Sous-groupes de Frattini

Perrine Jouteur

J'aime bien ce développement, qui est assez original et se recase bien. Je l'ai placé dans les leçons 101, 103, 104, 108 et 151. On pourra le trouver sous une forme un peu diluée dans *Un max de Maths* de Maxime Zavidovique.

1 Contexte et prérequis

Définition 1.1 Soit G un groupe. On note $\mathcal{M}$ l'ensemble (peut-être vide) des sous-groupes maximaux de G. Si $\mathcal{M} \neq \emptyset$, on définit alors le sous-groupe de Frattini de G par

$$\phi(G) := \bigcap_{M \in \mathcal{M}} M.$$

Si $\mathcal{M} = \emptyset$, on convient que $\phi(G) = G$.

Définition 1.2 Soit G un groupe, et $x \in G$. On dit que x est superflu lorsque pour toute partie $A \subset G$, si (A, x) engendre G alors A engendre G.
Pour résumer que A engendre G, on notera $\langle A \rangle = G$.

Notation 1.1 Soit G un groupe et p un entier. On note G^p l'ensemble des puissances p-èmes de G et $D(G)$ le groupe dérivé de G.

On utilisera le résultat suivants dans la suite.

Proposition 1.1 Soit G un p-groupe, et M un sous-groupe maximal de G. Alors M est distingué dans G et d'indice p.

Démonstration
Soit N le normalisateur de M dans G. On fait agir M sur G/M par conjugaison. Par formule des classes, on a

$$|G/M| = \text{ nb d'orbites de taille 1 } + \sum_{x \ | \ |Orb(x)| \rangle 1} |Orb(x)|.$$

Comme G est un p-groupe, p divise $|G/M|$ et p divise aussi $|Orb(x)|$ dès que la taille de l'orbite est strictement plus grande que 1. Donc p divise le nombre d'orbites de taille 1.
Or, pour $x \in G/M$, on a $|Orb(x)| = 1$ ssi $x \in N/M$. Donc p divise $|N/M|$ et donc $N \neq M$, et ainsi $N = G$ par maximalité de M. ∎

2 Le développement

Théorème 2.1
Soit G un p-groupe, avec p premier. Alors $\phi(G)$ est distingué dans G, engendré par les puissances pièmes et les commutateurs.
De plus, le groupe $G/\phi(G)$ est muni d'une structure de $\mathbb{F}_p$-espace vectoriel, dont la dimension est le cardinal des parties génératrices minimales de G.
Enfin, pour tout élément $x \notin \phi(G)$, on peut construire une famille génératrice minimale de G contenant x.

Démonstration
• Étape 1 : on montre que le sous-groupe de Frattini est l'ensemble des éléments superflus de G.
En effet, soit x superflu dans G. Soit M un sous-groupe maximal dans G. Alors $\langle M, x \rangle = M$ ou $\langle M, x \rangle = G$, mais si $\langle M, x \rangle = G$ alors $\langle M \rangle = G$ ce qui est absurde, donc $\langle M, x \rangle = M$ et donc $x \in M$.
Inversement, si $x \in M$ pour tout sous-groupe maximal de G, soit A une partie de G telle que $\langle A, x \rangle = G$.

Si $\langle A\rangle \neq G$, soit M un sous-groupe maximal qui contient $\langle A\rangle$. Alors $x \in M$ donc $\langle A, x\rangle \subset M$ et donc aïe. Ainsi $\langle A\rangle = G$ et donc x est superflu.

• Étape 2 : on montre que $\langle G^p, D(G)\rangle \subset \phi(G)$.
Soit $x \in G^p$. Montrer que $x \in \phi(G)$ revient à montrer que pour tout sous-groupe maximal M, la classe de x modulo M est la classe neutre. Soit M un sous-groupe maximal. D'après la proposition 1, le quotient G/M est un groupe, d'ordre p. Comme x est une puissance de p, $x = y^p$, on a $[x]_M = [y]_M^p = [1]_M$, par théorème de Lagrange. Donc $x \in \phi(G)$.
De même, soit $x \in D(G)$ et M un sous-groupe maximal. Comme G/M est un groupe d'ordre p premier, il est abélien et donc la classe de x modulo M est la classe neutre. Ainsi $x \in \phi(G)$.
D'où l'inclusion recherchée.

