Deux résultats de Burnside

Benoît Claudon

5 novembre 2009

On démontre ici deux résultats de Burnside sur les groupes finis (en lien avec les représentations linéaires). Le premier est bien connu.

Théorème 1 (Burnside, 1905)
Si G un groupe fini dont l'ordre a au plus deux facteurs premiers, G est alors résoluble.

La démonstration qui suit s'appuie sur la théorie des caractères pour laquelle on se reportera au livre de Jean-Piere Serre [Se78] (elle y est d'ailleurs proposée en exercice).

Lemme 1.1
Soit $\lambda_1, \dots, \lambda_n$ des racines de l'unité et posons

$$a = \frac{1}{n} \sum_{i=1}^{n} \lambda_i.$$

Si a est un entier algébrique, alors $a = 0$ ou $a = \lambda_1 = \cdots = \lambda_n$.

Démonstration :
Soit K le corps cyclotomique qui contient tous les λ_i et $a_1 = a, a_2, \dots, a_k$ les conjugués de a. Pour $j \leq k$, on a donc $a_j = \sigma_j(a)$ où σ_j est un élément du groupe de Galois de $K/\mathbb{Q}$. Comme sur les racines de l'unité, ce groupe agit par exponentiation, on a :

$$a_j = \sigma_j(a) = \frac{1}{n} \sum_{i=1}^{n} \sigma_j(\lambda_i) = \frac{1}{n} \sum_{i=1}^{n} \lambda_i^m$$

(pour un certain entier m). On en déduit en particulier : $|a_j| \leq 1$ pour tout $1 \leq j \leq k$. Si on pose

$$A = \prod_{j=1}^{k} a_j,$$

on a donc $|A| \leq 1$. De plus, A est un entier algébrique (par hypothèse) et, comme c'est le coefficient constant du polynôme minimal de a, on a également $A \in \mathbb{Q}$; A est donc un entier. Si a est non-nul, on en déduit immédiatement $|a| = 1$ et le cas d'égalité de l'inégalité triangulaire montre que les λ_i sont tous égaux. □

Lemme 1.2
Soit ρ une représentation irréductible d'un groupe fini G de caractère χ et de degré d. Soit $g \in G$ et $c(g)$ le cardinal de la classe de conjugaison de l'élément g. Si $c(g)$ et d sont premiers entre eux et si $\chi(g) \neq 0$, $\rho(g)$ est une homothétie.

Démonstration :

On applique tout d'abord le corollaire 1 p. 67 de [Se78] : $\dfrac{c(g)\chi(g)}{d}$ est un entier algébrique. Comme $c(g)$ et d sont premiers entre eux, on se donne des entiers a et b tels que $ac(g) + bd = 1$ et on a :

$$\frac{1}{d}\chi(g) = \frac{ac(g) + bd}{d}\chi(g) = a\frac{c(g)\chi(g)}{d} + b\chi(g).$$

Le lemme 1.1 s'applique puisque l'égalité ci-dessus montre que $\dfrac{1}{d}\chi(g)$ est un entier algébrique non-nul : toutes les valeurs propres de $\rho(g)$ sont égales et $\rho(g)$ est donc une homothétie. □

La proposition suivante va nous permettre de procéder par récurrence pour montrer le théorème 1.

Proposition 1.1
Soit G un groupe fini et $g \in G$ ($g \neq 1$) que $c(g) = p^\alpha$ avec p premier. Il existe alors un sous-groupe distingué propre *$N \lhd G$ tel que $\overline{g} \in Z(G/N)$ ($\overline{g}$ désigne la classe de g dans G/N).*

Démonstration :

On commence par appliquer l'orthogonalité des caractères. Comme $g \neq 1$, on a en effet :

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

Supposons alors que, pour tout caractère $\chi \neq 1$, on ait :

$$\chi(g) = 0 \text{ ou } \chi(1) \equiv 0\,[p].$$

La relation (1) s'écrit alors :

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

L'hypothèse faite ci-dessus montre alors que $1/p$ est un entier algébrique (comme combinaison à coefficients entiers d'entiers algébriques) ; on devrait donc avoir $1/p \in \mathbb{Z}$. On en déduit donc qu'il existe un caractère $\chi \neq 1$ avec $\chi(g) \neq 0$ et $\chi(1) \not\equiv 0\,[p]$. Si ρ désigne la représentation irréductible de caractère χ, le lemme 1.2 permet d'affirmer que $\rho(g)$ est une homothétie et le sous-groupe $N = \mathrm{Ker}(\rho)$ convient. □

Nous sommes maintenant en mesure de montrer le théorème 1.

