Degré de commutativité et structure d'un groupe fini (2)

par Paul Lescot.

Dans cette note, nous apportons quelques précisions aux résultats de [3] et de [4]; en particulier, nous déterminons complètement les groupes finis non nilpotents de degré de commutativité $\frac{1}{2}$, et les groupes finis non résolubles de degré de commutativité $\frac{1}{12}$. Plus précisément, dans la première partie, nous résolvons le problème posé dans l'introduction à [4] pour la classe des groupes nilpotents et, dans la seconde partie, nous le résolvons pour la classe des groupes résolubles; dans la troisième partie, nous présentons l'amorce d'une généralisation de la théorie du degré de commutativité, consistant à remplacer les couples d'éléments du groupe considéré par des n-uplets ($n \geqslant 2$).

Les notations et les définitions sont celles de [4]; en particulier, tous les groupes considérés sont finis. En outre, pour tout élément x d'un groupe G, $\omega(x)$ désignera l'ordre de x dans G, et, pour tout entier $n \geqslant 1$, $\mathbb{N}_n$ désignera l'ensemble $\{1, \ldots, n\}$. Le symbole ■, dû à Paul Halmos, indiquera la fin d'une démonstration.

A. — Groupes non nilpotents extrémaux.

Nous entendons par là un groupe non nilpotent ayant le plus grand degré de commutativité possible, c'est-à-dire $\frac{1}{2}$ d'après le théorème 3 et la remarque finale de [3]. Définissons, pour tout entier $m \geqslant 1$, un groupe G_m de la façon suivante:

$$G_m = \langle \sigma, \tau \mid \sigma^3 = \tau^{2^m} = 1,\ \tau^{-1}\sigma\tau = \sigma^{-1} \rangle.$$

On vérifie aisément que G_m est d'ordre 3.2^m, que $Z(G_m) = \langle \tau^2 \rangle$ est d'ordre 2^{m-1}, que $G_m/Z(G_m)$ est isomorphe à S_3 (en particulier, G_m n'est pas nilpotent), et que $G'_m = \langle \sigma \rangle$ est d'ordre 3. De plus, $A_m = \langle \sigma, \tau^2 \rangle$ est un sous-groupe commutatif distingué de G_m, donc le degré de tout caractère irréductible de G_m divise $|G_m : A_m| = 2$ ([5, p. 77, corollaire]), *i.e.* est égal à 1 ou à 2. Soit λ_m le nombre de caractères irréductibles de degré 2 de G_m; on a (d'après [3, p. 276, 1° et 2°]):

$$|G_m|\, d(G_m) = k(G_m) = \lambda_m + |G_m/G'_m|$$
$$|G_m| = |G_m/G'_m| + 4\lambda_m,$$

soit

$$3.2^m\, d(G_m) = \lambda_m + 2^m$$
$$3.2^m = 2^m + 4\lambda_m.$$

La seconde de ces équations nous donne que $\lambda_m = 2^{m-1}$; la première implique alors que $d(G_m) = \frac{1}{2}$. Les G_m sont donc des groupes non nilpotents extrémaux; en fait, comme nous allons le voir, ce sont les seuls, à un facteur direct abélien près:

Théorème 1. — *Soit* G *un groupe non nilpotent extrémal; alors il existe un groupe commutatif* A *et un entier* $r \geqslant 1$ *tels que* G *soit isomorphe à* $G_r \times A$.

Remarque. — G_1 est isomorphe à S_3, et G_2 au groupe qui apparaît dans la remarque suivant le théorème 5 de [4].

