Cas particulier du théorème de Feit-Thompson

Rachid Bekhtaoui
Mémoire de M1 (T.E.R)
Université Pierre et Marie Curie Paris 6

7 Juillet 2006

Introduction

En 1963, les mathématiciens Walter Feit et John G. Thompson donnèrent une démonstration de plusieurs centaines de pages ([FT]) d'une conjecture énoncée par Burnside en 1911 à savoir :

Tout groupe d'ordre impair est résoluble.

Ce résultat est à la base de la classification des groupes finis qui interviendra vers le milieu des années 80. La longueur de la démonstration de Feit et Thompson est impressionnante [1], mais finalement en rapport avec les démonstrations qui suivront à propos de la classification des groupes finis, faisant pour certaines plusieurs milliers de pages.

Dans ce T.E.R, on se propose de vérifier ce théorème pour les groupes finis d'ordre inférieur à 2006 (et même un peu plus...). La démonstration se fera en plusieurs étapes, en fonction du nombre de facteurs primaires des groupes considérés. Le cas d'un groupe à un seul facteur primaire est classique (théorème 1.1.1) ; le cas de deux facteurs primaires (dû à Burnside) fera l'objet du chapitre 2 (théorème 2.2.1) et, enfin, dans le troisième chapitre on s'interessera au cas de groupes ayant au moins trois facteurs primaires (théorème 3.0.2).

Je remercie M.Bertrand, qui a dirigé la préparation de ce mémoire, et M.Nekovar, qui a bien voulu participer au jury.

[1] Thompson a remarqué qu'elle pouvait être grandement allégée si l'énoncé suivant était satisfait : «Soient p et q deux nombres premiers disctincts. Alors $PGCD(\frac{p^q-1}{p-1}, \frac{q^p-1}{q-1}) = 1$». Malheureusement, cette assertion est fausse, voir [St], qui donne le contre-exemple p=17, q=3313.

Chapitre 1

Préliminaires

Cette partie vise d'une part à rappeler plusieurs définitions et théorèmes de base en théorie des groupes (paragraphe 1.1) et d'autre part à démontrer un théorème de Burnside (proposition 1.2.3) qui jouera un rôle fondamental au chapitre 3.

Dans toute la suite, si E est un ensemble fini, $|E|$ désignera son cardinal et on notera 1 l'élément neutre des groupes considérés.

1.1 Rappels sur les groupes

1.1.1 Quelques rappels

Un sous-groupe propre d'un groupe est un groupe différent du groupe trivial et du groupe tout entier.

Si G est un groupe, et H un sous-groupe de G, on dit que H est distingué dans G et on note $H \triangleleft G$, si $\forall g \in G, gHg^{-1} = H$, ou, ce qui est équivalent, si $\forall g \in G, gHg^{-1} \subset H$.

On dit que G admet un quotient abélien s'il existe un sous-groupe distingué H tel que le groupe quotient G/H soit abélien non trivial.

On appelle groupe dérivé de G et on note DG le sous-groupe de G engendré par la partie $\{xyx^{-1}y^{-1}, x, y \in G\}$; c'est le plus petit sous-groupe distingué de G tel que G/DG soit abélien.. Par récurrence, on définit le n ième groupe dérivé D^nG de G par :

$$\begin{cases} D^0G = DG \\ D^{n+1}G = D(D^nG) \end{cases}$$

On dit qu'un groupe G est résoluble s'il existe un entier $n \geq 1$ tel que $D^n G$ soit le groupe trivial. Cette définition est équivalente à l'existence d'une suite finie de sous-groupes $(H_i)_{0 \leq i \leq p}$ de G telle que :

– $\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{p-1} \lhd H_p = G$

– pour tout i, le groupe quotient H_{i+1}/H_i est abélien.

Par exemple, les groupes abéliens sont résolubles.

Le lemme suivant sera primordial dans la suite, car c'est lui qui permettra d'utiliser les raisonnements par récurrence.

Lemme 1.1.1. *Une extension d'un groupe résoluble par un groupe résoluble est encore un groupe résoluble. En d'autres termes, si H est un sous-groupe distingué d'un groupe G, si H et G/H sont résolubles alors G est résoluble.*

Si H est un sous-groupe de G, nous noterons $N_G(H)$ (ou plus simplement $N(H)$ s'il n'y a pas de confusion possible) le normalisateur de H dans G, c'est-à-dire le groupe $\{g \in G, gHg^{-1} = H\}$.

Le centralisateur de H dans G, qui est le groupe $\{g \in G, \forall h \in H gh = hg\}$ sera noté $C_G(H)$ ou plus simplement $C(H)$. Le centralisateur de G dans lui-même est son centre, généralement noté $Z(G)$.

Enfin, on note $Aut(G)$ le groupe des automorphismes de G.

1.1.2 Les p-groupes

Si G est un groupe fini, rappelons qu'on a la formule suivante, dite formule des classes :

$$|G| = |Z(G)| + \sum_{\omega, |\omega| \geq 2} |\omega|$$

où la somme du deuxième membre est prise sur l'ensemble des classes de conjugaison de G contenant au moins deux éléments.

