Sous-groupes de Sylow

Table des matières

D'après le Théorème de Lagrange, l'ordre d'un groupe est divisible par l'ordre de n'importe lequel de ses sous-groupes.
Etant donné un diviseur d de l'ordre d'un groupe G, G possède t'il un sous-groupe d'ordre d ?

1 p-groupes, p-sous-groupes de Sylow

Définition *Soit p un nombre premier.*
On appelle p-groupe, tout groupe d'ordre une puissance non nulle de p.

Exemple $\mathbb{Z}/8\mathbb{Z}$ *est un 2-groupe.*

Proposition 1.0.1 *Le centre d'un p-groupe n'est pas réduit à l'élément neutre.*

Démonstration *On considère l'opération de conjugaison de G sur lui-même.*
On note par cl(g), la classe de conjugaison de g, élément de G.
Si il n'y pas de classe de conjugaison de cardinal strictement supérieur à 1 alors tous les éléments de G sont dans le centre de G (cf cours Conjugaison*).*
D'où, $|Z(G)| = |G|$*>1 et donc Z(G) n'est pas réduit à l'élément neutre.*
On suppose donc qu'il existe des classes de conjugaison non réduites à un élément.
D'après la Formule des classes, $|G| = |Z(G)| + \sum \frac{|G|}{|G_{g_i}|}$ *où la somme est prise sur une famille* $\{g_1, \ldots, g_n\}$ *de représentants des classes de G non réduites à un élément.*
D'après la Formule de Lagrange, $|G_{g_i}|$ *divise* $|G|$ *pour tout i compris entre 1 et n.*
Soit i compris entre 1 et n.
Si $|G_{g_i}|$*=1 alors Card* $cl(g_i) = \frac{|G|}{|G_{g_i}|} = |G|$ *et donc* $cl(g_i)$*=G.*
D'où, l'opération de conjugaison est transitive ce qui est impossible puisque G n'est pas réduit à l'élément neutre (cf cours Conjugaison*).*
Si $|G_{g_i}| = |G|$ *alors Card* $cl(g_i) = \frac{|G|}{|G_{g_i}|}$*=1 ce qui est impossible par choix de* g_i*.*
D'où, pour tout i compris entre 1 et n, il existe un entier a_i *compris entre 1 et n-1 tel que* $\frac{|G|}{|G_{g_i}|} = p^{a_i}$*.*
En considérant la somme $|G| = |Z(G)| + \sum \frac{|G|}{|G_{g_i}|}$ *modulo p (c'est à dire en prenant les classes de ces nombres pour la relation de congruence modulo p), on obtient* $0 = cl(|Z(G)|) + 0$ *donc* $cl(|Z(G)|) = 0$ *c'est à dire p divise* $|Z(G)|$*.*
D'où, Z(G) n'est pas réduit à l'élément neutre. $\diamondsuit$

Corollaire 1.0.2 *Tout groupe d'ordre* p^2*, où p est un nombre premier, est abélien.*

Démonstration *D'après le Théorème de Lagrange et la Proposition précédente, l'ordre de Z(G) est soit p soit* p^2*.*
Si $|Z(G)| = p^2$ *alors Z(G)=G donc G est abélien (cf cours* Conjugaison*).*

Si $|Z(G)|=p$ alors $\frac{|G|}{|Z(G)|}=p$ donc $G/Z(G)$ est cyclique.
D'où, G est abélien (cf cours Conjugaison*).* $\diamondsuit$

Définition *Soit G un groupe d'ordre $p^n s$ où n est un entier strictement positif et s un entier naturel non divisible par p.*
On appelle p-sous-groupe de Sylow de G, tout sous-groupe de G d'ordre p^n.

Exemple *$<3>=\{0, 3, 6, 9\}$ est un 2-groupe de Sylow de $\mathbb{Z}/12\mathbb{Z}$.*

Remarque *Un p-sous-groupe de Sylow est un p-groupe.*

La première question que l'on est amené à se poser est l'existence de p-sous-groupes de Sylow pour un groupe G donné.

2 Premier Théorème de Sylow

Soit G un groupe d'ordre sp^n où n est un entier strictement positif et s un entier naturel non divisible par p.

