Lucas Toury - ENS Rennes

# Un théorème de Burnside

## 1 Introduction

J'ai voulu rédiger ce développement pour plusieurs raisons. Premièrement je n'ai trouvé aucune référence convaincante, soit elles utilisent des résultats trop sophistiqués (en tout cas je trouve au niveau de l'agreg), faisant appel à l'algèbre d'un groupe, soit le théorème est montré de manière trop longue, trop détournée, en multipliant les résultats intermédiaires qui ne font qu'engendrer un flou quant à ce qui se passe vraiment. Deuxièmement, je pense que c'est un très beau développement, transversal dans les mathématiques, qui n'est pas facile mais possède un très bon recasage et fait un très bel effet lorsqu'il est maitrisé, donnant lieu à beaucoup de questions que l'on peut prévoir. Cela permet de contrôler une partie des questions du jury ce qui n'est pas négligeable.

## 2 Prérequis

On commence tout d'abord avec une première proposition qui ne fait pas partie du développement, car il serait trop long mais dont le résultat est essentiel pour la suite.

**Propriété 2.1.** Soit $G$ un groupe fini, $C$ une classe de conjugaison de $G$ et $\chi$ un caractère irréductible de $G$. Alors $\frac{|C|\chi(C)}{\chi(1)}$ est un entier algébrique.

Ce résultat est montré dans NH2G2 dans la partie sur les représentations et caractères dans l'exercice où l'on montre que le degré d'une représentation irréductible divise le cardinal du groupe.

## 3 Le développement

Début du développement : On prend les mêmes notations que la proposition précédente.

**Propriété 3.1.** Si $\text{pgcd}(|C|, \chi(1)) = 1$. Alors $\frac{\chi(g)}{\chi(1)}$ est un entier algébrique. De plus, pour tout $g \in C$, si $\chi(g) \neq 0$ alors $\rho(g)$ est une homothétie. ($\rho$ étant la représentation associée au caractère $\chi$).

*Démonstration.* On écrit une identité de Bézout, il existe $(a, b) \in \mathbb{Z}^2$ tels que :

$$a|C| + b\chi(1) = 1$$

En multipliant l'égalité par $\frac{\chi(g)}{\chi(1)}$ et en utilisant le lemme précédent, on voit que le membre de gauche est un entier algébrique donc le membre de droite aussi. Ceci conclut le premier résultat.

Soit $g \in C$, on note $n := \chi(1)$ le degré de la représentation. On sait que $\chi(g) = \sum_{i=1}^{n} \lambda_i$ avec $\lambda_i$ des racines de l'unité. En passant en module on voit directement que $|\frac{\chi(g)}{\chi(1)}| \leq 1$. Soit $P$ le polynôme minimal de $\frac{\chi(g)}{\chi(1)}$ dans $\mathbb{Q}[X]$ et $z$ une racine de $P$. On sait qu'il existe un automorphisme de corps stabilisant $\mathbb{Q}$ qui envoit $z$ sur $\frac{\chi(g)}{\chi(1)}$. $n$ est donc envoyé sur $n$ et les racines de l'unité sur d'autres racines de l'unité (éléver à la bonne puissance pour en conclure que ce sont encore des racines de l'unité). On en déduit que $|z| \leq 1$. Soit $a_0$ le coefficient constant de $P$, on a $|a_0| = |\prod_{z \in \mathrm{rac}(P)} z|$, donc $|a_0| \leq 1$. Or $P \in \mathbb{Z}[X]$ car $\frac{\chi(g)}{\chi(1)}$ est un entier algébrique. Donc $a_0 \in \{-1, 0, 1\}$. Si $a_0 = 0$ alors $P = X$ et $\frac{\chi(g)}{\chi(1)} = 0$ donc $\chi(g) = 0$. Sinon $|a_0| = 1$ et alors $|\prod_{z \in \mathrm{rac}(P)} z| = 1$ donc tout les modules valent 1 en particulier celui de $\frac{\chi(g)}{\chi(1)}$ or c'est l'isobarycentre de racine de l'unité qui est lui-même sur le cercle unité. On en déduit que tout les $\lambda_i$ sont égaux or $\rho(g)$ est diagonalisable de valeur propre les $\lambda_i$, c'est donc une homothétie. □

**Théorème 3.2.** *Soient $p$ et $q$ des nombres premiers distincts et $a$, $b$ des entiers naturels alors tout groupe d'ordre $p^a q^b$ est résoluble.*

*Démonstration.* On fait la preuve par récurrence forte, l'hypothèse $H_n$ étant : "tout groupe d'ordre $p^a q^b$ avec $p^a q^b \leq n$ est résoluble".