Si p est un nombre premier, on appelle p-groupe tout groupe fini dont l'ordre est une puissance de p.

Lemme 1.1.2. *Tout p-groupe non trivial admet un centre non trivial.*

Démonstration. Conséquence de la formule des classes. □

On note $\mathbb{F}_p$ le corps à p éléments. Nous rappelons sans démonstration la proposition suivante (dont la preuve se trouve dans tous les cours de théorie des groupes) :

Lemme 1.1.3. *Si G est un groupe d'ordre p, où p est un nombre premier, alors G est cyclique (donc abélien) et $Aut(G) \simeq \mathbb{F}_p^*$ est cyclique d'ordre $p-1$.*

Si G est un groupe d'ordre p^2 alors G est abélien et isomorphe :

- *soit à* $\mathbb{Z}/p^2\mathbb{Z}$ *auquel cas* $|Aut(G)| = p^2 - p$
- *soit à* $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ *auquel cas* $Aut(G)$ *est isomorphe à* $GL_2(\mathbb{F}_p)$*, qui est d'ordre* $(p^2-1)(p^2-p)$.

Enfin, terminons cette section sur les p-groupes par le classique :

Théorème 1.1.1. *Si p est un nombre premier, alors tout groupe d'ordre une puissance de p est résoluble.*

Il s'agit d'un résultat élémentaire mais nous en donnons une démonstration car c'est une première étape dans la démonstration du cas particulier du théorème de Feit-Thompson qui nous occupe ici.

Démonstration. Soit p^n l'ordre de G. La démonstration se fait par récurrence sur l'entier n :

- si $n = 0$ alors un groupe d'ordre $p^0 = 1$ est le groupe trivial donc il est résoluble.
- Soit $n \in \mathbb{N}$ fixé quelconque. On suppose que tout groupe d'ordre p^n est résoluble et on considère alors G un groupe d'ordre p^{n+1}. Puisque G est un p-groupe, son centre $Z(G)$ (qui est distingué dans G) est non trivial (lemme 1.1.2), donc d'ordre p^m avec $1 \leq m \leq n+1$. On en déduit que le groupe quotient $G/Z(G)$ qui est d'ordre $p^{(n+1)-m}$ est résoluble via l'hypothèse de récurrence. Le groupe $Z(G)$ étant lui aussi résoluble (car abélien) on en déduit grâce au le lemme 1.1.1 que G est résoluble, ce qui prouve la propriété au rang $n+1$, et achève ainsi la démonstration.

□

1.1.3 Théorèmes de Sylow

Soient p un nombre premier et G un groupe fini d'ordre $|G| = p^n.m$ où p ne divise pas m. On appelle p-sous-groupe de Sylow de G tout sous-groupe de G d'ordre p^n. Rappelons les importants théorèmes de Sylow en théorie des groupes :

Lemme 1.1.4. *1. il existe des p-sous-groupes de Sylow de G*

2. les p-sous-groupes de Sylow de G sont conjugués entre eux, c'est-à-dire que si H et K sont deux p-sous-groupes de Sylow de G alors il existe $g \in G$ tel que $gHg^{-1} = K$

Démonstration. Voir un cours de théorie des groupes. □

Grâce aux théorèmes de Sylow, on peut montrer le :

Lemme 1.1.5. *Soit H un p-sous-groupe de Sylow de G. Si x et y sont deux éléments $C(H)$ qui sont conjugués dans G, alors il sont conjugués dans $N(H)$.*

Démonstration. Soit $u \in G$ tel que $y = uxu^{-1}$. Puisque x et y sont dans $C(H)$, H et uHu^{-1} sont inclus dans $C(\{y\})$ (le sous-groupe de G des éléments qui commutent avec y) et en sont ainsi des p-sous-groupes de Sylow. Le lemme 1.1.4 dit qu'il existe alors $z \in C(\{y\})$ tel que $H = z(uHu^{-1})z^{-1}$. Donc l'élément $zu \in N(H)$ et vérifie en plus $(zu)x(zu)^{-1} = zyz^{-1} = y$ puisque z commute avec y. □

1.2 L'homomorphisme de transfert

Dans cette section, nous allons definir le morphisme de transfert d'un groupe G vers un sous-groupe H de G. Dans l'application que nous avons en vue, H est commutatif, et nous limiterons notre description a ce cas.

