Séries normales. Groupes résolubles
Groupes nilpotents.

L'idée centrale de cette séction est d'éssayer d'obtenir de filtrations par des sous-groupes normaux, dans le but de mieux comprendre la structure d'un groupe fini donné.
Nous commençons par une suite de définitions :

<u>Définition</u> Soit G un groupe. Une séquence des sous-groupes $\{G_i\}_{0\le i\le n}$, avec $G_0 = G$, $G_n = 1$ et G_{i+1} sous-groupe normal de G_i $\forall\ i \in \{0, 1, \dots, n-1\}$ est appelée une <u>série normale</u> pour le groupe G.
Le nombre n est appelé la <u>longuer</u> de la série et les groupes quotient $G_i/_{G_{i+1}}$ le i-ème facteur de la série, pour $0 \le i \le n-1$.

<u>Remarque</u> : $G_{n-1}/_{G_n} \simeq G_{n-1}$, car $G_n = 1$.

<u>Notation</u> : Une série normale $\{G_i\}_{0\le i\le n}$ pour G sera notée $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_{n-1} \trianglerighteq G_n = 1$.

<u>Exemple</u> 1) $G = S_4$ une série normale est donnée par : $G = S_4 \trianglerighteq A_4 \trianglerighteq V_4 \trianglerighteq C_2 \trianglerighteq 1$
Ici S_4 et A_4 sont les groupe symétrique, respectiveement alterné sur 4 lettres et $V_4 = \{id, (12)(34), (13)(24), (14)(32)\}$ isomorphe à un groupe de Klein, $C_2 = \{id, (12)(34)\}$ isomorphe à un groupe cyclique d'ordre 2.

2) Pour tout groupe G, on a une série normale $G \trianglerighteq 1$.

3) Pour tout groupe G, avec $H \trianglelefteq G$, on a une série normale $G \trianglerighteq H \trianglerighteq 1$.

<u>Définition</u> On dit que G est un groupe <u>résoluble</u> si G admet une série normale avec les facteurs succesifs de groupes abélien, i.e. G_i/G_{i+1} est abélien, pour tout $0 \leq i \leq n-1$.

<u>Exemple</u> 1) S_4 est un groupe resoluble car

$$S_4/A_4 \,,\ A_4/V_4 \,,\ V_4/C_2 \text{ et } C_2 \text{ sont tous}$$

des groupes abéliens.

2) Tout groupe abélien est résoluble.

<u>Theorème</u> Tout groupe fini, d'ordre une puissance de p, pour p un nombre premier, est résoluble.

<u>Preuve</u> On construit la série normale inductivement. Si G est un p-groupe d'ordre p^m, alors, si $m \leq 2$, G est abélien, donc résoluble. Supposons $m \geq 3$. Alors $Z(G)$, le centre de G est non-trivial. Maintenant $G/Z(G)$ est aussi un p-groupe d'ordre strictement inférieur que G. Donc, par induction, $G/Z(G)$ est résoluble, donc on a une suite normale $G/Z(G) = \overline{G}_0 \trianglerighteq \overline{G}_1 \trianglerighteq \cdots \trianglerighteq \overline{G}_r = 1$ avec $\overline{G}_i/\overline{G_{i+1}}$ des groupes abéliens pour $0 \leq i \leq r-1$.

Soit G_i l'image inverse par la projection canonique $G \twoheadrightarrow G/Z(G)$ de $\overline{G}_i$. Alors, on a

$G_0 = G$, $G_r = Z(G)$ et $G_i/G_{i+1} \simeq \overline{G}_i/\overline{G_{i+1}}$, donc abélien. Ainsi,

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{r-1} \trianglerighteq G_r = Z(G) \trianglerighteq G_{r+1} = 1$$

est une série normale avec les facteurs successifs abélien, donc G est un groupe résoluble $\square$

Il y a une description équivalente d'un groupe résoluble en utilisant des commutateurs et sous-groupes dérivées successifs.

<u>Définition</u> Le <u>$n^{\text{ème}}$ sous-groupe dérivé</u> $G^{(n)}$ de G est défini par récurrence en posant $G^{(0)} = G$ et $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.

On remarque que $G^{(1)}$ est le sous-groupe dérivé de G, que nous avons étudié dans une section précédente. On se rappèle que $G/_{[G,G]}$ est un groupe abélien et que $G/_H$ est un groupe abélien si et seulement si $[G,G] \leq H$.