Lemme *$C_{sp^n}^{p^r} = \lambda p^{n-r}$ où λ est un entier naturel non divisible par p.*

Démonstration *Puisque pour tout couple (a,b) d'entiers strictement positifs, $C_a^b = \frac{a(a-1)...(a-b+1)}{b!}$, on a $C_{sp^n}^{p^r} = \frac{sp^n}{p^r}\frac{sp^n-1}{1}...\frac{sp^n-(p^r-1)}{p^r-1} = sp^{n-r}\frac{sp^n-1}{1}...\frac{sp^n-(p^r-1)}{p^r-1}$.*
Tout entier k compris entre 1 et p^r-1 peut s'écrire sous la forme qp^a avec $0\leq a<r$ et q entier non divisible par p. D'où, $\frac{sp^n-k}{k} = \frac{sp^{n-a}-q}{q}$.
p ne divise pas q donc p ne divise pas $sp^{n-a}-q$.
On en déduit, p étant premier, que p ne divise pas $\lambda = \frac{sp^n-1}{1}...\frac{sp^n-(p^r-1)}{p^r-1}$.
$C_{sp^n}^{p^r} = \lambda p^{n-r}$ avec λ entier naturel non divisible par p. $\diamondsuit$

Théorème 2.0.3 [Premier Théorème de Sylow]
Pour tout entier m compris entre 1 et n, G contient un sous-groupe d'ordre p^m.

Démonstration *On considère l'ensemble F des parties de G à p^r éléments.*
F est de cardinal $C_{sp^n}^{p^r}$ c'est à dire, d'après le Lemme précédent, λp^{n-r} où λ est un entier naturel non divisible par p.
Si A appartient à F et si g appartient à G alors $gA=\{ga \ / \ a\in A\}$ appartient à F (si a et b sont deux éléments distincts de A alors ga est différent de gb) donc G opère sur F par translation à gauche.

Soit $\{A_i,\ 1 \leq i \leq k\}$ une famille de représentants des orbites de F pour cette opération. Par la Formule des classes, on a $\sum_{i=1}^{n} \frac{|G|}{|G_{A_i}|} = Card\ F = \lambda p^{n-r}$.
Si p^{n-r+1} divise $\frac{|G|}{|G_{A_i}|}$ pour tout i compris entre 1 et n alors p^{n-r+1} divise $\sum_{i=1}^{n} \frac{|G|}{|G_{A_i}|}$ c'est à dire λp^{n-r}. On a alors p qui divise λ ce qui est exclu.
Il existe donc au moins un entier i compris entre 1 et k tel que p^{n-r+1} ne divise pas $\frac{|G|}{|G_{A_i}|}$. Posons $P = G_{A_i}$. Nous allons montrer que P est d'ordre p^r.
On a $sp^n = |G| = |P|\frac{|G|}{|G_{A_i}|}$ et p^{n-r+1} ne divise pas $\frac{|G|}{|G_{A_i}|}$ donc $\frac{|G|}{|G_{A_i}|} = s'p^a$ avec $0 \leq a \leq n\text{-}r$ et s' premier avec p.
s' divisant sp^n et s' étant premier avec p, s' divise s par le Lemme de Gauss.
On pose $s'' = \frac{s}{s'}$. On a alors $|P| = s''p^{n-a}$.
Puisque $0 \leq a \leq n\text{-}r$, on a $r \leq n\text{-}a \leq n$ et par conséquent, p^r divise $|P|$. D'où, $|P| \geq p^r$.
Soit a un élément de A_i. La correspondance de P dans A_i définie par $(g \rightarrow ga)$ est une application injective, on en déduit que $|P| \leq Card\ A_i = p^r$.
D'où, P est un sous-groupe d'ordre p^r de G. $\diamondsuit$

En prenant m=n, on obtient :

Corollaire 2.0.4 *Un groupe fini d'ordre divisible par un nombre premier p possède un p-sous-groupe de Sylow.*

3 Second Théorème de Sylow

Soit G un groupe d'ordre sp^n où n est un entier strictement positif et s un entier naturel non divisible par p.

D'après le Premier Théorème de Sylow, on sait que G possède des p-sous-groupes de Sylow. Nous allons maintenant voir comment sont liés les p-sous-groupes de Sylow entre eux et donner des indications sur leur nombre.

Définition *On note $S_p(G)$ l'ensemble des p-sous-groupes de Sylow de G.*

Théorème 3.0.5 [Second Théorème de Sylow]
1)Tout p-sous-groupe de G est inclus dans un p-sous-groupe de Sylow.
2)G opère transitivement par conjugaison sur $S_p(G)$.
3)Si on note $n_p(G)$ le cardinal de $S_p(G)$ alors $n_p(G)$ divise l'ordre de G et est congru à 1 modulo p.

