{R}$ et tout conjugué d'un élément de H (distinct de 1) s'écrit de façon unique rhr^{-1} avec $r \in \mathcal{R}$ et $h \in H$. Cela dit,

$$\langle \widetilde{f}, \theta \rangle_G = \frac{1}{|G|} \sum_{s \in G} \widetilde{f}(s^{-1}) \theta(s)$$

et $\widetilde{f}$ est nulle en dehors des conjugués d'éléments de H ; donc

$$\begin{aligned} \langle \widetilde{f}, \theta \rangle_G &= \frac{1}{|G|} \sum_{(r,h) \in \mathcal{R} \times H} \widetilde{f}(h^{-1}) \theta(h) \\ &= \langle f, \theta_H \rangle_H \end{aligned}$$

puisque $|G| = |H|.|\mathcal{R}|$. □

Cas particulier : si $\theta = 1$, on a $\langle \widetilde{f}, 1 \rangle_G = \langle f, 1 \rangle_G$. L'application $f \mapsto \widetilde{f}$ est donc une isométrie, autrement dit : $\langle \widetilde{f_1}, \widetilde{f_2} \rangle_G = \langle f_1, f_2 \rangle_H$. En effet,

$$\frac{1}{|G|} \sum_{s \in G} \widetilde{f_1}(s^{-1}) f_2(s) = \langle f_1^* \widetilde{f_2}, 1 \rangle_G$$

où l'on a posé $f_1^*(s) = f_1(s^{-1})$, et

$$\langle \widetilde{f_1}, \widetilde{f_2} \rangle_G = \langle \widetilde{f_1^* \widetilde{f_2}}, 1 \rangle_G = \langle f_1^* f_2, 1 \rangle_H = \langle f_1, f_2 \rangle_H$$

car $\widetilde{f_1 f_2} = \widetilde{f_1}\widetilde{f_2}$. On en déduit :

Proposition A.25 *Si χ est un caractère de H et θ un caractère de G, alors $\langle \widetilde{\chi}, \theta \rangle_G$ est un entier.*

Il suffit de montrer que dans (A.1) tous les termes du membre de droite sont dans $\mathbf{Z}$, ce qui est clair. □

Soient $\theta_1, \ldots, \theta_n$ les différents caractères irréductibles de G ; on a $\widetilde{\chi} = \sum c_i \theta_i$ avec $c_i \in \mathbf{Z}$ pour tout i d'après ce qui précède.

Proposition A.26 *Supposons χ irréductible. Alors tous les c_i sont nuls, sauf l'un d'eux qui est égal à 1.*
(Autrement dit $\widetilde{\chi}$ est un caractère irréductible de G.)

En effet, $\langle \widetilde{\chi}, \widetilde{\chi} \rangle_G = \langle \chi, \chi \rangle_H = 1 = \sum c_i^2$ donc tous les c_i sont nuls sauf un, soit c_{i_0}, dont le carré est 1. Si c_{i_0} était égal à -1, on aurait $\widetilde{\chi} = -\theta_{i_0}$. Or $\widetilde{\chi}(1) = \chi(1) > 0$ et $\theta_{i_0}(1) > 0$, donc c'est impossible. Donc $c_{i_0} = 1$, i.e. $\widetilde{\chi} = \theta_{i_0}$. □

Corollaire A.27 *Si χ est un caractère de H, alors $\widetilde{\chi}$ est un caractère de G.*

Cela résulte de la proposition, en décomposant χ comme somme de caractères irréductibles. $\square$

Démontrons maintenant le th. A.22. Choisissons une représentation ρ de H de noyau trivial, par exemple la représentation régulière. Soit χ le caractère de ρ et soit $\widetilde{\rho}$ une représentation de G de caractère $\widetilde{\chi}$, cf. cor. A.27. Si s est conjugué à un élément de $H - \{1\}$, on a $\widetilde{\rho}(s) \neq 1$. D'autre part, si $s \in N$, on a $\widetilde{\chi}(s) = \chi(1) = \widetilde{\chi}(1)$, d'où $\widetilde{\rho}(s) = 1$, cf. démonstration de la prop. A.14. On a donc $N = \ker \widetilde{\rho}$, ce qui montre que N est un sous-groupe normal de G. $\square$

Bibliographie

[1] N. Bourbaki, *Algèbre. Chapitre I. Structures algébriques*, Nouvelle édition, Hermann, 1970.

[2] N. Bourbaki, *Algèbre. Chapitre VIII. Modules et anneaux semi-simples*, Hermann, 1958.

[3] J. Cassels et A. Fröhlich (édit.), *Algebraic Number Theory*, Acad. Press, 1967.

[4] W. Feit, *Characters of Finite Groups*, Benjamin, 1967.

[5] M. Hall, *The Theory of Groups*, Macmillan, 1959.

[6] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.

[7] N. Jacobson, *Basic Algebra I*, W.H. Freeman and Cy, 1974.