Soit G un groupe fini, et H un sous-groupe commutatif de G. Fixons y un élément de G. Si $(x_i)_{1\leq i\leq n}$ est un système de représentants de l'ensemble des classes à gauche de G suivant H alors pour tout $i \in \{1, \ldots, n\}$ il existe un unique $j \in \{1, \ldots, n\}$ et $h_i \in H$ tels que :

$$yx_i = x_j h_i$$

En effet, $yx_i \in G = \bigcup_{j=1}^{n} x_j H$ (où la réunion est disjointe). De plus, l'application σ qui à i associe l'entier j définie comme précédemment est bijective car si $\sigma(i) = \sigma(i')$ alors :

$$x_i^{-1}x_{i'} = (yx_i)^{-1}(yx_{i'}) = (x_{\sigma(i)}h_i)^{-1}(x_{\sigma i'}h_{i'}) = h_i^{-1}h_{i'} \in H$$

donc $x_iH = x_{i'}H$ et donc $i = i'$. Nous avons donc attaché à y une permutation σ de $\mathfrak{S}_n$ et des éléments h_i de H qui dépendent du système de réprésentants choisi bien évidemment. Nous allons voir que le produit $\prod_{i=1}^{n} h_i$ ne dépend pas de celui-ci.

Si $(z_i)_{1\leq i\leq n}$ est un autre système de réprésentants, on peut, comme ci-dessus, trouver τ dans $\mathfrak{S}_n$ et des éléments a_i de H tels que pour tout $j \in \{1, \ldots, n\}$ on ait :

$$yz_i = z_{\tau(i)}a_i$$

Or, de la même manière que précédemment, il existe une permutation κ de $\mathfrak{S}_n$ et des éléments c_i de H tels que pour tout i, $z_i = x_{\kappa(i)}c_i$ (et en particulier, $x_i = z_{\kappa^{-1}(i)}(c_{\kappa^{-1}(i)})^{-1}$) de sorte que :

$$yz_i = yx_{\kappa(i)}c_i = x_{\sigma\circ\kappa(i)}h_{\kappa(i)}c_i = z_{\kappa^{-1}\circ\sigma\circ\kappa(i)}(c_{\kappa^{-1}\circ\sigma\circ\kappa(i)})^{-1}h_{\kappa(i)}c_i$$

Puisque les a_i sont uniques tels que $yz_i = z_{\tau(i)}a_i$ et que les elements $c_{\kappa^{-1}\circ\sigma\circ\kappa(i)})^{-1}h_{\kappa(i)}c_i$ appartiennent à H, on en deduit donc l'égalité :

$$a_i = (c_{\kappa^{-1}\circ\sigma\circ\kappa(i)})^{-1}h_{\kappa(i)}c_i$$

(ainsi que $\tau = \kappa^{-1} \circ \sigma \circ \kappa$). Par suite,

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} (c_{\kappa^{-1} \circ \sigma \circ \kappa(i)})^{-1} h_{\kappa(i)} c_i$$

et puisque H est commutatif et qu'on est en présence d'un produit d'éléments de H, on a :

$$\begin{aligned} \prod_{i=1}^{n} a_i &= \prod_{i=1}^{n} (c_{\kappa^{-1} \circ \sigma \circ \kappa(i)})^{-1} \prod_{i=1}^{n} h_{\kappa(i)} \prod_{i=1}^{n} c_i \\ &= \prod_{i=1}^{n} (c_i)^{-1} \prod_{i=1}^{n} h_i \prod_{i=1}^{n} c_i \\ &= \prod_{i=1}^{n} h_i \end{aligned}$$

ce qui montre bien que le produit en question est bien indépendant du système de représentants choisis. Nous pouvons donner la définition du morphisme de transfert :

Proposition-Définition 1.2.1. *Soit G un groupe fini et H un sous-groupe abélien de G. Le transfert de G vers H est le morphisme de G vers H noté $V_{G \to H}$ ou plus simplement V tel que pour tout $y \in G, V(y) = \prod_{i=1}^{n} h_i$ (où les h_i sont définis comme précédemment).*

Démonstration. Montrons qu'il s'agit bien d'un morphisme de groupe. Soient u et v dans G, et respectivement, σ et τ les permutations, ainsi que h_i et g_i dans H les éléments associés à un système de représentants $(x_i)_{1 \leq i \leq n}$ tels que

$$ux_i = x_{\sigma(i)} h_i$$

et

$$vx_i = x_{\tau(i)} g_i$$

Alors, $uvx_i = ux_{\tau(i)} g_i = x_{\sigma \circ \tau(i)} h_{\sigma(i)} g_i$ et donc :

$$V(uv) = \prod_{i=1}^{n} h_{\sigma(i)} g_i$$

Puisque H est commutatif on a donc :

$$\begin{aligned} V(uv) &= \prod_{i=1}^{n} h_{\sigma(i)} \prod_{i=1}^{n} g_i \\ &= \prod_{i=1}^{n} h_i \prod_{i=1}^{n} g_i \\ &= V(u)V(v) \end{aligned}$$

ce qui achève la démonstration. □

Sous sa forme actuelle, le morphisme de transfert n'est pas très pratique à manipuler. Le lemme suivante permet de donner une meilleure déscription de celui-ci.