Démonstration. — Soit G un groupe non nilpotent extrémal; d'après le théorème 5 de [4], $G/Z(G)$ est isomorphe à S_3; en outre, le même raisonnement que dans la preuve du théorème 3 de [3] montre que G' est d'ordre 3. Soit σ un générateur de G'; il est clair que σ n'appartient pas à $Z(G)$, donc il existe un élément x de G tel que $x^{-1}\sigma x \neq \sigma$. On a alors $x^{-1}\sigma x = \sigma^{-1}$ (car $\langle \sigma \rangle = G' \lhd G$); en remplaçant au besoin x par x^s, où s est la partie impaire de $\omega(x)$, on peut supposer que l'ordre de x est une puissance de 2. Choisissons maintenant un élément z de G d'ordre minimal tel que $\omega(z)$ soit une puissance de 2 et que $z^{-1}\sigma z = \sigma^{-1}$. En raison de l'isomorphisme $G/Z(G) \simeq S_3$, on a $u = z^2 \in Z(G)$; en outre, la définition de z entraîne que, pour tout 2-élément v de $Z(G)$

$$(*) \qquad \omega(uv^2) \geqslant \omega(u).$$

Supposons $u = 1$; alors z est une involution de G n'appartenant pas à $Z(G)$, donc, d'après la remarque suivant la démonstration du théorème 5 de [4],

$$G \simeq S_3 \times Z(G) \simeq G_1 \times Z(G),$$

d'où le résultat. On peut donc supposer $u \neq 1$; $(*)$ nous donne alors que u n'est pas le carré d'un élément de $Z(G)$, donc que $\langle u \rangle$ est un facteur direct de $Z(G)$. Écrivons

$Z(G) = \langle u \rangle \times Z_1$; il est maintenant clair que $G = \langle \sigma, z \rangle \times Z_1$ est isomorphe à $G_r \times Z_1$, où $2^r = \omega(z)$, *q.e.d.* ■

B. — Groupes non résolubles extrémaux.

D'après le théorème 1 de [4], tout groupe fini non résoluble est de degré de commutativité au plus $\frac{1}{12}$; en outre, $d(A_5) = \frac{1}{12}$. Donc, A_5 est un groupe non résoluble extrémal (au sens évident de cette expression); nous allons démontrer, améliorant ainsi le théorème 3 de [4], que c'est le seul, à un facteur direct abélien près. Pour cela, le lemme suivant nous sera nécessaire.

Lemme 1 (Gallagher [2]). — *Soit* G *un groupe et* H *un sous-groupe de* G; *alors* $d(G) \leqslant d(H)$. *De plus, en cas d'égalité,* H *est distingué dans* G *et* G/H *est commutatif.*

Démonstration. — Soient x et y deux éléments de G tel que $Hx \cap C_G(y) \neq \varnothing$, et soit alors v un élément de $Hx \cap C_G(y)$. On a $Hx = Hv$, d'où

$$Hx \cap C_G(y) = Hv \cap C_G(y) = Hv \cap C_G(y)v = (H \cap C_G(y))v = C_H(y)v,$$

d'où

$$|Hx \cap C_G(y)| = |C_H(y)|.$$

On a donc $|Hx \cap C_G(y)| \leqslant |C_H(y)|$ pour tous éléments x et y de G. Il en résulte que, si $x_1, \ldots, x_n$ désigne un système de représentants des classes à droite de G modulo H, on a pour tout élément y de G:

$$|C_G(y)| = \sum_{i=1}^{n} |Hx_i \cap C_G(y)| \leqslant \sum_{i=1}^{n} |C_H(y)| = n|C_H(y)| = |G : H|\,|C_H(y)|,$$

d'où

$$\begin{aligned} |G|^2 d(G) = \sum_{y \in G} |C_G(y)| &\leqslant \sum_{y \in G} |G : H|\,|C_H(y)| \\ &= |G : H| \sum_{y \in G} |\{x \in H \mid xy = yx\}| \\ &= |G : H| \sum_{x \in H} |\{y \in G \mid xy = yx\}| \\ &= |G : H| \sum_{x \in H} |C_G(x)|. \end{aligned}$$

Or, pour tout élément x de G, $|C_G(x)H| \leqslant G$, d'où

$$|C_G(x)| \leqslant |G : H|\,|C_H(x)|.$$

On a donc

$$\begin{aligned} |G|^2 d(G) &\leqslant |G : H| \sum_{x \in H} |C_G(x)| \\ &\leqslant |G : H| \sum_{x \in H} |G : H|\,|C_H(x)| \\ &= |G : H|^2 |H|^2 d(H) = |G|^2 d(H). \end{aligned}$$

