Sous-groupe de Frattini

Références : Calais, *Eléments de théorie des groupes* ou Rotman, *An Introduction to the theory of groups.*

Soit G un groupe. On définit le *sous-groupe de Frattini de* G, noté $\Phi(G)$, comme étant l'intersection des sous-groupes maximaux de G. (Un sous-groupe strict $M \subset G$ est dit *maximal* s'il n'y a pas de sous-groupe compris strictement entre M et G.)

Le but de ce qui suit est de montrer que si G est un p-groupe fini, $\Phi(G)$ est engendré par les puissances p-èmes et les commutateurs. La preuve montre aussi que $G/\Phi(G)$ est un $\mathbb{F}_p$-espace vectoriel, et fournit sa dimension.

Pour un développement d'oral, on peut élaguer un peu ; par exemple, on peut sauter la question (1) ; le point (4) peut être considéré comme « connu » ; la question (3) ne sert qu'à montrer (4) ; la question (7) (n')est (qu')un bonus.

Leçons concernées :
Groupes opérant sur un ensemble. Exemples et applications.
Exemples de sous-groupes distingués et de groupes quotients. Applications.
Groupes finis. Exemples et applications.
Exemples de parties génératrices d'un groupe.
Dimension d'un espace vectoriel. Rang. Exemples et applications.

L'exercice.

(1) On dit qu'une partie X d'un groupe G est *superflue* si pour toute partie $A \subset G$, on a :

$$\langle A, X \rangle = G \Rightarrow \langle A \rangle = G .$$

Montrez que si X est superflu, alors tout élément $x \in X$ est superflu. Montrez que si G est de type fini, la réciproque est vraie. Donnez un contre-exemple lorsque G n'est pas de type fini.

(2) Montrez que l'ensemble des éléments superflus de G est égal à $\Phi(G)$.

(3) Dans toute la suite, G est un p-groupe fini. Soit $H \subset G$ un sous-groupe et $N = N_G(H)$ son normalisateur. En faisant agir H par conjugaison sur G/H, montrez que $H \neq G \Rightarrow H \neq N$.

(4) Déduisez-en que les sous-groupes maximaux de G sont distingués et d'indice p.

(5) Notons $G^p[G, G]$ le sous-groupe engendré par les puissances p-èmes et les commutateurs. Montrez que $G^p[G, G] \subset \Phi(G)$.

(6) Soit $i\colon G/G^p[G, G] \to G/\Phi(G)$ le morphisme surjectif induit par l'inclusion précédente. En justifiant que $G/G^p[G, G]$ est un $\mathbb{F}_p$-espace vectoriel et en utilisant (1), montrez que i est un isomorphisme puis que $G^p[G, G] = \Phi(G)$.

(7) On note r le *rang* de G, c'est-à-dire le nombre minimal d'éléments d'un système de générateurs de G. Montrez que la dimension de $G/\Phi(G)$ comme $\mathbb{F}_p$-espace vectoriel est égale à r.

La correction.

(1) Supposons X superflu, soient $x \in X$, $A \subset G$. Si $\langle A, x\rangle = G$ alors $\langle A, X\rangle = G$ donc $\langle A\rangle = G$. Donc x est superflu.

On suppose maintenant G de type fini et on suppose que tout élément $x \in X$ est superflu. Soit $A \subset G$ tel que $\langle A, X\rangle = G$. Choisissons un système générateur fini $g_1, \dots, g_n$ de G, alors chaque g_i s'écrit comme un produit d'éléments de $A \cup X$ et de leurs inverses ; chaque tel produit fait intervenir un nombre fini d'éléments de X ; comme il y a un nombre fini de g_i, au total les éléments de X qui sont en jeu forment un ensemble fini $X_0 \subset X$. Puisque les g_i engendrent G, on a ainsi $\langle A, X_0\rangle = G$. Comme chaque $x \in X_0$ est superflu par hypothèse, on peut les enlever un à un, et comme X_0 est fini, après un nombre fini d'étapes on trouve $\langle A\rangle = G$. On a montré que X est superflu.

Si G n'est pas de type fini, il n'est pas vrai en général qu'une partie est superflue dès que tous ses éléments le sont. Par exemple, soit $G = \mathbb{Z}[1/n]$ le groupe additif des rationnels dont le dénominateur est une puissance de n. Posons $x_k = 1/n^k$ et $X = \{x_k\}_{k\geq 1}$. On voit que les sous-groupes monogènes $\langle x_k\rangle$ sont emboîtés et leur union est G. On en déduit que X engendre G, alors que les x_k sont tous superflus.

(2) Soit $x \in \Phi(G)$ et $A \subset G$ une partie. Si A n'engendre pas G, alors par le lemme de Zorn, il existe un sous-groupe maximal M contenant $\langle A\rangle$. Comme $x \in M$ par définition, on a donc $\langle A, x\rangle \subset M$ donc $\langle A, x\rangle \neq G$.