Lemme 1.2.1. *Soit G un groupe fini, H un sous-groupe commutatif de G d'indice $[G : H] = n$ et $(x_i)_{1\leq i\leq n}$ un système de représentants des classes à gauche modulo H. Pour tout $y \in G$, il existe une sous-suite d'éléments $(x_{i_j})_{1\leq j\leq r}$ du système de représentants et pour $j = 1, \ldots, r$ un entier n_j, tels que :*

$$V(y) = \prod_{j=1}^{r} x_{i_j}^{-1} y^{n_j} x_{i_j}$$

avec pour tout $j = 1, \ldots, r$, $x_{i_j}^{-1} y^{n_j} x_{i_j} \in H$ et $\sum_{j=1}^{r} n_j = [G : H]$.

Démonstration. Soit $\sigma \in \mathfrak{S}_n$ et $h_i \in H$ associés à y comme vu plus haut (c'est-à-dire tels que $yx_i = x_{\sigma(i)}h_i$ pour tout $i \in \{1, \ldots, n\}$). On sait que σ peut se décomposer en un produit de r cycles à supports disjoints $\tau_1, \ldots, \tau_n$, chaque cycle τ_j étant de longueur n_j avec $\sum_{j=1}^{r} n_j = n$. Si $\tau_j = (k_1, \ldots, k_{n_j})$ alors des égalités :

$$yx_{k_1} = x_{k_2}h_{k_1}, \ldots, yx_{k_{n_j-1}} = x_{k_{n_j}}h_{k_{n_j-1}}, yx_{k_{n_j}} = x_{k_1}h_{k_{n_j}}$$

on déduit que :

$$(x_{k_1})^{-1} y^{n_j} x_{k_1} = h_{k_{n_j}} \ldots h_{k_1} \in H$$

De sorte que pour tout $j \in \{1, \ldots, r\}$,

$$\prod_{k=1}^{n_j} h_{\tau_j(k)} = (x_{k_1})^{-1} y^{n_j} x_{k_1}$$

Finalement, on obtient le résultat voulu en remarquant que :

$$V(y) = \prod_{i=1}^{n} h_i = \prod_{j=1}^{r} \prod_{k=1}^{n_j} h_{\tau_j(k)} = \prod_{j=1}^{r} (x_{k_1})^{-1} y^{n_j} x_{k_1}$$

(Remarquer que le k_1 dépend de j à chaque fois...les notations devenant trop lourdes, il a fallu faire le choix de ne pas trop rajouter d'indices). □

Nous sommes en mesure désormais de prouver le résultat essentiel suivant, qui sera à la base du chapitre 3 :

Proposition 1.2.2. *Soit G un groupe fini et H un p-sous-groupe de Sylow de G tel que $N(H) = C(H)$. Alors il existe un sous-groupe P distingué de G tel que $G/P \simeq H$.*

Démonstration. Puisque $H \subset C(H) = N(H)$, le groupe H est abélien et on peut donc utiliser les formules supra pour décrire le transfert V de G vers H. Nous allons montrer que V est surjectif (on conclut alors en posant $P = KerV$). Soit y un élément de H. D'après le lemme 1.2.1 et en gardant les mêmes notations, on peut écrire : $V(y) = \prod_{j=1}^{r} x_{i_j}^{-1} y^{n_j} x_{i_j}$ avec $x_{i_j}^{-1} y^{n_j} x_{i_j} \in H$. Ainsi les éléments y^{n_j} et $x_{i_j}^{-1} y^{n_j} x_{i_j}$ sont deux éléments de H, donc de $C(H)$, conjugués dans G, ils sont donc conjugués dans $N(H)$ d'après le lemme 1.1.5, c'est-à-dire qu'il existe z_j dans $N(H)$ tel que $z_j^{-1} y^{n_j} z_j = x_{i_j}^{-1} y^{n_j} x_{i_j}$. Et puisque $N(H) = C(H)$ on a donc : $y^{n_j} = x_{i_j}^{-1} y^{n_j} x_{i_j}$. Par suite,

$$V(y) = \prod_{i=1}^{r} y^{n_j} = y^{\sum_{i=1}^{r} n_j} = y^{[G:H]}$$

Or, $[G : H]$ est premier avec l'ordre p^t de H, car H est un p-sous-groupe de Sylow. Donc, il existe des entiers u et v tels que $u[G : H] + vp^t = 1$. Comme $y \in H$, $y^{p^t} = 1$ et donc :

$$y = y^{u[G:H]} y^{vp^t} = y^{u[G:H]} = V(y^u)$$

ce qui revient bien à dire que $H \subset ImV$, d'où l'égalité entre ces ensembles et V est bien surjectif. □

Chapitre 2

Théorème de Burnside pour les groupes d'ordre $p^a q^b$

Le fait que les groupes d'ordre $p^a q^b$ soient résolubles est un classique théorème de Burnside. Nous en donnons ici une démonstration utilisant la théorie des caractères en suivant la démarche proposée dans [Se], section 6.5, exercices 3,4 et 5.