Il découle de là que $d(G) \leqslant d(H)$, et il est clair qu'en cas d'égalité on a $G = C_G(x)H$ pour tout élément x de H. Soient alors $g \in G$ et $x \in H$; on peut écrire $g = ch_1$, où $c \in C_G(x)$ et $h_1 \in H$, d'où

$$g^{-1}xg = h_1^{-1}c^{-1}xch_1 = h_1^{-1}xh_1 \in H.$$

Ceci vaut pour tout $x \in H$ et tout $g \in G$, donc H est distingué dans G; la commutativité de G/H résulte maintenant du lemme 1 de [4]. ■

Nous sommes dorénavant en mesure d'établir le

Théorème 2. — *Soit* G *un groupe non résoluble extrémal; alors il existe un groupe commutatif* C *tel que* G *soit isomorphe à* $A_5 \times C$.

Démonstration. — Soit H un sous-groupe non résoluble d'ordre minimal de G; il est clair que $H = H'$. D'après le lemme 1 de cet article et le théorème 1 de [4],

$$\frac{1}{12} = d(G) \leqslant d(H) \leqslant \frac{1}{12},$$

d'où

$$d(G) = d(H).$$

D'après le lemme 1, H est distigué dans G et G/H est abélien.

Examinons maintenant la structure de H; d'après le théorème 3 de [4], il possède deux sous-groupes M et N tels que $M \subset Z(H)$, que N/M soit isomorphe à A_5, et que H/N soit abélien. Mais $H = H'$, donc $H = N$; on a donc $H/M \simeq A_5$, donc H est une extension centrale essentielle de A_5. D'après [1, p. 170, (33.15) (1)], H est isomorphe à A_5 ou à $SL_2(\mathbb{F}_5)$; mais $d(SL_2(\mathbb{F}_5)) < \frac{1}{12}$, donc H est isomorphe à A_5. $G/C_G(H)$ se plonge donc de façon canonique dans

$$\mathrm{Aut}(H) \simeq \mathrm{Aut}(A_5) \simeq S_5,$$

et

$$HC_G(H)/C_G(H)$$

correspond par cet isomorphisme au sous-groupe A_5 de S_5. Si $G/C_G(H)$ était isomorphe à S_5, on aurait

$$\frac{1}{12} = d(G) \leqslant d(G/C_G(H)) = d(S_5) = \frac{7}{120} < \frac{1}{12}: \text{ absurde !}$$

Donc

$$G = HC_G(H) = H \times C_G(H),$$

et

$$C_G(H) \simeq G/H$$

est commutatif, avec $H \simeq A_5$, *q.e.d.* ■

C. — Une généralisation du degré de commutativité.

Définition. — Soit G un groupe fini, et $n \geqslant 1$ un entier ; le degré de n-commutativité de G est défini par

$$d_n(G) = \frac{1}{|G|^{n+1}} |\{x_1, \ldots, x_{n+1}) \in G^{n+1} \quad \forall (i, j) \in \mathbb{N}^2_{n+1}\ x_i x_j = x_j x_i\}|$$

Il est clair que $d_1(G) = d(G)$ pour tout groupe fini G, et qu'on a la relation suivante, pour tout entier $n \geqslant 1$:

$$(**) \quad |G|^{n+1} d_n(G) = \sum_{x \in G} |C_G(x)|^n d_{n-1}(C_G(x)).$$

Nous nous limiterons à la démonstration d'un seul résultat concernant les $d_n(G)$ pour $n \geqslant 2$; l'étude plus détaillée de leurs valeurs possibles et des liens entre ces dernières et la structure de G sera certainement du plus haut intérêt.

Théorème 3. — *Soit* G *un groupe fini non abélien ; alors* $d_2(G) \leqslant \frac{11}{32}$, *et on a l'égalité si, et seulement si,* G *est de la forme* P × A, *où* A *est un groupe abélien d'ordre impair et* P *un 2-groupe tel que* $P/Z(P) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ et $|P'| = 2$.