[8] S. Lang, *Algebra*, Addison-Wesley, 1965 ; Troisième édition, 1993.

[9] S. Lang, *Rapport sur la cohomologie des groupes*, Benjamin, 1966 ; trad. anglaise : LN 1625.

[10] J.-P. Serre, *Corps Locaux*, Hermann, 1968.

[11] J.-P. Serre, *Représentations linéaires des groupes finis*, Cinquième édition, Hermann, 1998.

[12] J. Wolf, *Spaces of Constant Curvature*, McGraw-Hill, 1967.

[13] H. Zassenhaus, *The Theory of Groups*, Deuxième édition, Vandenhoek and Ruprecht, 1956.

Mode d'emploi

- Groupes résolubles et nilpotents, p-groupes et théorèmes de Sylow : [1], [5], [6], [7], [8], [13].
- Applications à la théorie de Galois : [7].
- Extensions, systèmes de facteurs et cohomologie : [3], [6], [9], [10], [13].
- Théorèmes de Hall : [5], [6].
- Groupes de Frobenius : [4], [6] (pour la structure des groupes de type $\mathcal{F}$, voir [12]).
- Transfert : [6], [9], [10], [13] (voir aussi I. Schur, *Gesam. Abh.*, vol. 1, p.79).
- Représentations et caractères : [2], [4], [6], [8], [11] (voir aussi F.G. Frobenius, *Gesam. Abh.*, vol.3, et I. Schur, *Gesam. Abh.*, vol.1).

Index

action (de groupe –) : 1.1
Alperin (théorème d'–) : 2.14
Burnside (théorèmes de –) : 2.4, 5.1, A.6
caractère (d'une représentation) : A.1
caractéristique (sous-groupe –) : 1.2
Cauchy (théorème de –) : 2.2
centrale (fonction –) : A.3
centralisateur (d'un élément) : 1.1
centre (d'un groupe) : 1.2
Chebotarev-Frobenius (théorème de –) : 6.1
classe (de conjugaison) : 1.1
classe (de nilpotence d'un groupe) : 3.3
— (de résolubilité d'un groupe) : 3.1
cobord : 4.1
cochaîne : 4.1
cocycle : 4.1
cohomologie : 4.1
commutateur : 3.1
commutateurs (groupe des –) : 3.1
couple de Frobenius : 6.2
degré (d'une représentation linéaire) : A.1
dérivé (groupe –) : 3.1
descendante (suite centrale –) : 3.2
drapeau complet : 3.1
élémentaire (p-groupe abélien –) : 3.6
entier algébrique : A.5
extension : 4.2
Feit-Thompson (théorème de –) : 3.1
filtration : 1.3
fixateur : 1.1
Frattini (sous-groupe de –) : 3.6
— (théorème de –) : 2.3
Frobenius (théorème de –) : 6.2, A.7
fusion : 2.4
Gauss (lemme de –) : 7.3.1
gradué : 1.3
Hall (sous-groupe de –) : 5.1
— (théorème de –) : 5.1

homomorphisme croisé : 4.1
image réciproque (d'une extension) : 4.5
invariant (sous-groupe –) : 1.2
Jordan (théorème de –) : 6.1
Jordan-Hölder (suite de –, théorème de –) : 1.3
Kolchin (théorème de –) : 3.3
localement conjugués (éléments –) : 2.4
maximal (sous-groupe –) : 3.6
Miller-Wielandt (démonstration de –) : 2.2.2
minimal (groupe simple –) : 3.6
nilpotent (groupe –) : 3.3
normal (sous-groupe –) : 1.2
normalisateur (d'un sous-groupe) : 1.2
orbite : 1.1
orthogonalité (de caractères) : A.2
p-complément : 5.6
p-groupe : 2.1
p-Sylow : 2.1
permutable (système – de sous-groupes de Sylow) : 5.3
permutables (sous-groupes –) : 5.2
Π-sous-groupe : 5.1
Π-Sylow : 5.1
primitive (action –) : 3.6
propriété $\mathcal{F}$: 6.4
régulière (représentation –) : A.3
relèvement (d'un homomorphisme) : 4.5
représentation (linéaire) : A.1
résoluble (groupe –) : 3.1
sans point fixe (action –) : 6.4
Schur (lemme de –) : A.2
— (théorème de –) : 7.1
section : 4.2
semi-direct (produit –) : 4.2, 4.4
simple (groupe –) : 1.2
stabilisateur : 1.1
Stallings-Swan (théorèmes de –) : 7.3.2
suite centrale descendante : 3.2
Sylow (théorèmes de –) : 2.2, 2.3
Thompson (théorèmes de –) : 3.6, 6.3
transfert : 7.1
transitive (action –) : 1.1
triviale (extension –) : 4.2
Wedderburn (théorème de –) : 6.1
Wielandt (théorème de –) : 5.5
Zassenhaus (théorème de –) : 4.4