2.1 Rappels sur les caractères

Soit G un groupe fini. On appelle *représentation de* G la donnée d'un $\mathbb{C}$-espace vectoriel V de dimension finie et d'un homomorphisme de groupes ρ de G dans $GL(V)$. Un sous-espace vectoriel W de V sera dit stable par ρ si pour tout $g \in G, \rho(g)(W) \subset W$. La représentation ρ sera dite irréductible si aucun sous-espace vectoriel propre de V n'est stable par ρ. On appelle représentation triviale, le morphisme de G dans $GL(\mathbb{C})$ (où $\mathbb{C}$ est vu en tant qu'espace vectoriel sur lui-même) qui à $g \in G$ associe l'application identité de $\mathbb{C}$: c'est clairement une représentation irréductible.

Une application χ de G dans $\mathbb{C}$ est appelée caractère de G s'il existe une représentation ρ de G telle que pour tout $g \in G, \chi(g) = Trace(\rho(g))$. Dans ce cas, ρ est alors entièrement determinée (à isomorphisme près) par χ, et s'appelle la représentation associée àχ. De plus, le caractère χ sera dit irréductible si la représentation ρ est elle-même irréductible. On appelle caractère trivial le caractère associé à la représentation triviale : c'est un caractère irréductible.

Soit χ un caractère de G. Si 1 est l'élément neutre de G, l'élément $\chi(1)$ est un nombre entier, égal àla dimension de la représentation correspondante, et est appelé degré du caractère χ. Si C est une classe de conjugaison de G alors tous les éléments de C ont la même image par χ : on notera alors $\chi(C)$ cette valeur commune.

On notera $\hat{G}$ l'ensemble des caractères irréductibles de G : on sait que

c'est un ensemble fini, de cardinal égal au nombre de classes de conjugaison de G. Rappelons enfin la relation d'orthogonalité : si C est une classe de conjugaison de G différente de $\{1\}$ alors

$$\sum_{\chi \in \hat{G}} \chi(1)\chi(C) = 0$$

Nous donnons sans démonstration les deux premiers lemmes suivants, dont la preuve est dans [Se], section 6.5, proposition 15 et corollaire 1.

Lemme 2.1.1. *Soit $\rho : G \to GL_n(\mathbb{C})$ une représentation, de caractère χ. Pour tout $g \in G$, $\rho(g)$ est conjugué àune matrice diagonale formée de racines de l'unité. En particulier, $\chi(g)$ est une somme finie de racines de l'unité de $\mathbb{C}$.*

Lemme 2.1.2. *Si C est une classe de conjugaison de G et χ est un caractère irréductible sur G alors pour tout $g \in C, |C|\frac{\chi(g)}{\chi(1)}$ est un entier algébrique.*

Nous aurons besoin par la suite des deux lemmes suivants :

Lemme 2.1.3. *Soit G est un groupe fini et p un nombre premier divisant $|G|$. Si C une classe de conjugaison d'ordre une puissance > 0 de p alors il existe un caractère irréductible qui ne soit pas le caractère trivial tel que : $PGCD(\chi(1), |C|) = 1$ et $\chi(C) \neq 0$.*

Démonstration. Par la relation d'orthogonalité, on a :

$$\sum_{\chi \in \hat{G}, PGCD(\chi(1),|C|)=1, \chi(C)\neq 0} \chi(1)\chi(C) = - \sum_{\chi \in \hat{G}, p|\chi(1)} \chi(1)\chi(C)$$

Si jamais l'ensemble des $\{\chi \in \hat{G}, PGCD(\chi(1), |C|) = 1, \chi(C) \neq 0\}$ était réduit au seul caractère trivial, alors on aurait l'égalité :

$$1 = - \sum_{\chi \in \hat{G}, p|\chi(1)} \chi(1)\chi(C)$$

et donc, par le lemme 2.1, il existerait donc un entier algébrique ω tel que :

$$1 = p.\omega$$

Ainsi, $1/p$ serait un entier algébrique, ce qui est absurde. D'où le résultat. □

Lemme 2.1.4. *Soit n un entier, et $x_1, \ldots, x_n$ des racines de l'unité de $\mathbb{C}$. Si $\lambda = \frac{1}{n}\sum_{i=1}^{n} x_i$ est un entier algébrique non nul alors les x_i sont égaux deux à deux.*

Démonstration. Nous allons d'abord démontrer que si $\zeta_1, \ldots, \zeta_N$ sont N racines de l'unité de $\mathbb{C}$ telles que $\sum_{i=1}^{N} \zeta_i = N$ alors $\forall i, \zeta_i = 1$.

En effet, l'égalité précédente est équivalente à $\sum_{i=1}^{N}(\zeta_i - 1) = 0$ ce qui signifie que 1 est le barycentre du système $((\zeta_i, 1))_{1 \leq i \leq N}$: le barycentre est situé sur le cercle unité donc nécéssairement les ζ_i sont tous confondus donc égaux à leur barycentre, à savoir 1.

