Le théorème $p^a q^b$ de Burnside

L'objectif de ce problème est de montrer le théorème $p^a q^b$ de Burnside, qui s'énonce en ces termes : si G est un groupe fini de cardinal $p^a q^b$, où p, q sont premiers et $a, b \in \mathbb{N}$, alors G est résoluble. Il demande une certaine familiarité avec la théorie des groupes finis, et en particulier avec la théorie des représentations des groupes finis, et de leurs caractères.

Rapellons les quelques définitions inhérentes au problème. On fixe G un groupe fini de cardinal $n \in \mathbb{N}^*$, de neutre noté e. Le groupe dérivé de G, noté $D(G)$, est défini comme le sous-groupe de G engendré par les commutateurs de G :

$$D(G) = \mathrm{Gr}\{[x, y] \mid x, y \in G\}$$

(où on a noté $[x, y] = xyx^{-1}y^{-1}$ pour tous $x, y \in G$.).
On définit récursivement la suite dérivée de G, notée $(D^n(G))_{n\geq 0}$, par :

$$D^0(G) = G \qquad \forall n \in \mathbb{N},\ D^{n+1}(G) = D(D^n(G))$$

Le groupe G est dit *résoluble* si et seulement si sa suite dérivée stationne à $\{e\}$.
On donne également la définition d'un groupe simple : G est dit *simple* si et seulement si ses seuls sous-groupes distingués sont G et $\{e\}$.

1 Quelques exemples

1. Dans cette question, $\mathbb{K}$ désigne un corps de caractéristique nulle. On considère le groupe $G = \mathrm{GL}_n(\mathbb{K})$. On note $(E_{i,j})_{1\leq i,j\leq n}$ la base canonique de $\mathcal{M}_n(\mathbb{K})$, et pour tous $i, j \in [\![1, n]\!]$, tout $\lambda \in \mathbb{K}$, on note $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$.

a) Pour tous $i, j, k, l \in [\![1, n]\!]$ et tous $\lambda, \mu \in \mathbb{K}$, calculer le commutateur $[T_{i,j}(\lambda), T_{k,l}(\mu)]$.

b) En déduire que $D(\mathrm{SL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$. On pourra utiliser (après l'avoir démontré !) le fait que $\mathrm{SL}_n(\mathbb{K})$ est engendré par les $T_{i,j}(\lambda)$ où $i, j \in [\![1, n]\!]$ avec $i \neq j$ et $\lambda \in \mathbb{K}$.

c) En déduire la suite dérivée du groupe $\mathrm{GL}_n(\mathbb{K})$. Ce groupe est-il résoluble ?

2. Dans cette question, on traite le cas des groupes symétriques.

a) Calculer les suites dérivées de S_2 et S_3. Ces groupes sont-ils résolubles ?

b) Faire de même avec S_4. On vérifiera entre autres que $D^2(S_4)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

c) Soit maintenant $n \geq 5$. Vérifier que chaque 3-cycle de S_n peut s'écrire comme un commutateur de 3-cycles.

d) En déduire la suite dérivée de S_n. Ce groupe est-il résoluble ?

2 Interlude sur les entiers algébriques

On rappelle la définition d'un entier algébrique : un complexe $z \in \mathbb{Z}$ est dit un *entier algébrique* si et seulement si il est annulé par un polynôme unitaire à coefficients dans $\mathbb{Z}$. On note $\mathcal{A}$ l'ensemble des entiers algébriques.

3. Déterminer $\mathcal{A} \cap \mathbb{Q}$.

4. Soit $z \in \mathbb{C}$. L'objectif de cette question est de démontrer l'équivalence entre les propositions suivantes :
(i) z est un entier algébrique
(ii) Le sous-anneau $\mathbb{Z}[z]$ de $\mathbb{C}$ de type fini.
(iii) Il existe un sous-anneau de type fini $\mathbb{A}$ de $\mathbb{C}$ contenant z.

a) Vérifier les implications $(i) \Rightarrow (ii) \Rightarrow (iii)$.

b) On suppose maintenant (iii) et on considère une famille génératrice finie $(e_1, ..., e_d)$ de $\mathbb{A}$. Vérifier l'existence d'entiers $a_{i,j} \in \mathbb{Z}$ pour $i, j \in [\![1, d]\!]$ tels que :

$$\forall j \in [\![1, d]\!], \quad ze_j = \sum_{i=1}^{d} a_{i,j} e_i$$

c) Vérifier que z est valeur propre de la matrice $(a_{i,j})_{1 \leq i,j \leq n}$ et en déduire la propriété (i).

5. Déduire de ce qui précède que l'ensemble des entiers algébriques $\mathcal{A}$ est un sous-anneau de $\mathbb{C}$.

6. Soit $z \in \mathbb{C}$ un entier algébrique, et $\pi_z \in \mathbb{Q}[X]$ son polynôme minimal sur $\mathbb{Q}$ (qui est donc unitaire). Montrer que π_z est à coefficients entiers. On pourra remarquer à cet effet que les coefficients de π_z sont des entiers algébriques et utiliser la 4.

On établit dans cette dernière question un petit lemme sur les entiers algébriques, qui sera utile dans la démonstration du théorème $p^a q^b$ de Burnside.

