Groupes nilpotents

Références : Calais, *Eléments de théorie des groupes* (th. 7.60 page 254) ou Rotman, *An Introduction to the theory of groups* (th. 5.39).

Définition 1 Soit G un groupe. On définit la *suite centrale descendante* de G par récurrence, par $C^1G = G$ et $C^{i+1}G = [G, C^iG]$ (groupe engendré par les commutateurs d'un élément de G et un élément de C^iG). C'est une suite décroissante de sous-groupes distingués de G. (Vérifiez-le.)

On dit que G est *nilpotent* s'il existe n tel que $C^{n+1}G = \{1\}$. Si c'est le cas, le plus petit tel n est appelé la *classe de nilpotence* de G.

Remarque 2 $\star\star\star$ Si G est nilpotent, alors pour un certain n on a $C^nG \neq 1$ et $C^{n+1}G = \{1\}$. Ceci veut dire que C^nG est central, donc le centre de G est non trivial. (On connaît une autre classe de groupes qui ont cette propriété : les p-groupes finis.)

Exercice 3 (1) Montrez qu'un groupe G est nilpotent si et seulement s'il existe une suite de sous-groupes distingués de G,

$$G^1 = G \supset G^2 \supset \cdots \supset G^n \supset G^{n+1} = 1$$

telle que G^i/G^{i+1} est central dans G/G^{i+1} pour tout i (ou encore, de manière équivalente, $[G, G^i] \subset G^{i+1}$).

(2) Montrez que tout sous-groupe et tout quotient d'un groupe nilpotent sont nilpotents.

(3) Montrez que tout produit *fini* de groupes nilpotents est nilpotent.

Exercice 4 Soit p un nombre premier, montrez qu'un p-groupe fini est nilpotent.
(*Indication : utilisez le (1) de l'exercice précédent en construisant une suite*

$$\cdots \supsetneq G_3 \supsetneq G_2 \supsetneq G_1$$

Il est plus simple de construire cette suite à l'envers, c'est pourquoi la numérotation est inversée. Commencez par choisir un sous-groupe $G_1(= G^n)$ avec les propriétés requises, puis $G_2(= G^{n-1})$,...)

D'après les derniers exercices, tout produit fini de p-groupes finis est nilpotent. En fait, tout les groupes finis nilpotents sont comme ça :

Exercice 5 *Tout groupe fini nilpotent G est produit direct de ses sous-groupes de Sylow.*

On note $|G| = (p_1)^{\alpha_1} \dots (p_n)^{\alpha_n}$ l'ordre de G et $Z \subset G$ son centre. Pour tout i on note Z_i le p_i-Sylow de Z (il n'y en a qu'un, car les p_i-Sylow sont conjugués or Z est abélien), et on choisit un p_i-Sylow P_i de G. Montrez successivement que :

(1) $Z_i \subset P_i$.

(2) P_i est distingué dans G.

(3) Pour $i \neq j$, on a $[P_i, P_j] = \{1\}$, c'est-à-dire, P_i et P_j commutent.

(4) Conclure.

Corrigé du dernier exercice au dos. Prière de ne pas le regarder trop vite...

Corrigé du dernier exercice.

(1) Comme G est nilpotent, son centre Z n'est pas réduit à $\{1\}$. Considérons le morphisme de quotient $\pi\colon G \to G/Z$. L'image de P_i par π est un sous-p_i-groupe de G/Z, isomorphe à $P_i/P_i \cap Z_i$ (en effet, il est clair que le noyau de $P_i \hookrightarrow G \to G/Z$ est $P_i \cap Z_i$). Comme $P_i \cap Z_i \subset Z_i$, on a

$$|\pi(P_i)| = |P_i/P_i \cap Z_i| = \frac{|P_i|}{|P_i \cap Z_i|} \geq \frac{|P_i|}{|Z_i|} .$$

Or si on note $(p_i)^{\beta_i}$ l'ordre de Z_i, on a $|G/Z| = (p_1)^{\alpha_1-\beta_1} \dots (p_n)^{\alpha_n-\beta_n}$. Donc $|P_i|/|Z_i| = (p_i)^{\alpha_i-\beta_i}$ est l'ordre d'un p_i-Sylow de G/Z. Un sous-p_i-groupe de G/Z ne peut avoir un ordre strictement plus grand, donc $|P_i/P_i \cap Z_i| = (p_i)^{\alpha_i-\beta_i}$. Ainsi $|P_i \cap Z_i| = (p_i)^{\beta_i} = |Z_i|$, donc $P_i \cap Z_i = Z_i$ puis $Z_i \subset P_i$.

(2) Soit $g \in G$, on doit montrer que $gP_ig^{-1} = P_i$. Or on a là deux p_i-Sylow de G, qui d'après le (1) contiennent Z_i. On considère le morphisme de quotient $\pi\colon G \to G/Z$. Par une récurrence sur l'ordre de G, les images de gP_ig^{-1} et P_i par π, qui sont des p_i-Sylow de G/Z (voir (1)), sont égales. Ceci s'écrit, d'après (1) encore, $P_i/Z_i = gP_ig^{-1}/Z_i$. On en déduit que $P_i = gP_ig^{-1}$.

(3) Soient $a \in P_i$ et $b \in P_j$, utilisant le fait que P_i et P_j sont distingués, on a :

$$aba^{-1}b^{-1} = \underbrace{(\underbrace{aba^{-1}}_{\in P_j})b^{-1}}_{\in P_j} = \underbrace{a(\underbrace{ba^{-1}b^{-1}}_{\in P_i})}_{\in P_i} \in P_i \cap P_j$$

Comme P_i et P_j sont d'ordres premiers entre eux, $P_i \cap P_j = \{1\}$. Donc tous les commutateurs sont triviaux, le sous-groupe de commutateurs engendré est trivial.

(4) Comme les P_i commutent entre eux, pour tout $m \leq n$, l'application suivante

$$\begin{aligned} \varphi_m\colon \quad & P_1 \times P_2 \times \cdots \times P_m \to G \\ & (a_1, a_2, \dots, a_m) \mapsto a_1a_2\dots a_m \end{aligned}$$

est un morphisme de groupes. (Il est utile de considérer tous les φ_m et pas seulement φ_n pour pouvoir faire la récurrence qui va suivre.) Montrons par récurrence sur m que φ_m est injectif. En effet, pour $m = 1$ c'est clair, et pour $m \geq 2$, si $a_1a_2\dots a_m = 1$ alors $a_1a_2\dots a_{m-1} = (a_m)^{-1}$ est dans l'intersection de $P_1 \times P_2 \times \cdots \times P_{m-1}$, vu comme sous-groupe de G par l'hypothèse de récurrence, et de P_m. Ces deux groupes ont des ordres premiers entre eux, donc leur intersection est réduite à $\{1\}$, donc $a_1a_2\dots a_{m-1} = (a_m)^{-1} = 1$. Par l'hypothèse de récurrence on a donc $a_1 = a_2 = \cdots = a_m = 1$, et φ_m est injectif. Pour $m = n$, on a φ_n injectif entre deux groupes de même ordre, c'est un isomorphisme.