Maintenant, considérons un entier n, et des racines de l'unité de $\mathbb{C}$ $x_1, \ldots, x_n$ tels que $\lambda = \frac{1}{n}\sum_{i=1}^{n} x_i$ soit un entier algébrique non nul. Quitte à diviser tous les x_i par x_1 on peut toujour supposer $x_1 = 1$. Soit K le corps de nombres $\mathbb{Q}(x_1, \ldots, x_n)$ et $\sigma_1 = Id, \ldots, \sigma_d$ les $d = [K : \mathbb{Q}]$ plongements de K dans $\mathbb{C}$. Il est clair que λ ainsi que ses conjugués sont de norme inférieure à 1. Mais puisque la norme $N_{K/\mathbb{Q}}(\lambda) = \prod_{i=1}^{d} \sigma_i(\lambda)$ appartient à $\mathbb{Z}$ (car λ est un entier algébrique) alors $N_{K/\mathbb{Q}}(\lambda)$ vaut soit 1, 0 ou -1. λ étant non nul, on exclut le cas 0, donc :

$$\prod_{i=1}^{d} \sigma_i(\lambda) = \pm 1$$

c'est-à-dire :

$$\prod_{i=1}^{d} (\sigma_i(x_1) + \cdots + \sigma_i(x_n)) = \pm n^d$$

Par suite,

$$\sum_{i_1, \ldots, i_d \in \{1, \ldots, n\}} \sigma_1(x_{i_1}) \ldots \sigma_d(x_{i_d}) = \pm n^d$$

Par la remarque qui a débuté la démonstration, on a alors :

$$\forall i_1, \ldots, i_d, \sigma_1(x_{i_1}) \ldots \sigma_1(x_{i_d}) = \pm 1$$

En particulier, si on choisit $i_1 = \cdots = i_d = 1$ cela exclut la possibilité d'un signe moins dans l'égalité ci-dessus. Finalement, pour tout $j \in \{1, \ldots, n\}$, en choisissant $i_1 = j$ et $i_2 = \cdots = i_d = 1$, on trouve que $x_j = 1$ qui est bien égal à x_1. □

2.2 Résolubilité des groupes d'ordre $p^a q^b$

Théorème 2.2.1. *Soient p et q deux nombres premiers distincts, et G un groupe d'ordre $p^a q^b$ avec $a \in \mathbb{N}, b \in \mathbb{N}$. Alors G est résoluble.*

Démonstration. La démonstration se fait par récurrence sur l'ordre du groupe G tel que l'ordre admet au plus deux facteurs premiers.

- Les groupes d'ordre $n = 1 = p^0 q^0$ sont résolubles.
- Soit $n \geq 2$ fixé quelconque. On suppose que tout groupe d'ordre de la forme $p^u q^v$ avec $p^u q^v \leq n$ est résoluble et on considère alors G un groupe d'ordre $n + 1 = p^a q^b$. Distinguons trois cas de figure :

1. Si l'ordre de G a juste un facteur premier, G est résoluble en vertu du théorème 1.1.1.
2. Si l'ordre de G admet deux facteurs premiers et que G admet un sous-groupe distingué propre H, alors H et G/H sont donc des groupes d'ordre $< n+1$ dont les ordres admettent au plus deux facteurs premiers. Par récurrence, ils sont résolubles. D'après le lemme 1.1.1, G est résoluble.
3. Si l'ordre de G a deux facteurs premiers et que G n'admet pas de sous-groupe distingué propre, alors le centre de G vaut soit G soit 1. Si $Z(G) = G$ alors G est abélien donc résoluble. Si $Z(G) = \{1\}$ alors il existe une classe de conjugaison d'ordre p^r $(r > 0)$. En effet, si ce n'était pas le cas, alors toutes les classes de conjugaison autres que $\{1\}$ (qui est la seule classe de conjugaison à un élément puisque le centre de G est le groupe trivial) seraient de cardinal divisible par q et étant donné la formule des classes :

$$|G| = p^a q^b = 1 + \sum_{|C_i|>1} |C_i|$$

on aurait donc que $1 \equiv 0 \mod (q)$, ce qui est absurde. Soit alors C une telle classe de conjugaison, et $y \neq 1$ un de ses éléments (un tel y existe car C a p^r éléments $(r > 0)$. Par le lemme 2.1.3, on peut considérer un caractère irréductible non trivial de G, qu'on note χ tel que $PGCD(\chi(1), |C|) = 1$ et $\chi(y) \neq 0$. Si on note ρ la réprésentation linéaire associée à χ, nous allons voir que $\rho(y)$ est une homothétie : en effet, si k et l sont deux entiers tels que $k\chi(1) + l|C| = 1$ alors en multipliant par $\chi(y)$ on obtient

$$l \underbrace{\chi(y)}_{ent.alg.} + k \underbrace{|C| \frac{\chi(y)}{\chi(1)}}_{ent.alg.} = \frac{\chi(y)}{\chi(1)}$$