7. On fixe $n, d \in \mathbb{N}^*$, et $z_1, ..., z_n$ des racines d-ièmes de l'unité. On suppose que le nombre $z = \frac{1}{n}(z_1 + ... + z_n)$ est un entier algébrique non nul, et on souhaite prouver que $z_1 = ... = z_n$.

a) On note π_z le polynôme minimal de z sur $\mathbb{Q}$. Soit z' une racine de π_z. Montrer l'existence d'un morphisme de corps $f : \mathbb{C} \to \mathbb{C}$ tel que $f(z) = z'$.

b) En remarquant que f envoie une racine de l'unité sur une racine de l'unité, en déduire que $|z'| \leq 1$.

c) Montrer enfin que $|z| = 1$ et conclure.

3 Un critère de non simplicité

Dans toute cette partie, G désigne un groupe fini, de cardinal $n \in \mathbb{N}^*$, de neutre noté e. On suppose l'existence d'un élément $g_0 \in G$ différent de e et tel que la classe de conjugaison de g_0 soit de cardinal p^m, où p est un nombre premier et où $m \in \mathbb{N}$. L'objectif de cette partie est de montrer que, sous ces hypothèses, G n'est pas simple ou G est abélien.

On note $\mathbb{Z}^G$ l'ensemble des fonctions de G dans $\mathbb{Z}$. Pour tout $g \in G$, on note $\delta_g \in \mathbb{Z}^G$ l'indicatrice de g (qui prend la valeur 1 en g et vaut 0 partout ailleurs). Enfin, on définit sur $\mathbb{Z}^G$ la somme usuelle, ainsi que le produit défini par les formules $\delta_g * \delta_h = \delta_{gh}$ pour tous $g, h \in G$ et étendu par bilinéarité.

8. a) Vérifier que ces deux opérations munissent Z^G d'une structure d'anneau (non nécessairement commutatif). Quel est son élément neutre multiplicatif ?

b) On note Z le centre de l'anneau $\mathbb{Z}^G$, c'est à dire :

$$Z = \{f \in \mathbb{Z}^G \mid \forall f' \in \mathbb{Z}^G, \ f * f' = f' * f\}$$

Montrer que Z est l'ensemble des fonctions $f \in \mathbb{Z}^G$ qui sont constantes sur chaque classe de conjugaison.

9. Soit maintenant $\rho : G \to \mathrm{GL}(V)$ une représentation irréductible de G dans le $\mathbb{C}$-espace vectoriel de dimension finie V. On note χ le caractère associé à cette représentation. De plus, pour tout $f \in \mathbb{Z}^G$, on définit :

$$\eta(f) = \sum_{g \in G} f(g)\rho(g) \in \mathcal{L}(V)$$

Si $u \in \mathcal{L}(V)$ est une homothétie, on note $r(u)$ le rapport de cette homothétie.

a) Soit $f \in Z$. Montrer que tout sous-espace propre de $\eta(f)$ est stable par tous les $\rho(g)$ pour $g \in G$. En déduire que $\eta(f)$ est une homothétie.

b) Montrer que $\mathbb{A} = \{r(\eta(f)) \mid f \in Z\}$ est un sous-anneau de $\mathbb{C}$. Est-il de type fini ?

c) Soit maintenant $g \in G$. On note $c(g)$ le cardinal de la classe de conjugaison de g dans G. Montrer que $\frac{c(g)\chi(g)}{\dim(V)}$ et un entier algébrique. En notant ensuite $d(g)$ le pgcd de $c(g)$ et de $\dim(V)$, en déduire que $\frac{d(g)\chi(g)}{\dim(V)}$ est un entier algébrique.

10. On reprend les hypothèses du début de cette partie : g_0 est un élément de G différent de e, dont le cardinal de la classe de conjugaison s'écrit $c(g_0) = p^m$ où p est un nombre premier et $m \in \mathbb{N}$.

a) En utilisant les relations d'orthogonalité de la table de caractères, montrer la relation :

$$\sum_{\chi} \chi(g_0)\chi(e) = -1$$

où la somme porte sur les caractères des représentations irréductibles non triviales (c'est à dire différentes de la représentation $G \to \{1\}$) de G.

b) En déduire l'existence d'une représentation irréductible non triviale $\rho : G \to \mathrm{GL}(V)$ de G, de caractère associé χ, telle que $\chi(g_0) \neq 0$ et telle que p ne divise par $\dim(V)$.

c) Vérifier que $\frac{\chi(g_0)}{\dim(V)}$ est un entier algébrique.

d) En utilisant le lemme de la question 7., en déduire que $\rho(g_0)$ est une homothétie.

11. a) On suppose que G est simple. Montrer que ρ induit un isomorphisme de G dans l'ensemble des homothéthies de $\mathrm{GL}(V)$.

b) Démontrer le résultat annoncé au début de cette partie.

4 Le théorème $p^a q^b$ de Burnside

12. Soit G un groupe fini, H un sous-groupe distingué de G tel que H et le quotient G/H soient résolubles. Montrer que G est résoluble.

13. Soit maintenant G un groupe de cardinal $p^a q^b$ où p, q sont des entiers premiers et $a, b \in \mathbb{N}$. On note toujours e son élément neutre, et on suppose que $G \neq \{e\}$.

a) En écrivant $p^a q^b$ comme somme des cardinaux des classes de conjugaisons des éléments de G, montrer l'existence de $g_0 \in G$ différent de e dont la classe de conjugaison est de cardinal une puissance d'un nombre premier.

b) En déduire que G n'est pas simple ou G est abélien.

14. Montrer le théorème de Burnside : si G est un groupe de cardinal $p^a q^b$ où p, q sont des nombres premiers et $a, b \in \mathbb{N}$, alors G est résoluble.
Indication : Raisonner par récurrence.