Démonstration. — Soit G un groupe fini non abélien ; on a, d'après (**),

$$\begin{aligned}
|G|^3 d_2(G) &= \sum_{x \in G} |C_G(x)|^2 d(C_G(x)) \\
&= \sum_{x \in Z(G)} |C_G(x)|^2 d(C_G(x)) + \sum_{x \in G \setminus Z(G)} |C_G(x)|^2 d(C_G(x)) \\
&= |Z(G)||G|^2 d(G) + \sum_{x \in G \setminus Z(G)} |C_G(x)|^2 d(C_G(x)) \\
&\leqslant |Z(G)||G|^2 d(G) + \frac{|G|^2}{4}(|G| - |Z(G)|) \\
&\leqslant \frac{5}{8}|G|^2|Z(G)| + \frac{1}{4}|G|^2(|G| - |Z(G)|)
\end{aligned}$$

(d'après le théorème 2 de [3])

$$\begin{aligned}
&= \frac{3}{8}|G|^2|Z(G)| + \frac{1}{4}|G|^3 \\
&\leqslant \frac{3}{8}|G|^2\frac{|G|}{4} + \frac{1}{4}|G|^3 = \frac{11}{32}|G|^3
\end{aligned}$$

(d'après le lemme 2 de [4]),

d'où $d_2(G) \leqslant \frac{11}{32}$. Il est clair qu'en cas d'égalité on a $d(G) = \frac{5}{8}$, donc, d'après le théorème 7 de [4], G est de la forme indiquée ; réciproquement, si G est de cette forme, il est facile de voir que $d(G) = \frac{5}{8}$, que $|G/Z(G)| = 4$ et que $C_G(x)$ est abélien et d'indice 2 dans G pour tout élément x de $G \setminus Z(G)$, donc qu'on a l'égalité partout dans le calcul précédent, d'où $d_2(G) = \frac{11}{32}$. ∎

Remarque 1. — On peut vérifier aisément que la condition $|P'| = 2$ est superflue dans l'énoncé du théorème 3, *i.e.* que tout 2-groupe P satisfaisant $P/Z(P) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ possède un groupe des commutateurs d'ordre 2.

Remarque 2. — Un raisonnement utilisant (**) et analogue à celui du théorème 2 permet de démontrer que, pour tout groupe fini non abélien G et pour tout entier $n \geqslant 1$, on a

$$d_n(G) \leqslant \frac{3.2^n - 1}{2^{2n+1}},$$

et qu'on a l'égalité si, et seulement si, G est de la forme décrite ci-dessus.

Bibliographie

[1] M. Aschbacher, *Finite Group Theory*, Cambridge University Press, 1986.

[2] P. X. Gallagher, « The number of conjugacy classes in a finite group », *Mathematische Zeitschrift*, **118** (1970), 175-179.

[3] P. Lescot, « Sur certains groupes finis », *RMS* (avril 1987), 276-277.

[4] P. Lescot, « Degré de commutativité et structure d'un groupe fini », *RMS* (avril 1988), 276-279.

[5] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, Paris, 1971.

Diagonalisation des matrices symétriques réelles : la méthode variationnelle

par J.-B. Hiriart-Urruty, Université Paul Sabatier, Toulouse
et G. Lion, Université de Limoges.

Dans les classes de Spéciales et en 2e année des premiers cycles universitaires, comme dans les manuels que l'on y utilise, la tradition veut que les endomorphismes symétriques de $\mathbb{R}^n$ soient prolongés à $\mathbb{C}^n$, puis étudiés dans leurs rapports avec le produit hermitien (notion qui ne figure pas dans tous les programmes), et que l'existence de leur spectre soit déduite du théorème de d'Alembert-Gauss (résultat non toujours démontré à ce niveau).