Démonstration du théorème 1 :

Par récurrence sur $|G|$, il suffit de montrer que G n'est pas simple (tout sous-groupe et tout quotient vérifie la même hypothèse que G) sauf bien entendu si $G = \mathbb{Z}/p\mathbb{Z}$. On examine alors la dichotomie suivante. Si $Z(G)$ n'est pas trivial (et distinct de G), $Z(G)$ fournit un sous-groupe distingué non trivial. On peut donc supposer que $Z(G) = 1$.

Comme $Z(G) = 1$, la partition de G en classes de conjugaison donne :

$$|G| = p^\alpha q^\beta = 1 + \sum_{j \in J} c(g_j)$$

où g_j désigne des représentants des classes. On en déduit donc qu'il existe un élément $g \neq 1$ de G dont le cardinal de la classe de conjugaison est une puissance d'un nombre premier. On applique alors la proposition 1.1 : il existe un sous-groupe distingué propre N de G tel $\overline{g} \in Z(G/N)$. Comme on a supposé que $Z(G) = 1$, le sous-groupe N est non trivial et le groupe G n'est pas simple. □

Remarque 1

Le théorème 1 n'admet bien sûr pas d'extension au cas où le cardinal de G admet au moins trois facteurs premiers. Le groupe A_5 (de cardinal $60 = 2^2.3.5$) est simple. On peut d'ailleurs remarquer que tout groupe d'ordre < 60 est résoluble (et A_5 est ainsi le premier exemple non-résoluble). En effet, avec le théorème 1, il suffit d'examiner les nombres < 60 qui ont au moins trois facteurs premiers : il s'agit de $30 = 2.3.5$ et $45 = 2.3.7$. Or, dans un groupe d'ordre 45, le 7-Sylow est distingué. Dans un groupe d'ordre 30, si n_3 (resp. n_5) désigne le nombre de 3-Sylow (resp. de 5-Sylow), on a : $n_3 \in \{1, 10\}$ et

$n_5 \in \{1, 6\}$. Un argument de comptage montre qu'on ne peut avoir $n_3 = 10$ et $n_5 = 6$, ce qui montre bien qu'un groupe d'ordre 30 n'est pas simple (et est donc résoluble).

Remarque 2
Il est naturel de se demander si il existe une démonstration du théorème 1 qui ne fasse pas appel à la théorie des caractères. La réponse à cette interrogation est positive... mais il aura fallu attendre plus de 60 ans pour disposer d'une telle démonstration ! On pourra trouver une approche du théorème de Burnside sans caractère dans le livre [KS04], ainsi que des remarques intéressantes sur le sujet.

Le second résultat de Burnside que nous allons présenter est sans-doute moins connu.

Théorème 2
Soit χ un caractère irréductible de degré > 1 d'un groupe fini G. Il existe un élément $g \in G$ tel que $\chi(g) = 0$.

Démonstration :
Posons :

$$N(\chi) = \prod_{g \in G} |\chi(g)|^2 .$$

Si $K = \mathbb{Q}(e^{2i\pi/n})$ (avec $n = |G|$), on a bien entendu $N(\chi) \in K$. D'autre part, si $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$, on sait que σ agit sur les racines de l'unité (contenues dans K) par $\sigma(z) = z^m$ avec m premier avec n. Si $g \in G$ et $\lambda_1, \ldots, \lambda_d$ désignent les valeurs propres de $\rho(g)$, on a :

$$\sigma(\chi(g)) = \sum_i \sigma(\lambda_i) = \sum_i \lambda_i^m = \chi(g^m).$$

Comme σ commute à la conjugaison complexe, on a donc :

$$\sigma(N(\chi)) = \prod_{g \in G} |\chi(g^m)|^2 .$$

Comme m est premier à l'ordre de G, l'application $g \mapsto g^m$ est une bijection de G et $N(\chi)$ est donc invariant par l'action de $\mathrm{Gal}(K/\mathbb{Q})$. On a ainsi montré $N(\chi) \in \mathbb{Q}$. Ceci entraîne immédiatement que $N(\chi)$ est un entier (positif) puisque c'est un entier algébrique.

On va maintenant utiliser le fait que la représentation est irréductible. En effet, l'inégalité arithmético-géométrique donne :

$$N(\chi)^{1/n} \leq \frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2 = 1,$$

les caractères irréductibles formant une base orthonormée des fonctions centrales sur G. L'entier $N(\chi)$ vaut donc soit 0 soit 1. Le cas $N(\chi) = 1$ correspond au cas d'égalité dans l'inégalité arithmético-géométrique : $|\chi(g)| = 1$ pour tout $g \in G$ et la représentation est alors de degré 1. Comme nous avons supposé que ce n'était pas le cas, on a $N(\chi) = 0$, ce qui achève la démonstration du théorème 2. $\square$

Références

[Se78] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, Paris (1978)

[KS04] H. Kurzweil, B. Stellmacher, *The theory of finite groups. An introduction*, Springer-Verlag, New-York (2004)