<u>Proposition</u> G est un groupe résoluble si et seulement si il existe n tel que $G^{(n)} = 1$.

<u>Preuve</u>: Si $G^{(n)} = 1$, alors

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \cdots \trianglerighteq G^{(n-1)} \trianglerighteq G^{(n)} = 1$$

est une série normale de G avec

$$G^{(i)}/_{G^{(i+1)}} = G^{(i)}/_{[G^{(i)}, G^{(i)}]} \text{ groupe abélien},$$

pour tout $0 \leq i \leq n-1$. Donc G est résoluble.

Réciproquement, si G est résoluble, on a une série normale pour G : $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{m-1} \trianglerighteq G_m = 1$ avec $G_i/_{G_{i+1}}$ abélien pour tout $0 \leq i \leq m-1$.

Ceci implique, en particulier, que $[G_i, G_i] \leq G_{i+1}$.

Par induction, on obtient $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [G_i, G_i] \leq G_{i+1}$

Donc $G^{(m)} \leq G_m = 1$, ce qui implique $G^{(m)} = 1$ $\square$

Nous sommes maintenant en mesure de démontrer que A_n n'est pas résoluble pour $n \geq 5$, résultat obtenu pour la première fois par Galois.

<u>Théorème</u> A_n est un groupe simple, pour $n \geq 5$.

<u>Preuve</u> Soit $n \geq 5$ et $K \trianglelefteq A_n$ un sous-groupe normal non-trivial. On démontre que $K = A_n$. En fait, il est suffisant de démontrer que K contient un (et donc tous les) 3-cycle, car les 3-cycles engendrent A_n. En effet (123) et (ijk) sont conjugués dans S_n par une permutation du type $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & \ell & m & \end{pmatrix}$
Si γ est impaire, alors $\gamma \circ (\ell m)$ est paire et conjugue aussi (123) en (ijk). Donc (123) et (ijk) sont conjugues dans A_n (pas seulement dans S_n). Comme K est normal dans A_n, si K contient (123) alors il ~~contient~~ tous les 3 cycles, donc $K = A_n$.
Soit $\alpha \in K \setminus \{e\}$ une permutation avec nombre maximal de points fixes. On démontre que α est un 3-cycle. Sinon elle est de la forme:
i) $\alpha = (123 \cdots) \cdots$ ou ii) $\alpha = (12)(34) \cdots$
Comme $\alpha \neq (123k)$, qui est une permutation impaire, dans le cas i) α bouge au moins encore deux élément, disons 4 et 5. Prenons $\beta = (345) \in A_n$ et démontrons que $\alpha_1 = \beta\alpha\beta^{-1}\alpha^{-1}$ a moins de points fixes que α.
Premièrement, $\beta\alpha\beta^{-1}$ est $(12)(45)\cdots$ dans le cas ii) et $(124\cdots)\cdots$ dans le cas i). Donc $\beta\alpha\beta^{-1} \neq \alpha$, ce qui

implique que $\alpha_1 \neq 1$. Maintenant, tout nombre >5 est fixé par β, donc, si il est aussi fixé par α, il le sera aussi par α_1. De plus, $\alpha_1(2)=2$ dans le cas i) donc α_1 a plus de points fixes que α car α bougeait $1,2,3,4,5$. Aussi, dans le cas ii) $\alpha_1(1)=1$ et $\alpha_1(2)=2$ et, comme α bougeait au moins $1,2,3,4$ parmi les nombres ≤ 5, de nouveau α_1 a plus de points fixes de α. Ceci est une contadiction avec la supposition que α a un nombre de points fixes maximale parmi les éléments de K. Donc, forcement, α est un 3 cycle et $K = A_n$. Il en suit que A_n est simple pour $n \geq 5$.

<u>Corollaire</u> A_n n'est pas résoluble pour $n \geq 5$.

<u>Preuve</u> $[A_n, A_n]$ est un sous-groupe normal de A_n. Comme A_n est simple $[A_n, A_n]=1$ ou $[A_n, A_n] = A_n$. Comme A_n n'est pas abélien, on a que $[A_n, A_n] \neq 1$. Donc $[A_n, A_n] = A_n$ et $A_n^{(k)} = A_n$ pour tout $k \geq 0$. On en déduit que A_n n'est pas résoluble. □

<u>Théorème</u> Tout sous-groupe et tout groupe quotient d'un groupe résoluble est résoluble. De plus, si nous avons une suite exacte courte $1 \longrightarrow K \longrightarrow G \longrightarrow H \longrightarrow 1$ alors G est résoluble si et seulement si K et H sont résolubles.