Démonstration *1)Soient H un p-sous-groupe de G et P un p-sous-groupe de Sylow de G. H opère sur l'ensemble quotient $(G/P)_g$ de G par la relation ${}_PR$ (cf cours* Sous-groupes normaux*) par translations à gauche.*
On peut donc décomposer $(G/P)_g$ en orbites pour cette opération.
Le cardinal de chacune des orbites divise l'ordre de H (cf cours Opération*) donc les orbites sont soit de cardinal 1 soit de cardinal une puissance non nulle de p.*
Montrons qu'il existe au moins une orbite de cardinal 1 :
Si toutes les orbites sont de cardinal une puissance non nulle de p alors p divise $\sum_{g_iP\in R}$ Card Ω_i (où R est une famille de représentants des orbites et Ω_i est l'orbite de représentant g_iP) c'est à dire p divise Card $((G/P)_g)$ (puisque les orbites forment une partition de $(G/P)_g$).
Or Card $((G/P)_g)$=$[G:P]$=$|G|/|P|$=s (cf cours Sous-groupes normaux*) n'est pas divisible par p donc il existe au moins une orbite W de cardinal 1.*
Soit gP un représentant de cette orbite ($W\subset(G/P)_g$).
Puisque W est de cardinal 1, on a, pour tout élément h de H, h.gP=hgP=gP.
On en déduit que $g^{-1}hgP$=P ce qui entraîne que g-1hg appartient à P pour tout élément h de H. D'où, pour tout élément h de H, h appartient à gPg^{-1}.
H est donc inclus dans gPg^{-1}. Il est clair que ($x\rightarrow gPg^{-1}$) est une bijection de P dans gPg^{-1} donc $|gPg^{-1}| = |P| = p^n$.
Par conséquent, gPg^{-1} est un p-sous-groupe de Sylow de G.
H est ainsi inclus dans un p-sous-groupe de Sylow de G.
On a montré une propriété plus générale : (P) Etant donné un p-sous-groupe H de G, il existe, pour tout p-sous-groupe de Sylow P de G, un élément g de G tel que H est inclus dans le p-sous-groupe de Sylow gPg^{-1}.
2)Si P est un p-sous-groupe de Sylow de G alors, pour tout élément g de G,
$|gPg^{-1}| = |P| = p^n$ donc gPg^{-1} est aussi un p-sous-groupe de Sylow de G.
G opère donc par conjugaison sur $S_p(G)$.
Montrons que deux p-sous-groupes de Sylow P et Q de G sont toujours conjugués :
Q étant un p-sous-groupe de G, il existe, d'après la Propriété (P), un élément g de G tel que Q est inclus dans gPg^{-1}. Or, $|Q| = |gPg^{-1}| = p^n$ donc Q=gPg^{-1}.
P et Q sont par conséquent conjugués.
G opère transitivement par conjugaison sur $S_p(G)$.
Pour démontrer le troisième résultat, on a besoin d'un lemme intermédiaire :

Lemme *Si P est un p-sous-groupe de Sylow de Sylow de G alors P est l'unique p-sous-groupe de Sylow de $N_G(P)$.*

Démonstration *Puisque $N_G(P)$ est un sous-groupe de G, l'ordre de $N_G(P)$ est de la forme s'p^a avec 0≤aleqn, p ne divisant pas s' et s' divisant s.*
Mais P est un sous-groupe de $N_G(P)$ donc $|P| = p^n$ divise $|N_G(P)|$.
On en déduit que a=n. Ainsi, $|N_G(P)|$=s'p^n avec p ne divisant pas s'.
Puisque $|P| = p^n$, P est un p-sous-groupe de Sylow de $N_G(P)$.
Soit Q un p-sous-groupe de Sylow de $N_G(P)$.
Alors, d'après la partie 2, P et Q sont conjugués dans $N_G(P)$.
Il existe donc un élément x de $N_G(P)$ tel que xPx^{-1}=Q.
x appartenant à $N_G(P)$, on a xPx^{-1}=P et par conséquent P=Q. $\diamondsuit$