Puisque l'ensemble des entiers algébriques forme un anneau, $\frac{\chi(y)}{\chi(1)}$ est donc un entier algébrique. Or, d'après le lemme 2.1.1, $\chi(y)$ s'écrit comme une somme de $n := \chi(1)$ racines de l'unités ω_1, ..., ω_n et puisque $\chi(y) \neq 0$, le lemme 2.1.4 montre que $\omega_1 = \cdots = \omega_n$. Or, les ω_i sont les valeurs propres de $\rho(y)$ et puisque $\rho(y)$ est diagonalisable (car y étant d'ordre fini dans G, il existe un entier q tel que $\rho(y)^q = Id_n$) alors $\rho(y) = \omega_1 Id_n$.
$Ker\rho$ étant un sous-groupe distingué, alors puisque G n'a pas de sous-groupe distingué propre, il est égal soit à G, soit à $\{1\}$. Mais puisque χ n'est pas le caractère trivial, $Ker\rho$ ne peut être G. Donc $Ker\rho = \{1\}$ et ρ est injective. L'endomorphisme $\rho(y)$ étant une homothétie, il commute avec tous les $\rho(g), g \in G$. Comme ρ

est injective cela entraîne que y commute avec tous les $g \in G$, c'est-à-dire $y \in Z(G)$. Or, nous avions choisi $y \neq 1$ plus haut, ce qui contredit notre hypothèse que $Z(G) = \{1\}$ et donc ce cas est impossible.

□

Chapitre 3

Théorème de Feit-Thompson pour les groupes d'ordre inférieur à 2006

Dans ce chapitre, nous allons enfin démontrer le résultat annoncé au début, à savoir que tout groupe d'ordre impair inférieur ou égal à 2006 est résoluble. Pour cela, nous aurons besoin des deux lemmes suivants :

Lemme 3.0.1. *Soient G un groupe fini n'admettant pas de quotient abélien propre, p un nombre premier divisant $|G|$ et H un p-sous-groupe de Sylow de G.*

1. *Si $|H| = p$, alors il existe un nombre premier l divisant $p-1$ et $|G|$*
2. *Si $p = 3$ et $|H| = 3^2$ alors $|G|$ est pair.*

Démonstration. Tout d'abord, notons que le groupe $N(H)/C(H)$ s'injecte dans $Aut(H)$. En effet, le morphisme f de $N(H)$ dans $Aut(H)$ qui àun élément h associe l'isomorphisme $g \mapsto ghg^{-1}$ a pour noyau exactement $C(H)$ (qui est donc un sous-groupe distingué de $N(H)$) donc il se factorise en une injection de $N(H)/C(H)$ dans $Aut(H)$. En particulier, $[N(H) : C(H)]$ divise $|Aut(H)|$.

1. On suppose ici que $|H| = p$: si on avait $N(H) = C(H)$ alors d'après la proposition 1.2.2 il existerait un sous-groupe distingué P de G tel que $G/P \simeq H$. Or, H est abélien (car cyclique, cf. lemme 1.1.3), donc G admettrait un quotient abélien propre, ce qui n'est pas. On a alors l'inclusion stricte $C(H) \subsetneq N(H)$ et donc $[N(H) : C(H)] > 1$. Si l en est un diviseur premier, par la remarque ci-dessus, l divise $|Aut(H)| = p-1$ (lemme 1.1.3). Enfin, puisque $[N(H) : C(H)]$ divise l'ordre de G, l divise donc aussi $|G|$.
2. Si $|H| = 3^2$ alors pour les mêmes raisons que ci-dessus, $N(H)$ ne peut être égal à $C(H)$. En effet, si c'était le cas, d'après la proposition 1.2.2

il existerait un sous-groupe distingué P de G tel que $G/P \simeq H$. Mais H est abélien en vertu du lemme 1.1.3, donc G admettrait un quotient abélien propre. Donc $[N(H) : C(H)] > 1$ admet des diviseurs premiers. Si l est l'un d'entre eux, alors il divise $|Aut(H)|$. Toujours d'après le lemme 1.1.3, cet ordre vaut soit $3^2 - 3 = 6$, soit $(3^2 - 3)(3^2 - 1) = 6.8$ d'où, $l = 2$ ou $l = 3$. Si jamais on avait $l = 3$, alors puisque H est abélien, il est contenu dans $C(H)$ et donc on a la formule suivante : $[N(H) : H] = [N(H) : C(H)][C(H) : H]$. Puisque $l = 3$ divise $[N(H) : C(H)]$ alors $[N(H) : H]$ est divisible par 3, ce qui est impossible car H est un 3-groupe de Sylow et donc $[N(H) : H]$ est premier avec 3. Par suite, $l = 2$, et divise $[N(H) : C(H)]$ donc $|G|$, ce qui termine la démonstration.