<u>Preuve</u> Soit G un groupe résoluble et H un sous-groupe de G. Alors G admet

une série normale $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{n-1} \trianglerighteq G_n = 1$ avec les facteurs succésifs abéliens. Considérons la suite $H_i := G_i \cap H$, $0 \leq i \leq n$. On a clairement $H_0 = G \cap H = H$, $H_n = 1 \cap H = 1$ et $H_{i+1} \trianglelefteq H_i$. De plus

$$H \cap G_i / H \cap G_{i+1} = H \cap G_i / (H \cap G_i) \cap G_{i+1} = (H \cap G_i) G_{i+1} / G_{i+1} \leq G_i / G_{i+1}$$

Donc $H \cap G_i / H \cap G_{i+1}$ est abélien, et H est résoluble.

Une autre preuve, utilisant la caractérization de la résolubilité à l'aide de sous-groupes dérivées, peut se faire en remarquant qu'il existe n tel que $G^{(n)} = 1$. Mais, comme $H^{(k)} \leq G^{(k)}$ $\forall\, k \geq 0$, on a que $H^{(n)} = 1$, donc H est résoluble.

Analoguement, si $K \trianglelefteq G$, alors on construit une série normale pour G/K en prenant $\overline{G_i} := G_i K / K$. De nouveau $\overline{G_i} / \overline{G_{i+1}} \simeq G_i K / G_{i+1} K \simeq G_i G_{i+1} K / G_{i+1} K \simeq$

$$\simeq G_i / G_{i+1} K \cap G_i \simeq \frac{G_i / G_{i+1}}{G_{i+1} K \cap G_i / G_{i+1}}$$

qui est un facteur de groupe abélien, donc abélien. Il s'en suit que G/K est résoluble.

Une autre preuve peut être donnée en remarquant que $[H, H] K / K = [HK/K, HK/K]$ pour tout $H \leq G$. Donc $G^{(i)} K / K = (G/K)^{(i)}$. Donc $G^{(n)} = 1$ implique que $(G/K)^{(n)} = 1 \cdot K / K = 1$ et, ainsi, G/K est résoluble.

Supposons maintenant que $1 \to K \xrightarrow{\iota} G \xrightarrow{\pi} H \to 1$ est une suite exacte courte et que K et H sont des groupes resolubles.

Alors $K = K_0 \trianglerighteq K_1 \trianglerighteq \cdots \trianglerighteq K_{r-1} \trianglerighteq K_r = 1$ et $H = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_s = 1$ sont des séries normales pour H et K avec K_i/K_{i+1} et H_j/H_{j+1} abéliens avec $0 \leq i \leq r-1$, $0 \leq j \leq s-1$. On construit une série normale pour G en prenant l'image inverse dans G pour la série $\{H_j\}$ suivie de la série $\{K_i\}$

$$G_j := \pi^{-1}(H_j) \text{ et } G_{i+s} := K_i \ , \ j \in \{0, \dots, s\}, i \in \{0, \dots, r\}$$

Il est facile a vérifier que la série

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = K \trianglerighteq G_{s+1} \cdots \trianglerighteq G_{r+s} = 1 .$$

est normale pour G et que les facteurs succésifs sont abéliens. Ainsi, on obtient que G est résoluble.

Alternativement, on peut utiliser qu'il existe r et s tels que $H^{(s)} = 1$, $K^{(r)} = 1$. Comme $KG^{(k)}/K = (G/K)^{(k)} = H^{(k)}$, on a que $KG^{(s)}/K = 1$. Donc $G^{(s)} \leq K$. Mais $K^{(r)} = 1$, donc $G^{(r+s)} = (G^{(s)})^{(r)} \leq (K^{(r)}) = 1$. Ceci implique que $G^{(r+s)} = 1$, et, donc, que G est résoluble. □

<u>Corollaire</u> S_n n'est pas résoluble pour $n \geq 5$.

<u>Preuve</u> Si S_n était résoluble alors A_n ~~le~~ serait aussi, car A_n est un sous-groupe de S_n. Mais A_n n'est pas résoluble, donc S_n ne l'est pas non plus □

Nous donnons maintenant encore un critère pour la solvabilité. Pour ceci, nous devrons introduire un nouveau concepte, celui de série de composition. L'avantage de celle-ci est que, contrairement aux séries normales, il y a, essentièlement une unique série de composition pour G. C'est le théorème de Jordan-Hölder qu'on presentera par la suite. On donne, premièrement, la définition d'une série de composition.