3)D'après la partie 2, G opère transitivement par conjugaison sur $S_p(G)$.
On a donc une seule orbite pour cette opération : $S_p(G)$.
D'où, $n_p(G)$=Card $S_p(G)$ divise $|G|$ (cf cours Opération*).*
Soit P un p-sous-groupe de Sylow de G.
Puisque G opère par conjugaison sur $S_p(G)$, P opère aussi par conjugaison sur $S_p(G)$.
$S_p(G)$ se décompose donc en orbites pour cette opération.
Le cardinal de ces orbites divise l'ordre de P donc chacune de ces orbites est soit de cardinal 1 soit de cardinal une puissance non nulle de p.
$\{P\}$ est une orbite de cardinal 1. Montrons que c'est la seule :
Soit Q un p-sous-groupe de Sylowde G tel que l'orbite de Q est $\{Q\}$.
Alors, pour tout élément x de P, $x.Q=xQx^{-1}=Q$.
On en déduit que P est inclus dans le normalisateur de Q dans G.
On a vu dans la démonstration du lemme que $|N_G(Q)|$ est de la forme $s'p^n$ où p ne divise pas s. On en déduit que P et Q sont des p-sous-groupes de Sylow de $N_G(Q)$.
D'où, d'après le lemme, P=Q.
On a donc une orbite de cardinal 1 et toutes les autres de cardinal divisible par p.
Puisque les orbites forment une partition de $S_p(G)$, on a
$n_p(G)$=Card $S_p(G)=1+\sum_{Q\in R}$ Card Ω_Q (où R est une famille de représentants des orbites différentes de $\{P\}$ et Ω_Q est l'orbite de représentant Q).
D'où, $n_p(G)$ est congru à 1 modulo p. $\diamondsuit$

Corollaire 3.0.6 *$n_p(G)$ divise s.*

Démonstration *n_p divise $|G|$ donc n_p est de la forme $s'p^a$ avec $0\leq a\leq n$, p ne divisant pas s' et s' divisant s.*
Si a est différent de 0 alors n_p est congru à 0 modulo p.
Contradiction avec la Propriété 3 du Second Théorème de Sylow.
D'où, a=0 et n_p=s' divise s. $\diamondsuit$

4 Applications

Théorème 4.0.7 (Théorème de Cauchy) *G possède un élément d'ordre p.*

Démonstration *D'après le Premier Théorème de Sylow, G possède un groupe P d'ordre p. p étant premier, P est un groupe cyclique (cf cours Sous-groupes normaux). Tout générateur de P est d'ordre p.* $\diamondsuit$

Remarque *Le Théorème de Cauchy ($\simeq$1825) est antérieur au Premier Théorème de Sylow (1872). En exercice est proposé une preuve directe du Théorème de Cauchy.*

D'après le Théorème de lagrange, les éléments d'un p-groupe sont d'ordre une puissance de p. La réciproque est aussi vraie :

Corollaire 4.0.8 *Si G est un groupe non réduit à* $\{1\}$ *dont tous les éléments différents de 1 sont d'ordre une puissance non nulle d'un nombre premier p alors G est un p-groupe.*

Démonstration *Soit q un diviseur premier de l'ordre de G.*
D'après le Théorème de Cauchy, G possède un élément d'ordre q.
Or tous les éléments de G, différents de 1, sont d'ordre une puissance non nulle de p donc q=p. Le seul diviseur premier de l'ordre de G est p donc G est un p-groupe. $\diamondsuit$

Regardons comment un p-sous-groupe de Sylow passe au sous-groupe et au quotient :

Proposition 4.0.9 *Soient G un groupe fini d'ordre divisible par un nombre premier p, N un sous-groupe normal de G d'ordre divisible par p et P un p-sous-groupe de Sylow de G. Alors,*
1)$P \cap N$ *est un p-sous-groupe de Sylow de N.*
2)PN/N *est un p-sous-groupe de Sylow de* G/N.