Initialisation : On se débarasse des groupes pour lesquels $a = 0$ ou $b = 0$. En effet le groupe trivial est résoluble. Les groupes d'ordre $p^a$ ou $q^b$ sont résolubles (ce sont des $p - groupes$). On peut aussi rajouter les groupes d'ordre $pq$ car alors (en supposant $q > p$, le $q - Sylow\ S$ est distingué et $G/S$ et $S$ sont résolubles ($p - groupes$) donc $G$ aussi.

Hérédité : Si $G$ a un centre non trivial $Z$ alors $G/Z$ est résoluble par hypothèse et $Z$ l'est aussi (par hypothèse ou simplement parce qu'il est abélien) donc $G$ est résoluble.

Supposons donc $Z = \{1\}$. Alors il existe une classe de conjugaison $C$ différente de celle du neutre telle que $q$ ne divise pas $|C|$. En effet dans le cas contraire on aurait :

$$|G| = 1 + \sum_{C \neq 1} |C|$$

ce qui donne $1 = 0$ modulo $q$ ce qui est absurde. On en déduit donc que $|C| = p^i$ avec $i \in \mathbb{N}^*$.

Il existe aussi un caractère irréductible $\chi$ non trivial tel que pour tout $g \in C$, $\chi(g) \neq 0$ et $\chi(1) \neq 0\ (mod\ p)$. En effet dans le cas contraire en écrivant la relation d'orthogonalité entre les colonnes de la classe du neutre et de celle de $C$, on obtient pour $g \in C$ :

$$0 = 1 + \sum_{\chi \neq 1} \chi(1)\chi(g)$$

soit

$$\frac{-1}{p} = \sum_{\chi \neq 1} \chi(g)\frac{\chi(1)}{p}$$

On en déduit donc que $\frac{-1}{p}$ est un entier algébrique donc qu'il appartient à $\mathbb{Z}$, c'est absurde. On est donc dans les conditions d'application de la proposition précédente et on en déduit que pour tout $g \in C$, $\rho(g)$ est une homothétie donc appartient au centre de $GL_n(\mathbb{C})$. On considère donc $ker(\rho)$ qui est un sous-groupe distingué de $G$. Il est différent de $G$ car $\chi$ est non trivial. Il est non trivial car sinon on aurait que $\rho$ est injective et alors pour tout $h \in G$ et $g \in C$,

l'égalité $\rho(gh) = \rho(hg)$ (venant du fait que $\rho(g)$ commute) impliquerait $hg = gh$ par injectivité donc $g \in Z$ or le centre est trivial et $C$ est différent de la classe du neutre. Donc $ker(\rho)$ est un sous-groupe distingué non trivial, on en déduit que $ker(\rho)$ et $G/ker(\rho)$ sont résolubles par hypothèse de récurrence donc que $G$ est résoluble. □

# 4 Commentaires

C'est un très beau résultat qui est un pas en direction du très dur théorème de Feit-Thompson affirmant que tout groupe de cardinal impair est résoluble. Le fait que les caractères soient des entiers algébriques est au coeur de la démonstration, ce genre de résultat venant de l'intégralité des caractères est souvent souligné.

Cela permet par exemple de montrer que tout groupe d'ordre inférieur à 60 non abélien n'est pas simple (les cas 30 et 42 sont à traiter à la main, mais ils se règlent vite avec les théorèmes de Sylow). $A_5$ est donc le premier groupe simple non abélien (il s'agit du seul à isomorphisme près mais c'est un autre développement).

# 5 Recasages

Ce développement admet un très bon recasage, encore meilleur si on accepte de forcer un peu...