<u>Définition</u> Soit $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{n-1} \trianglerighteq G_n = 1$ une série normale pour G. On dit que celle-ci est une <u>série de composition</u> si G_{i+1} est maximal parmi les sous-groupes normaux de G_i, $\forall\, 0 \leq i \leq n-1$

<u>~~Remarque~~</u> Equivalent, on peut demander que tous les facteurs successifs soient des groupes simples, car si $G \geq H \geq K$ et $K \trianglelefteq G$, alors $H \trianglelefteq G$ si et seulement si $H/K \trianglelefteq G/K$.

<u>Théorème</u> (Jordan-Hölder) Soit G un groupe fini et $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1$, et $G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = 1$ deux séries de composition pour G. Alors $m = n$ et il existe une permutation $\sigma \in S_n$ telle que
$G_{i-1}/G_i \simeq H_{\sigma(i)-1}/H_{\sigma(i)}$, $\forall\, 1 \leq i \leq n$.

<u>Preuve</u> On raisonne par induction sur $|G|$. Si $|G| = 1$, le théorème est trivial sinon on distingue deux cas I) $G_1 = H_1$. Alors $|G_1| < |G|$ et $G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n$ et $G_1 = H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_m$ sont des séries de composition pour G_1. Par induction $n-1 = m-1$ et il existe une permutation $\tilde{\sigma}$ de $\{2, \ldots, n\}$ avec $G_{i-1}/G_i \simeq H_{\tilde{\sigma}(i)-1}/H_{\tilde{\sigma}(i)}$. On a donc $n = m$ et on prend $\sigma \in S_n$ définie par $\sigma(1) = 1$ et $\sigma(i) = \tilde{\sigma}(i)$, $2 \leq i \leq n$.

<u>II</u>) $G_1 = H_1$ alors $H_1 G_1 = G$ car $H_1 G_1 \trianglelefteq G$. et $H_1 G_1 \neq G_1$, $H_1 G_1 \neq H_1$, et aussi H_1, G_1 sont des sous-groupes normaux maximaux de G.

Soit $K_2 := H_1 \cap G_1$. On a alors $H_1/_{H_1 \cap G_1} \simeq G/_{G_1}$ et $G_1/_{H_1 \cap G_1} \simeq G/_{H_1}$, qui sont des groupes simples par hypothèse. Soit $K_2 \trianglerighteq K_3 \trianglerighteq \cdots \trianglerighteq K_\ell$ une série de composition de K_2. Alors, on a quatre séries de composition pour G :

(A) $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n$

(B) $G = G_0 \trianglerighteq G_1 \trianglerighteq K_2 \trianglerighteq K_3 \trianglerighteq \cdots \trianglerighteq K_\ell$.

(C) $G = H_0 \trianglerighteq H_1 \trianglerighteq K_2 \trianglerighteq K_3 \trianglerighteq \cdots \trianglerighteq K_\ell$.

(D) $G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m$.

En comparant (A) et (B) on a $n = \ell$; en comparant (C) et (D) on a $m = \ell$ par la première partie de la preuve. De plus, les facteurs sont les mêmes à permutation près. En comparant (B) et (C), les derniers $\ell - 2$ facteurs sont les mêmes et, de plus, $G_0/_{G_1} \simeq H_1/_{K_2}$ et $H_0/_{H_1} \simeq G_1/_{K_2}$. Donc les facteurs sont les mêmes, à transposition des premiers deux facteurs près, entre (B) et (C). On conclut que les facteurs sont les mêmes à permutation près entre (A) et (D) et que $m = \ell = n$. □

<u>Définition</u> : Avec les notations plus haut, n est la <u>longueur de composition</u> pour G et les facteurs successifs sont les <u>facteurs de composition</u> de G

<u>Théorème</u> : Soit G un groupe fini. On a que G est résoluble si et seulement si les facteurs de composition de G sont tous de groupes cycliques.

<u>Preuve</u> : Si les facteurs de compositions sont cycliques, ils sont, en particulier, abéliens, donc

G est un groupe résoluble.