□

Lemme 3.0.2. *Soit G un groupe fini d'ordre n impair, ayant au moins 3 facteurs premiers. Soit $n = p_1^{r_1}...p_s^{r_s}$ la décomposition de $|G|$ en produit de facteurs premiers, avec $1 < p_1^{r_1} < \cdots < p_s^{r_s}$. On suppose que G n'a pas de quotient abélien propre. Alors :*

1. *Pour tout $j = 1, \ldots, s$, $p_j^{r_j} \neq 3, 5$ ou 3^2.*
2. *Si $p_1^{r_1} = 7$ alors n est divisible par 3^3 et il existe un facteur premier $p_i \neq 3, 7$ tel que $p_i^{r_i} \geq 11$. En particulier, $|G| \geq 7.3^3.11 = 2079$.*
3. *Si $p_1^{r_1} = 11$ alors n est divisible par 5^2 et il existe un facteur premier $p_i \neq 5, 11$ tel que $p_i^{r_i} \geq 13$. En particulier, $|G| \geq 11.5^2.13 = 3575$.*

Démonstration. 1. D'après le lemme 3.0.1, aucun $p_j^{r_j}$ ne peut valoir 3^2 car sinon $|G|$ serait pair. D'autre part, s'il existe j tel que $p_j^{r_j} = 3$ (resp. 5) alors le lemme précédent donnerait l'existence d'un nombre premier l divisant $|G|$ et $3 - 1 = 2$ (resp. 5-1=4). Donc l serait 2 et $|G|$ serait pair, ce qui n'est pas.

2. Si $p_1^{r_1} = 7$ alors toujours par le lemme 3.0.1, il existe un nombre premier l divisant 7-1=6 et $|G|$. Mais puisque $|G|$ est impair, nécéssairement $l = 3$ divise l'ordre de G, donc il existe un j tel que $p_j^{r_j}$ soit une puissance de 3. Mais la première assertion prouvée auparavant interdit que ce soit 3, ni 3^2, donc $p_j^{r_j} \geq 3^3$ et donc 3^3 divise $|G|$. Or, l'ordre de G possède au moins 3 facteurs primaires, donc si $p_k \neq 3, 7$ est un troisième facteur premier de $|G|$, puisqu' on a les inégalités $7<9<11$ (rappelons que $p_1^{r_1} = 7$ est le plus petit facteur primaire) alors on a la minoration suivante $p_k^{r_k} \geq 11$. Et finalement, $|G| \geq 7.3^3.11 = 2079$.

3. Si $p_1^{r_1} = 11$ de la même manière il existe un nombre premier l divisant 11-1=10 et $|G|$. Mais puisque $|G|$ est impair, nécéssairement $l = 5$ divise l'ordre de G, donc il existe un j tel que $p_j^{r_j}$ soit une puissance de 5. Toujours à cause de la première assertion, ce ne peut être 5 lui-même, donc $p_j^{r_j} \geq 5^2$, et 5^2 divise l'ordre de G. Or, l'ordre de G possède au

moins 3 facteurs primaires, donc si $p_k \neq 5, 11$ est un troisième facteur premier de $|G|$, puisqu'on a l' inégalité $11 < 13$, on en déduit que $p_k^{r_k} \geq 13$. Et $|G| \geq 11.5^2.13 = 3575$.

□

Concluons en donnant la démonstration du théorème de Feit-Thompson dans le cas particulier des groupes d'ordre plus petit que 2006 :

Théorème 3.0.2. *Tout groupe d'ordre impair $\leq$ 2006 est résoluble.*

Démonstration. La démonstration se fait par récurrence sur l'ordre des groupes.

1. Si $n = 1$, la propriété est vraie.
2. Soit $1 \leq n \leq 2005$ fixé quelconque. On suppose que tout groupe d'ordre impair inférieur ou égal à n est résoluble. Soit alors G un groupe d'ordre impair inférieur à $n + 1$. Distinguons là aussi deux cas :
   - Si G admet un sous-groupe distingué propre H, alors H et G/H sont d'ordre impair strictement plus petit que $n + 1$ donc l'hypothèse de récurrence associée au lemme 1.1.1 montre que G est résoluble.
   - Si G n'a pas de sous-groupe distingué propre alors en particulier il n'admet pas de quotient abélien. Si $|G|$ a au plus deux facteurs alors on conclut à la résolubilité de G avec les théorèmes 1.1.1 et 2.2.1. S'il en a au moins 3, comme $13^3 > 2006 \geq |G|$ alors le plus petit facteur primaire de G vaut 3,5,7,9 ou 11. Il ne peut valoir 3,5 ou 9 en vertu de la première assertion du lemme 3.0.2. De plus, il ne peut valoir 7 (resp. 11) car sinon, encore d'après le lemme 3.0.2 l'ordre de G serait supérieur à 2079 (resp. 3575). Donc ce cas est impossible, et cela termine la demonstration.

□

Bibliographie

[FT] W. FEIT , J.G. THOMPSON : *Solvability of groups of odd order* ; Pacific J. Math. 13, 1963, 775-1029

[Sc] W.R. SCOTT : *Group theory* ; Dover , 1987, ISBN : 0-486-65377-3

[Se] J-P. SERRE : *Représentations linéaires des groupes finis* ; Hermann, 1978, ISBN :2-7056-5630-8

[St] N.M. STEPHENS : *On the Feit-Thompson Conjecture* ; Math. Comput. 25, 1971, 625.