Démonstration *Posons* $|G| = sp^n$ *et* $|N| = s'p^m$ *où n et m sont des entiers strictement positifs,* $n \geq m$, *p ne divise pas s et s' divise s.*
1)Soit Q un p-sous-groupe de Sylow de N.
Q est un p-sous-groupe de N donc un p-sous-groupe de G.
D'où, d'après le Second Théorème de Sylow, il existe un p-sous-groupe de Sylow P' de G tel que Q est inclus dans P'.
Mais toujours d'après le Second Théorème de Sylow, il existe un élément g de G tel que $gP'g^{-1} = P$. *Donc,* gQg^{-1} *est inclus dans P.*
N étant normal dans G et Q étant inclus dans N, gQg^{-1} *est inclus dans N.*
D'où, gQg^{-1} *est inclus dans* $P \cap N$.
L'ordre de $P \cap N$ *divise les ordres de P et de N par le Théorème de Lagrange.*
D'où, P étant un p-sous-groupe de G, l'ordre de $P \cap N$ *est de la forme* p^a *avec* $0 \leq a \leq m$.
Puisque $P \cap N$ *contient le p-sous-groupe de Sylow* gQg^{-1}, $|P \cap N| \geq p^n$.
Ainsi, $|P \cap N| = p^n$ *et* $P \cap N$ *est donc un p-sous-groupe de Sylow de N.*
2)Par le Deuxième Théorème d'isomorphisme, PN/N *est isomorphe à* $P/P \cap N$.
D'où, $|PN/N| = |P/P \cap N| = p^{n-m}$ *car* $P \cap N$ *est un p-sous-groupe de Sylow de N.*
Comme $|G/N| = \frac{s}{s'}p^{n-m}$, PN/N *est un p-sous-groupe de Sylow de* G/N. $\diamondsuit$

Enonçons un des résultats les plus utiles découlant du Second Théorème de Sylow :

Proposition 4.0.10 *Soit G un groupe fini d'ordre divisible par un nombre premier p. Soit P un p-sous-groupe de Sylow de G.*
Alors, P est l'unique p-sous-groupe de Sylow de G si et seulement si P est normal dans G.

Démonstration *D'après le Second Théorème de Sylow, G opère transitivement par conjugaison sur $S_p(G)$.*
($\Rightarrow$) Pour tout élément g de G, gPg^{-1} est un p-sous-groupe de Sylow de G donc, par unicité, $gPg^{-1}=P$. P est normal dans G.
($\Leftarrow$) Soit Q un p-sous-groupe de Sylow de G. Il existe un élément g de G tel que $Q=gPg^{-1}$. Or $gPg^{-1}=P$ donc $Q=P$. P est l'unique p-sous-groupe de Sylow de G. $\diamondsuit$

Remarque *En particulier, si G est un groupe abélien fini d'ordre divisible par un nombre premier p alors G ne possède qu'un seul p-sous-groupe de Sylow.*

Cette Proposition est souvent utilisée pour démontrer la simplicité de certains groupes. Par exemple :

Corollaire 4.0.11 *Tout groupe fini d'ordre pq, où p et q sont deux nombres premiers distincts, n'est pas simple.*

Démonstration *Supposons $q<p$ et montrons que $n_p(G)=1$: par le Second Théorème de Sylow et le Corollaire 3.0.6, $n_p(G)$ divise q et est congru à 1 modulo p.*
Mais $1<q<p$ donc q ne peut être congru à 1 modulo p. D'où, $n_p(G)=1$.
G possède un unique p-sous-groupe de Sylow P donc, d'après la Proposition précédente, P est normal dans G.
P étant différent de $\{1\}$ et de G (car $1<p=|P|<pq=|G|$), G n'est pas simple. $\diamondsuit$

Avec des conditions supplémentaires, on a un meilleur résultat :

Proposition 4.0.12 *Soit G un groupe fini d'ordre pq où p et q sont deux nombres premiers distincts. Si p est non congru à 1 modulo q et q non congru à 1 modulo p alors G est cyclique, abélien et isomorphe à $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$.*

Démonstration *D'après le Second Théorème de Sylow et le Corollaire 3.0.6, $n_p(G)$ divise q et est congru à 1 modulo p.*
Comme q n'est pas congru à 1 modulo p, $n_p(G)=1$. De même, $n_q(G)=1$.
D'où, G possède un unique p-sous-groupe de Sylow P et un unique q-sous-groupe de Sylow Q. D'après la Proposition 4.0.10, P et Q sont normaux dans G.
P étant d'ordre p premier, P est cyclique engendré par un élément x (cf cours Sous-groupes normaux*). De même, Q est cyclique engendré par un élément y.*
Montrons que x et y commutent : d'après le Théorème de Lagrange, $|P\cap Q|$ divise $|P|=p$ et $|Q|=q$. Or p et q sont premiers entre eux donc $|P\cap Q|=1$ et $P\cap Q=\{1\}$.
Puisque P et Q sont normaux dans G, $xyx^{-1}y^{-1}$ appartient à $P\cap Q=\{1\}$.
D'où, $xy=yx$ et x et y commutent.
Montrons que xy engendre G : puisque x et y commutent $xy^{pq}=x^{pq}y^{pq}=1$ car x est d'ordre p et y est d'ordre q.