Supposons maintenant que G est résoluble. Alors tout facteur de composition G_i/G_{i+1} de G est résoluble. Comme, de plus G_i/G_{i+1} est simple, on en déduit que G_i/G_{i+1} est abélien, donc cyclique. $\square$

On définit maintenant un type de groupe entre les p-groupes et les groupes résolubles. On a besoin de quelques définitions de plus :

<u>Définition</u> Soit G un groupe

- La série centrale descendante pour G est donnée par $G^0 = G$, $G^{i+1} = [G, G^i]$.
- La série centrale ascendante pour G est donnée par $Z_0^G = 1$, Z_{i+1}^G est l'image inverse du centre $Z(G/Z_{i+1})$ sous la projection canonique.

<u>Remarques</u> 1) $Z_1^G = Z(G)$ est le centre de G.

2) Si G est un groupe fini ces deux séries sont stationnaires pour i assez grand mais, en général G^i ne descend pas jusqu'à 1 et Z_i^G ne monte pas jusqu'à G.

<u>Exemple</u> Soit $G = S_4$

- $G^{(0)} = S_4$, $G^{(1)} = A_4$, $G^{(2)} = V_4$, $G^{(1)} = 1$
- $G^0 = S_4$, $G^1 = A_4$, $G^2 = A_4$
- $Z_0^G = 1$, $Z_1^G = 1$

$G = A_4$
- $G_0^{(0)} = A_4$, $G^{(1)} = V_4$, $G^{(2)} = 1$
- $G^0 = A_4$, $G^1 = V_4$, $G^2 = V_4$
- $Z_0^G = 1$, $Z_1^G = 1$.

<u>Définition</u> On dit que G est un groupe <u>nilpotent</u> s'il existe n, tel que $G^n = 1$. Autrement dit, si la suite centrale descendante pour G "descend" jusqu'au groupe trivial. Le plus petit n pour lequel $G^n = 1$ est appelé la <u>classe de nilpotence</u> de G.

La notion de nilpotence peut aussi être définie en utilisant la suite centrale ascendante.

<u>Théorème</u>

G est nilpotent si et seulement si $Z_m(G) = G$ pour un $m \geq 0$. De plus, si la classe de nilpotence de G est n, alors n est le plus petit entier tel que $Z_n(G) = G$.

<u>Preuve</u>

Supposons que G est nilpotent de classe n. Alors $G^n = 1$ et G^{n-1} est un sous-groupe non-trivial de G. On va montrer par induction sur r que $G^{n-r} \subseteq Z_r^G$, pour tout $r \in \{0, 1, \dots, n\}$.
Pour $r = 0$ on a $G^n = 1$ et $Z_0^G = 1$, donc $G^n \subseteq Z_0^G$.
Supposons maintenant que $G^{n-r} \subseteq Z_r^G$. On a que

(1) $G^{n-r-1}/G^{n-r} \subseteq Z\left(G/G^{n-r}\right)$, car $G^{n-r} = [G^{n-r-1}, G]$ donc il contient tous les commutateurs de G avec G^{n-r-1}!
Ainsi, à G^{n-r} près, G et G^{n-r-1} commutent, d'où (1).
Comme, par hypothèse, $Z_r^G \supseteq G^{n-r}$ il en résulte que, à Z_r^G près, $G^{n-r-1}Z_r^G$ commute avec G.
Donc $G^{n-r-1}Z_r^G / Z_r^G \subseteq Z\left(G/Z_r^G\right)$ ce qui implique que $G^{n-r-1} \subseteq Z_{r+1}^G$. Pour $r=0$ on obtient

$G = G^0 \subseteq Z^G_{n-0}$. Donc $Z^G_n = G$

Réciproquement, supposons que $Z^G_m = G$.
On démontre par induction que $G^r \subseteq Z^G_{m-r}$.
Pour $r=0$ on a $G^0 = G$, $Z^G_m = G$, donc $G^0 \subseteq Z^G_m$.
Supposons $G^r \subseteq Z^G_{m-r}$. Comme $G^{r+1} = [G, G^r]$ on a que $G^{r+1} \subseteq [G, Z^G_{m-r}]^{(2)}$. De plus, comme $Z^G_{m-r}/Z^G_{m-r-1} = Z(G/Z^G_{m-r-1})$, on a que $Z^G_{m-r-1} \supseteq [G, Z^G_{m-r}]^{(3)}$. Par (2) et (3) on obtient $G^{r+1} \subseteq Z^G_{m-r-1}$. Donc $G^r \subseteq Z_{m-r}$ pour tout r. En particulier, pour $r=m$, on a $G^m \subseteq Z_0 = 1$. Donc $G^m = 1$. En particulier si G est de classe n, n est le plus petit nombre tel que $Z^G_m = G$ car $G^m \neq 1$ pour tout $m < n$ □

On conclut la section par quelques propriétés des groupes nilpotents.