- 102 : Nombres complexes de module 1 : Excellent, en plus dans une leçon où j'ai peiné à trouver des développements. On fait le dessin avec l'isobarycentre et l'intégralité des caractères découle de celle des racines de l'unité.
- 103 : Conjugaison dans un groupe, sg distingués/quotients : C'est excellent aussi, les caractères sont constants sur les classes de conjugaison et tout la démonstration consiste en la recherche d'un sous-goupe distingué non trivial pour faire un quotient et appliquer l'hypothèse de récurrence. De plus le théorème à des implications directes sur la simplicité des groupes, notion qui a toute sa place dans la leçon.
- 104 : Groupes finis : A-t-on besoin d'en dire plus ?
- 127 : Nombres remarquables, anneaux de nombres remarquables : Évident via le fait que l'anneau des entiers algébriques est au coeur du développement.
- 121 : Nombres premiers : C'est dans l'énoncé du théorème. Cela se case très bien si on fait une partie sur les p-groupes par exemple.
- 141 : Polynômes irréductibles, corps de rupture : On arrive sur les recasages un peu plus forcés mais je pense que sa place peut se justifier si on prend le temps de détailler un peu plus la proposition au début.
- 144 : Racines d'un polynôme. Fonctions symétriques élémentaires : Pareil il faut plus insister sur le fait que le polynôme minimal d'un entier algébriques est dans $\mathbb{Z}[X]$.
- 125 : Extension de corps : Là ça devient peut-être un peu abusé. Il faut sûrement faire une sous-partie sur les corps de rupture et bien insité sur ça pendant la preuve mais je ne conseille pas vraiment.

# 6 Questions auxquelles il faut savoir répondre

Ce développement de très bon niveau (je pense), a beaucoup de résultats admis et il faut savoir les démontrer. Par ordre dans le développement :

1. Il faut connaître la démonstration de la proposition qui n'est pas démontrée. Elle n'a rien d'évident et utilise le lemme de Schur qui est au coeur des représentations (il faut donc connaître le lemme de Schur).
2. Il faut savoir démontrer que les entiers algébriques forment un anneau (via le résultant par exemple ou les idéaux $\mathbb{Z}[x]$ de type fini).
3. Il faut savoir démontrer que les caractères sont des sommes de racines de l'unité et que les $\rho(g)$ sont diagonalisables.
4. Il faut savoir justifier le passage avec l'automorphisme de corps, soit via le théorème sur les corps de rupture, soit en le redémontrant (ce n'est pas plus long et évite des questions en ce sens). Il faut aussi savoir montrer que les racines de l'unité sont envoyées sur des racines de l'unité.
5. Il faut savoir que le polynôme minimal d'un entier algébrique est dans $Z[X]$ (via les polynômes symétriques, relations coefficients-racines).
6. C'est bien de faire un dessin lorsqu'on dit que si l'isobarycentre de points sur le cercle est lui-même sur le cercle alors tout les points sont confondus (et donner plus de détails si c'est demandé).
7. Il faut savoir démontrer que les $p-groupes$ sont résolubles (via le fait qu'ils aient un centre non trivial, chose qu'il faut aussi savoir démontrer).
8. Être un minimum à l'aise avec les théorèmes de Sylow.
9. Connaître les deux définitions de la résolubilité (via les groupes dérivées et les suite à quotients abéliens). Savoir montrer que $G$ est résoluble ssi $H$ et $G/H$ sont résolubles.
10. Il faut bien sûr être un minimum à l'aise avec la théorie des représentations et celle des caractères. Il faut connaître le résultat d'orthogonalité des caractères (qui vient du lemme de Schur) et savoir aussi que celui qu'on utilise n'est pas exactement le même. C'est un résultat d'orthogonalité qui vient après l'autre en ayant démontrer que les caractères irréductibles forment une base de l'espace des fonctions centrales. Il peut se démontrer de plusieurs manières mais je trouve la démonstration faite dans Jean-Pierre Serre assez éclairante en décomposant une fonction indicatrice d'une classe de conjugaison dans la base des caractères irréductibles. Il faut aussi savoir que le résultat d'orthogonalité qu'on utilise (spécialement entre la classe du neutre et une autre) peut aussi se retrouver d'une manière moins compliquée sans utiliser le fait que les caractères soient une base mais simplement en exprimant la représentation régulière de $G$ avec les caractères irréductibles (pas besoin de savoir que c'est une base pour faire ça car c'est un caractère donc juste besoin du théorème de Maschke, qu'il faut donc connaître aussi).
11. Il faut aussi par conséquent savoir ce qu'est une table de caractère et savoir un peu la lire.
12. Il faut savoir montrer qu'un élément de $\mathbb{Q}$ qui est un entier algébrique est en fait dans $\mathbb{Z}$.

Cela peut paraître beaucoup de choses à savoir mais un bon cours sur les représentations suffira. Je recommande particulièrement le livre de Jean-Pierre Serre sur le sujet mais aussi de mixer et de voir plusieurs référence. Par exemple dans Le Grand Combat, NH2G2 (où les exercices sont très biens), Algèbre et calcul formel ou encore le livre de Gérard Rauch qui contient le principal du développement. J'ai juste dû prendre des résulats dans NH2G2 pour justifier les propositions avant le théorème sans utiliser la notion d'algèbre de groupe.