Soit m un entier strictement positif tel que $xy^m=1$.
On a alors $x^m y^m=1$ c'est à dire $x^m=y^{-m}$ et $y^{-m}=x^m$.
D'où, x^m et y^m appartiennent à $P\cap Q=\{1\}$.
On a donc $x^m=1$ ce qui entraîne que p divise m et $y^m=1$ qui implique que q divise m.
Ainsi, ppcm(p,q)=pq divise m.
D'où, xy est d'ordre $pq=|G|$. G est cyclique engendré par xy.
Puisque $|P\cap Q|=1$, on a $|PQ|=|P||Q|=pq=|G|$ (cf cours Produit semi-direct*) donc $G=PQ$.*
D'où, P et Q étant normaux dans G et $P\cap Q$ étant réduit à $\{1\}$, $G=PQ$ est isomorphe à $P\times Q$ (cf cours Produit semi-direct*).*
P étant cyclique d'ordre p, P est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (cf cours Groupes cycliques*).*
De même, Q est isomorphe à $\mathbb{Z}/q\mathbb{Z}$.
D'où, G est isomorphe à $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$. $\diamondsuit$

Remarques *1)Pour montrer que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$, on pouvait aussi utiliser le Théorème chinois (cf Exercice 10 des cours* Congruence, groupes cycliques*) : G étant un groupe cyclique d'ordre pq, G est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$ groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$.*
2)D'après cette Proposition, il n'y a qu'un seul groupe, à isomorphisme près, d'ordre pq où p et q sont deux nombres premiers distincts, p non congru à 1 modulo q et q non congru à 1 modulo p.
Par exemple, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ est le seul groupe, à isomorphisme près, d'ordre 15.

Considérons un cas plus général :

Proposition 4.0.13 *Soit G un groupe fini d'ordre $p_1^{n_1}...p_k^{n_k}$ où p_1, ... , p_k sont des nombres premiers distincts et n_1, ... , n_k des entiers strictement positifs.*
Si, pour tout i compris entre 1 et k, G ne possède qu'un seul p_i-sous-groupe de Sylow P_i alors $G=P_1...P_k$, G est isomorphe au produit direct $P_1\times...\times P_k$.

Démonstration *D'après la Proposition 4.0.10, P_i est normal dans G pour tout i compris entre 1 et k. D'où, l'ensemble $H=P_1...P_k$ est un sous-groupe normal de G (cf cours* Produit semi-direct*).*
Montrons que H est isomorphe à $P_1\times...\times P_k$: il suffit de montrer que $P_i\cap P_{i+1}...P_k$ est réduit à $\{1\}$ quel que soit l'entier i compris entre 1 et k-1 (cf cours Produit semi-direct*). Soit i compris entre 1 et k-1.*
D'après le Théorème de Lagrange, $|P_i\cap P_{i+1}...P_k|$ divise $|P_i|$ et $|P_{i+1}...P_k|$.
Si i=n-1 alors $|P_{i+1}...P_k|=|P_k|$.
Sinon, $|P_{i+1}...P_k|=\frac{|P_{i+1}||P_{i+2}...P_k|}{|P_{i+1}\cap(P_{i+2}...P_k)|}$ (cf cours Produit semi-direct*).*
D'où, quel que soit i compris entre 1 et k-1, $|P_{i+1}...P_k|$ divise $|P_{i+1}|$.
Par conséquent, $|P_i\cap P_{i+1}...P_k|$ divise $|P_i|$ et $|P_{i+1}|$.
Mais p_i et p_{i+1} sont premiers entre eux donc $|P_i\cap P_{i+1}...P_k|=1$ et $P_i\cap P_{i+1}...P_k=\{1\}$.
Ainsi, H est isomorphe à $P_1\times...\times P_k$.
On en déduit que $|H|=|P_1|...|P_k|=p_1{}^{n_1}...p_k{}^{n_k}=|G|$ et donc $G=H=P_1\times...\times P_k$. $\diamondsuit$

Corollaire 4.0.14 *Soit G un groupe abélien fini d'ordre $p_1^{n_1}...p_k^{n_k}$ où p_1, ... , p_k sont des nombres premiers distincts et n_1, ... , n_k des entiers strictement positifs.*
Alors, G est isomorphe au produit direct de ses p_i-sous-groupes de Sylow.

Démonstration *Puisque G est abélien, il ne possède, pour chaque i compris entre 1 et n, qu'un seul p_i-sous-groupe de Sylow. On applique alors la Proposition précédente.*
♢