§6. Théorèmes de Sylow

0. Théorème (Cauchy):

Soit G un groupe abélien fini d'ordre n, et soit p un nombre premier qui divise n. Alors il existe un élément de G d'ordre p.

Preuve:

On fera la preuve par récurrence sur l'entier n.

- Si $n=1$, c'est évident.
- Si $n>1$, on suppose comme H.R. que le résultat est réalisé pour tous les groupes abéliens finis d'ordre $\leq n-1$. On distingue deux cas possibles:

* 1er Cas: G n'est pas simple

Soit alors H un s/g propre de G; si p divise $o(H)$ alors, $1 \leq o(H) \leq n-1$, l'H.R. implique qu'il existe $x \in H$ tel que $o(x)=p$. Si p ne divise pas $o(H)$ alors $pgcd(p, o(H))=1$ donc p divise $o(G/H)$ (car p divise $o(H).o(G/H)$), G/H abélien et $o(G/H) \leq n-1$, l'H.R. appliquée à G/H entraîne qu'il existe $\dot{a} \in G/H$ tel que $o(\dot{a})=p$, donc $(\dot{a})^p = \overline{a^p} = \dot{e}$ (ie) $a^p \in H$ et par suite $(a^p)^{o(H)} = e$, soit $b = [illegible]^{o(H)}$, montrons que $o(b)=p$.

On a $b^p = (a^{o(H)})^p = (a^p)^{o(H)} = e$, et si $k \in \mathbb{N}^*$ tel que $b^k = e$, alors

$(a^{o(H)})^k = a^{k.o(H)} = e$, donc $\dot{a^{k.o(H)}} = \dot{e}$

(i.e) $\dot{a}^{k.o(H)} = \dot{e}$, or $o(\dot{a}) = p$, donc p divise $k.o(H)$ et par suite p divise k, donc

$o(b) = p$.

* 2ème cas: G est simple.

Soit $x \in G - \{e\}$, $\langle x \rangle$ est un s/g de G, distinct de $\{e\}$, G étant simple, donc $G = \langle x \rangle$ (i.e) G cyclique engendré par x; si $k_1 \in \mathbb{N}^*$ avec $n = p.k_1$, soit $y = x^{k_1} \in G$, on a

$$o(y) = o(x^{k_1}) = \frac{o(x)}{pgcd(o(x), k_1)} = \frac{n}{pgcd(n, \frac{n}{p})} = p$$

C.Q.F.D

§ Théorèmes de Sylow.

(Les premières preuves datent de 1872)

1. Théorème :

Soit G un groupe fini d'ordre n et p^k / n, p étant premier et $k \in \mathbb{N}^*$, alors il existe un sous groupe de G d'ordre p^k.

Preuve :

le théorème est trivial si $n = 1$.

On raisonne par récurrence sur n, en supposant le théorème vrai pour tous les groupes d'ordre strictement inférieur à n. On fait opérer G sur lui même par conjugaison ($G \times G \longrightarrow G$, $(g, x) \longrightarrow g \cdot x = gxg^{-1}$). On distingue alors deux cas :

1ère cas :

$\exists\, x \notin Z(G)$ tel que $\text{card}\, \Omega_x \not\equiv 0 \pmod p$, or $\text{card}\, \Omega_x \cdot \text{card}\, C_x = \text{card}\, G$, p^k divise $\text{card}\, \Omega_x \cdot \text{card}\, C_x$ et $pgcd(p^k, \text{card}\, \Omega_x) = 1$, donc p^k divise $\text{card}\, C_x$, mais $x \notin Z(G) \iff \Omega_x = \{ gxg^{-1} / g \in G \} \neq \{x\}$ donc $\text{card}\, C_x < n$, d'après l'H.R. C_x contient un s/g d'ordre p^k et par suite G contient un s/g d'ordre p^k.

2ème cas :

$\forall x \notin Z(G)$, $\text{card}\, \Omega_x \equiv 0 \pmod p$, or on sait que $\text{card}\, Z(G) = n - \sum_{x \in P_1} \text{card}\, \Omega_x \equiv 0 \pmod p$

car $P_1 \cap Z(G) = \emptyset$

d'où $Z(G) \neq \{e\}$, p divise $\text{card}(Z(G))$, d'après le théorème de Cauchy il existe $a \in Z(G)$ d'ordre p, Soit $H = gr(a)$, H st distingué car contenu dans $Z(G)$ et $o(H) = p$; on a $\text{card } G/H \cdot \text{card } H = \text{card } G = n$, p^k/n d'où $p^{k-1}/\text{card}(G/H)$, donc l'H.R. appliquée à G/H, entraine l'existence de K_1 s/g de G/H et $o(K_1) = p^{k-1}$, $\exists K$ s/g de G tel que $H \subseteq K$ et $K_1 = K/H$, $\text{card } K = \text{card } K/H \cdot \text{card } H = p^{k-1} \cdot p = p^k$ d'où K st un s/g de G d'ordre p^k.