• Étape 3 : on montre que $G/\langle G^p, D(G)\rangle$ est un $\mathbb{F}_p$-espace vectoriel, et qu'on a un isomorphisme entre cet espace et $G/\phi(G)$.
Le groupe $\langle G^p, D(G)\rangle$ est distingué dans G car $D(G)$ et $\langle G^p\rangle$ le sont. De plus, comme le groupe dérivé $D(G)$ est inclus dans $\langle G^p, D(G)\rangle$, le quotient $G/\langle G^p, D(G)\rangle$, qu'on note E dans la suite, est abélien. Considérons alors la loi externe suivante

$$\cdot : \begin{array}{ccc} \mathbb{F}_p \times E & \longrightarrow & E \\ (\overline{k}, x) & \longmapsto & x^k \end{array}.$$

Cette loi est bien définie car E est un groupe abélien dont tous les éléments sont d'ordre divisant p. Cela muni E d'une structure de $\mathbb{F}_p$-espace vectoriel, de dimension finie puisque E est fini.

D'autre part, pour tout sous-groupe maximal M de G, le quotient G/M est isomorphe (en tant que groupe) à $\mathbb{F}_p$, et donc par théorème d'isomorphisme, le quotient $G/\phi(G)$ est isomorphe (en tant que groupe) à $\mathbb{F}_p^d$, avec d le nombre de sous-groupe maximaux dans G. Cet isomorphisme de groupes induit une structure de $\mathbb{F}_p$-espace vectoriel sur $G/\phi(G)$, de dimension d. La loi de composition externe est donnée par $\overline{k} \cdot [x]_{\phi(G)} = [x^k]_{\phi(G)}$. On va alors montrer que $G/\phi(G)$ est isomorphe, en tant que $\mathbb{F}_p$-espace vectoriel, à E.

L'inclusion $\langle G^p, D(G)\rangle \subset \phi(G)$ induit un morphisme de groupes $\iota : E \longrightarrow G/\phi(G)$, qui préserve en fait les structures de $\mathbb{F}_p$-espaces vectoriels de part et d'autres. De plus ι est surjective. Montrons qu'elle est injective.
Pour cela, soit $e \in \mathrm{Ker}(\iota)$, et supposons que e soit non nul.
Par théorème de la base incomplète, on peut compléter (e) en une base de E : $(e, e_2, \cdots, e_n)$. Comme ι est surjective, la famille des images $(\iota(e), \iota(e_2), \cdots, \iota(e_n))$ engendre $G/\phi(G)$.
Mais $\iota(e) = 0$ par définition, donc la famille $(\iota(e_2), \cdots, \iota(e_n))$ engendre $G/\phi(G)$. Soient $(g_2, \cdots, g_n)$ des représentants dans G de $(\iota(e_2), \cdots, \iota(e_n))$. La famille $(g_2, \cdots, g_n, \phi(G))$ engendre donc G. Mais on a vu que $\phi(G)$ est l'ensemble des éléments superflus de G, donc en fait $(g_2, \cdots, g_n)$ engendre G.
Ainsi en passant modulo $\langle G^p, D(G)\rangle$, on a que la famille $([g_2], \cdots, [g_n])$ engendre E. Ceci est absurde car une base est une famille génératrice minimale. Donc ι est injective, et réalise un isomorphisme d'espaces vectoriels entre $G/\phi(G)$ et E.

• Étape 4 : on montre le résultat sur la dimension.
Notons r le rang de G, i.e. le nombre minimal d'éléments de G nécessaires pour engendrer G.
On vient de voir que si $(g_1, \cdots, g_s)$ est une famille génératrice de G, alors $s \geqslant d$, où d est la dimension de E. Donc $r \geqslant d$.
Soit à présent $([g_1], \cdots, [g_d])$ une base de $G/\phi(G)$. Ceci signifie que la famille $(g_1, \cdots, g_d, \phi(G))$ engendre G, mais comme $\phi(G)$ est superflu, $(g_1, \cdots, g_d)$ engendre G et donc $d \geqslant r$ par minimalité de r.
Ainsi $r = d$. ■

Autre version pour le développement, plus efficace :

On commence par montrer en lemme que si M est un sous-groupe maximal d'un p-groupe G, alors M est distingué dans G d'indice p.

On en déduit par théorème d'isomorphisme que $G/\phi(G) \simeq (\mathbb{Z}/p\mathbb{Z})^d$, avec d le nombre de sous-groupes maximaux dans G, ce qui munit par transport $G/\phi(G)$ d'une structure de $\mathbb{F}_p$-espace vectoriel de dimension d.

On montre que si $(g_1, \cdots, g_r)$ est une famille génératrice minimales, alors $r = d$. Pour cela, on commence par dire que $r \geq d$ vu que la famille des projections va engendrer $G/\phi(G)$ en tant que groupe donc en tant qu'espace vectoriel. Puis on extrait de cette famille une base (vectorielle) de $G/\phi(G)$. On dit (attention !) que ça signifie que cette famille extraite engendre $G/\phi(G)$ en tant que groupe, puis on remonte à G et on conclut.