Réciproquement, si x est un éléments superflu, soit M un sous-groupe maximal. Comme M n'engendre pas G (c'est un sous-groupe strict), et que x est superflu, alors $\langle M, x\rangle \neq G$. En particulier, $x \in M$, par maximalité de M. Donc $x \in \Phi(G)$.

(3) Faisons agir H sur G/H par $h.gH = hgh^{-1}H$. Ceci a bien un sens, car si on change le représentant g pour un représentant $g' = gk$ de la même classe ($k \in H$), alors du fait que $hkh^{-1} \in H$, on a $h.g'H = hgkh^{-1}H = hgh^{-1}hkh^{-1}H = hgh^{-1}H = h.gH$.

Les orbites ponctuelles pour cette action sont les $\{gH\}$ tels que pour tout $h \in H$, on a $hgh^{-1}H = gH$. Ceci équivaut à $g^{-1}hgh^{-1}H = H$, ou encore $g^{-1}hg \in H$ pour tout h, i.e. $g^{-1}Hg = H$. Ce sont donc les orbites $\{gH\}$ avec $gH \in N/H$. La formule des classes donne :

$$|G/H| = |N/H| + \sum |\omega|$$

où le premier terme compte les orbites de cardinal 1 (orbites ponctuelles), et le second, les orbites de cardinal > 1 (donc divisible par p). Modulo p, ceci donne $0 \equiv |N/H|$ (p) et il en découle que $|N/H| \neq 1$, donc $H \neq N$.

(4) Soit M un sous-groupe maximal de G. D'après (2), le normalisateur N de M contient strictement M, donc $N = G$ par maximalité, c'est-à-dire, M est distingué. On regarde ensuite le quotient $\pi \colon G \to G/M$ et on choisit, par le lemme de Cauchy, un sous-groupe $H \subset G/M$ cyclique d'ordre p. La préimage de H par π est un sous-groupe qui contient strictement M, donc c'est G par maximalité. Ainsi $G/M \simeq H$ est cyclique d'ordre p, cqfd.

(5) Soit $x \in G$ un élément qui est soit une puissance p-ème, soit un commutateur. Soit M un sous-groupe maximal de G. Comme $G/M \simeq \mathbb{Z}/p\mathbb{Z}$ d'après (3), en particulier G/M est abélien et d'exposant p (c'est-à-dire que la puissance p-ème de tout élément est égale à 1). Donc l'image de x dans G/M est 1. Il en découle que $x \in \Phi(G)$. Ainsi, le sous-groupe $G^p[G, G]$, qui est engendré par les puissances p-èmes et les commutateurs, est inclus dans $\Phi(G)$.

(6) Par le procédé de quotient, dans le groupe $E = G/G^p[G, G]$, les puissances p-èmes et les commutateurs sont nuls. Donc ce groupe est abélien (on le notera donc additivement) et

d'exposant p. Ainsi l'application $\mathbb{F}_p \times E \to E$, donnée par $(n, g) \mapsto ng$, est bien définie et fait de E un $\mathbb{F}_p$-espace vectoriel. Notons s sa dimension.

Il reste à voir que i est injectif (donc un isomorphisme). Supposons qu'il existe un élément non nul e_1 dans le noyau de i. On peut compléter e_1 en une base $e_1, e_2, \dots, e_s$ de E. Ce système engendre E, donc $i(e_2), \dots, i(e_s)$ engendrent $G/\Phi(G)$ (rappelons-nous que $i(e_1) = 0$). Notons x_i un antécédent de e_i dans G. Il s'ensuit que la partie formée de $x_2, \dots, x_s$ et $\Phi(G)$ engendre G. Comme $\Phi(G)$ est fini et ses éléments sont superflus d'après (2), on peut les enlever un à un tout en conservant une partie génératrice ; ainsi $x_2, \dots, x_s$ engendre G. Ceci est impossible, car il en découlerait que $e_2, \dots, e_s$ engendrent E, en contradiction avec le fait que $e_1, e_2, \dots, e_s$ est une base. Donc i est injectif, c'est un isomorphisme, donc $G^p[G, G] = \Phi(G)$.

(7) Soit r le rang de G. En choisissant des éléments $x_1, \dots, x_s$ dont les images dans $E = G/\Phi(G)$ forment une base, on voit que $x_1, \dots, x_s$ et $\Phi(G)$ engendrent G. En utilisant le point (2), comme dans (6), on voit que $x_1, \dots, x_s$ engendrent G. Donc $s \geq r$. Maintenant, soit $y_1, \dots, y_r$ un système de générateurs de G, de cardinal minimal égal au rang. Alors les images des y_i engendrent E, donc $r \geq s$. En conclusion $r = s$.