C.Q.F.D

2. Définition.

Soit p un nombre premier, on appellera p. groupe tout groupe fini d'ordre une puissance de p.

Un p sous groupe H, d'un groupe fini G, d'ordre p^m est dit un p sous groupe de Sylow si p^m st la plus grande puissance de p divisant l'ordre de G.

3. Corollaire.

G groupe fini, p premier qui divise l'ordre de G, alors a) il existe un p sous groupe de Sylow de G. b) Tout

conjugué d'un p sous groupe de sylow est un p sous groupe de sylow.

4. Théorème.

Si H est un p sous groupe de sylow d'un groupe fini G, alors tout p sous groupe du normalisateur de H est contenu dans H.

Preuve:

Soit K un p sous groupe contenu dans $N(H)$, H etant un sous groupe distingué de $N(H)$ donc HK est un s/g de G et on a $\frac{K}{H\cap K} \simeq \frac{HK}{H}$, donc

$\text{card}\frac{HK}{H}$ est une puissance de p, il en est de même de card (KH), ainsi KH est un p s/g de G, or $H \subseteq KH$ et H un p s/g de sylow, donc $H = KH$ (ie) $K \subseteq H$.

C.Q.F.D

5. Théorème.

Soient G un groupe fini et p un nombre premier divisant l'ordre de G, alors:

1°) Si K est un p s/g de G et H un p s/g de sylow de G, alors il existe $x \in G$ tel que $K \subseteq xHx^{-1}$. Ainsi tout p s/g de G est contenu dans un p s/g de sylow de G.

2°) Les p s/g de Sylow de G sont deux à deux conjugués.

3°) le nombre de p s/g de sylow de G est congru à 1 modulo p (ie) de la forme $1+kp$ avec $k \in \mathbb{N}$.

Preuve : On a $o(G) = m \cdot p^n$ avec $pgcd(p, m) = 1$.

1°) Soit K un p s/g de G et H un p s/g de Sylow de G, on a $[G : H] = m$, d'après (12) (« Groupe opérant sur un ensemble »)
il existe $x \in G$ tel que $K \subseteq xHx^{-1}$.

2°) Si H_1 et H_2 sont deux p s/g de sylow de G, d'après 1°) il existe $x \in G$ tel que $H_1 \subseteq x H_2 x^{-1}$, H_1 et $x H_2 x^{-1}$ sont tous les deux des p s/g de Sylow, donc $H_1 = x H_2 x^{-1}$.

3°) Soit $\mathcal{H}$ l'ensemble des s/g de G, on fait opérer G sur $\mathcal{H}$ par conjugaison (ie)

$$\begin{array}{ccc} G \times \mathcal{H} & \longrightarrow & \mathcal{H} \\ (g, H) & \longmapsto & gHg^{-1} \end{array}$$

Soit H un p s/g de Sylow, l'orbite $\Omega_H = \{gHg^{-1} / g \in G\}$ est l'ensemble de tous les s/g de G conjugués à H (ie) l'ensemble de tous les p s/g de sylow (voir 2°)).

$C_H = \{ g \in G / gH = Hg \} = N(H)$. Soit r le nombre de p s/g de Sylow, on a $r = \text{card}\, \Omega_H = \frac{\text{card}\, G}{\text{card}\, C_H} = \frac{\text{card}\, G_1}{\text{card}(N(H))}$

On fait opérer H sur Ω_H par conjugaison, soit U l'orbite de H sous cette action, on a $U = \{ xHx^{-1} / x \in H \} = \{ H \}$, donc $\text{card}\, U = 1$. Si $Hi \in \Omega_H$ avec $Hi \neq H$, soit $U_i = \{ xHix^{-1} / x \in H \}$ l'orbite de Hi sous la seconde opération, montrons que $\text{card}\, U_i \neq 1$, sinon $U_i = \{ Hi \}$ (ie, $\forall x \in H$: $xHix^{-1} = Hi$, donc $H \subseteq N(Hi)$, d'après le théorème 4, on aura $H \subseteq Hi$, $o(H) = o(Hi) = p^m$ et $H = Hi$, absurde et donc $\text{card}(U_i) \neq 1$;

$r = \text{card}\, \Omega_H = \text{card}\, U + \sum_{Hi \neq H} \text{card}\, U_i$, mais $\forall Hi \neq H$: $\text{card}\, U_i$ divise $\text{card}\, H = p^m$ et $\text{card}\, U_i \neq 1$, donc $\text{card}\, U_i \equiv 0 \pmod p$

Ainsi $r \equiv 1 \pmod p$.

C.Q.F.D.

6. Remarque :

Ω divise $m = [G : H]$, où H est un p s/g de Sylow.