<u>Théorème</u>

(i) Sous-groupes et groupes quotient des groupes nilpotents sont nilpotents
(ii) Le produit direct des groupes nilpotents est un groupe nilpotent
(iii) Tout p-groupe fini est nilpotent

<u>Preuve</u>

(i) Si H est un sous-groupe de G, alors $H^i \leq G^i$. Donc $G^n = 1$ implique $H^n = 1$. Si $K \trianglelefteq G$ alors $Z^G_i/K \leq Z^{G/K}_i$. Donc $Z^G_n = G$ implique $Z^{G/K}_n = G$.
Donc ~~H~~ H est nilpotent, alors H et G/K le sont aussi.

ii) on a clairement that $Z_i^{G\times H} = Z_i^G \times Z_i^H$.
Soit n tel que $Z_n^G = G$ et $Z_n^H = H$ (il existe car G et H sont supposés nilpotents). Donc $Z_n^{G\times H} = G\times H$, ce qui implique que $G\times H$ est nilpotent

iii) Tout p-groupe fini a la propriété que son centre est non-trivial. Cette propriété implique que la série Z_i^G a la propriété que Z_i^G est un sous-groupe propre de Z_{i+1}^G si $Z_i^G \neq G$. Donc il existe n tel que $Z_n^G = G$. □

<u>Théorème</u> Si G est un groupe nilpotent et $H \leq G$ est un sous-groupe propre de G, alors H est un sous-groupe propre de $N_G(H)$, le normalizateur de H dans G.

<u>Preuve</u> Soit i le plus grand entier tel que $Z_i^G \leq H$. Comme H est un sous-groupe propre de G, on a $i < n$, où n est la classe de nilpotence de G. Donc on a que Z_i^G est un sous-groupe propre de Z_{i+1}^G. Comme dans la preuve d'un des théorèmes précédants, on a $[G, Z_{i+1}^G] \leq Z_i^G$, donc $[G, Z_{i+1}^G] \subseteq H$.
En particulier, $[H, Z_{i+1}^G] \subseteq H$, donc H est un sous-groupe normal de HZ_{i+1}^G. Donc $HZ_{i+1}^G \leq N_G(H)$ et, comme H ne contient pas Z_{i+1}^G on a que $N_G(H) \setminus H \neq \emptyset$. Donc H est un sous-groupe propre de $N_G(H)$. □

<u>Théorème</u> : Soit G un groupe fini. Alors G est nilpotent si et seulement si il est le produit direct de ses sous-groupes de Sylow.

<u>Preuve</u> : Si G est le produit direct de ses sous-groupes de Sylow alors il est nilpotent car tout p-groupe est nilpotent et le produit direct des groupes nilpotents est nilpotent.

Réciproquement, soit G un groupe nilpotent et $H := N_G(P)$ le normalizateur d'un p-sous-groupe de Sylow P de G. On démontre que $N_G(P) = G$, donc que P est normal dans G et, a fortiori, l'unique p-sous-groupe de Sylow de G. Supposons que $N_G(P) \neq G$. Alors, le théorème précédant implique que $N_G(P)$ est un sous-groupe propre de $N_G(H)$. Mais $N_G(H)$ envoye un p-sous-groupe de Sylow de H sur un p-sous-groupe de Sylow de H. Comme $Syl_p(H) = \{P\}$, on en déduit que $N_G(H) \leq H$. Ceci est une contradiction. Donc tous les sous-groupes de Sylow de G sont normaux dans G. Maintenant $G = P_1 \cdot P_2 \cdot \cdots \cdot P_r$ où $\{P_i\}_{1 \leq i \leq r}$ est l'ensemble des sous groupes de Sylow de G. On a $P_1 \trianglelefteq G$ $P_2 \cdot P_3 \cdot \cdots \cdot P_r \trianglelefteq G$, donc $G \simeq P_1 \times (P_2 \cdot P_3 \cdots P_r)$ car $P_1 \cap (P_2 \cdot P_3 \cdot \cdots \cdot P_r) = \{1\}$. Par induction, on obtient $G \simeq P_1 \times P_2 \times \cdots \times P_r$. $\square$