Pour éviter tous ces paradoxes, nous proposons une approche *qui ne sort pas du cadre des espaces réels*, et qui met seulement en œuvre un théorème d'analyse du programme, démontré habituellement tôt dans l'année. La méthode préconisée consiste à maximiser une fonction de plusieurs variables sur un compact (d'où l'appellation de *méthode variationnelle*) et à utiliser à bon escient des inégalités sur les fonctions polynômiales de degré deux.

Les résultats à obtenir sont les suivants :

1. *Toutes les valeurs propres d'une matrice symétrique réelle sont réelles.*

2. *Un endomorphisme symétrique* u *d'un espace euclidien* E *est diagonalisable dans une base orthonormée de* E *formée de vecteurs propres de* u.

Sans attendre l'étude des espaces euclidiens et des endomorphismes symétriques (qui se fait plus tard dans l'année), le lecteur-étudiant peut considérer le résultat 2 dans un contexte simple connu de lui (niveau bac + 1) : $\mathbb{R}^n$ muni de sa base canonique et du produit scalaire usuel. D'ailleurs, tout ce qui suit peut être vu dans ce contexte sans que cela entraîne une perte de généralité. Il est bon de connaître le résultat 1 très tôt dans l'année, dès que la question des valeurs propres d'une matrice réelle est abordée. Tenter de montrer d'entrée ce résultat conduit habituellement à « complexifier » d'une manière ou d'une autre (*cf.* exercice 1.13 de [1] par exemple) ; la méthode variationnelle permet précisément d'éviter cela.

I. — Définitions essentielles.

Soit E un espace vectoriel réel, que la donnée du produit scalaire $(x, y) \mapsto \langle x, y \rangle$ munit d'une structure d'espace *euclidien*. On dit que u, endomorphisme de E, est *symétrique*, lorsque l'on a, pour tous x et y de E

$$\langle x, u(y) \rangle = \langle u(x), y \rangle.$$

Si l'on désigne par $B(x, y)$ le nombre réel qui vient d'apparaître, on définit une forme bilinéaire symétrique B sur E. Posons enfin pour tout $x \in E$:

$$Q(x) = B(x, x) ;$$

Q est une forme quadratique sur E, dont la connaissance permet réciproquement de retrouver B, grâce à la relation :

$$B(x, y) = \frac{1}{4}[Q(x + y) - Q(x - y)].$$

On dit que Q est *positive* (on dit aussi *semi-définie positive*) si, pour tout x de E, on a $Q(x) \geqslant 0$.

Démontrons alors l'inégalité de Schwarz [1] :

Pour tous x *et* y *de* E, *on a, si* Q *est positive,*

$$[B(x, y)]^2 \leqslant Q(x).Q(y).$$

En effet, pour tout t réel, le polynôme du second degré

$$t \mapsto P(t) = Q(x + ty) = t^2Q(y) + 2tB(x, y) + Q(x)$$

est $\geqslant 0$. Ce polynôme peut donc être :

— de degré 0, auquel cas $Q(y) = B(x, y) = 0$, et l'inégalité recherchée est vérifiée ;

— de degré 2, auquel cas P a un discriminant nécessairement négatif, ce qui s'écrit :

$$[B(x, y)]^2 - Q(x).Q(y) \leqslant 0. \quad ∎$$

(1) Schwarz s'écrit sans T ! S'il y a plusieurs mathématiciens du nom de Schwartz, celui-ci est Herman A. Schwarz, mathématicien allemand (1843-1921), dont le lecteur-étudiant retrouvera le nom en analyse, par exemple à propos du théorème d'interversion des dérivées partielles d'ordre 2 d'une fonction.

Pour des raisons historiques, il serait plus juste de parler de l'inégalité de Cauchy-Buniakovski-Schwarz (C.B.S.), ce que ne manquent pas de faire nos collègues soviétiques. Si A.-L. Cauchy (1789-1857) prouva le premier une inégalité de ce type dans $\mathbb{R}^n$, une version plus générale fut donnée par V. Buniakovski (1804-1889), puis la forme générale par H. A. Schwarz. Cela explique que l'on se contente souvent de dire « inégalité de Schwarz ».