104

Groupes finis. Exemples et applications.

I. Définitions et premières propriétés.

1) Groupe fini et ordre

[ULM] p2 **Déf 1** : L'ordre d'un groupe G, noté $|G|$ est le cardinal de G. On dit que G est fini si $|G|$ est fini

[Combes] p4 **Ex 2** : $\mathbb{Z}/m\mathbb{Z}$ est un groupe fini de cardinal m.

Déf 3 : On appelle ordre d'un élément $g \in G$, l'ordre du sous groupe $\langle g \rangle$ engendré par g.

[ULM] p3 **Ex 4** : $M_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in GL(2,2)$ est d'ordre 2.

[Perrin] p11 **Déf 5** : On appelle exposant de G, le ppcm des ordres des éléments de G si celui-ci est défini.

Ex 6 : Un groupe fini d'exposant 2 est abélien.

[Oral X-ENS] p111 p112 **Thm 7** : (Burnside) Tout sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini est fini DVP

C-ex 8 : $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ est d'exposant fini égal à 2 mais est infini.

2) Théorème de Lagrange. [ULM] p24-25

Déf 9 : Soit G un groupe, H un sous-groupe de G. On appelle indice de H dans G, et on note $(G:H)$ le cardinal de l'ensemble quotient G/H.

Ex 10 : $(\mathbb{Z} : 2\mathbb{Z}) = 2$.

Thm 11 : Soit H sous-groupe de G alors $|G| = |H|\,(G:H)$.

Thm 12 : (Lagrange). Soit G un groupe fini et $H < G$ alors l'ordre de H divise l'ordre de G. En particulier l'ordre d'un élément de G divise toujours l'ordre de G.

[Com] p22 **Appli 13** : K, H deux sous-groupes de G d'ordres k et m. Si $k \wedge m = 1$ alors $K \cap H = \{e\}$.

3) Théorème de factorisation de morphismes. [Com] p24

Prop 14 : Soit G un groupe et $H \lhd G$. Soit j le morphisme canonique de G sur G/H. Soit $f : G \to G'$ un morphisme de groupes. Si $H \subset \mathrm{Ker}(f)$, il existe un unique morphisme $\bar{f} : G/H \to G'$ tel que $\bar{f} \circ j = f$. De plus $\mathrm{Ker}(\bar{f}) = j(\mathrm{Ker}(f))$ et $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$.

Coro 15 : Soient G, G' deux groupes, $f : G \to G'$ un morphisme de groupes. Alors $G/\mathrm{Ker}(f)$ et $f(G)$ sont isomorphes. Si G et G' sont finis, l'ordre de $f(G)$ divise $|G|$ et $|G'|$.

Ex 16 : $\mathbb{Z}/m\mathbb{Z}$ est isomorphe à $\mathbb{U}_m$.

4) Action de groupe.

Déf 17 : Une action de G sur X est une application $\begin{array}{l} G \times X \longrightarrow X \\ (g,x) \longmapsto g.x \end{array}$ [Com] p27

où $g.(h.x) = (gh).x \quad \forall g,h \in G, \forall x \in X$

et $e.x = x, \quad \forall x \in X$.

A une action d'un groupe G sur un ensemble X correspond le morphisme $\begin{array}{l} G \to \mathfrak{S}(X) \\ g \mapsto \sigma_g \end{array}$ où $\sigma_g(x) = g.x$.

Déf 18 : L'orbite de x sous G est $G.x = \{g.x \,/\, g \in G\} \subset X$ [Com] p29

Le stabilisateur de x dans G est $G_x = \{g \in G \,/\, g.x = x\} \subset G$

Rq 19 : $|G| = |G_x|\,|G.x|$.

Coro 20 : G un groupe fini, $G \curvearrowright X$. Si $X = \bigsqcup_{i=1}^{n} X_i$ (partition de X en orbites sous l'action de G) et si $x_i \in X_i$ alors :

$$|X| = \sum_{i=1}^{n} |X_i| = \sum_{i=1}^{n} (G : G_{x_i}) = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|} \quad \text{(formule des classes)}$$ [ULM] p67-69

Coro 21 : (formule de Burnside) Soit $g \in G$, on note $X^g = \{x \in X \,/\, g.x = x\}$. Le nombre n des orbites de X sous l'action de G est

$$n = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Prop 22 : Soit p nombre premier, G un p-groupe et $G \curvearrowright X$ avec $|X|$ fini. Alors $|X^G| \equiv |X| \, [p]$.

[COR] p45

Appli 23 : Théorème de Cauchy : Soit G un groupe fini et p un nombre premier tel que $p \mid |G|$ alors il existe dans G au moins un élément d'ordre p.

Coro 24 : Soit G un groupe fini et p un nombre premier. $|G|$ est une puissance de p ssi l'ordre de tout élément de G est une puissance de p.

[ULM] p12

Ex 25 : Soit G un groupe fini non trivial et p le plus petit nombre premier divisant $|G|$ alors tout sous-groupe H de G d'indice p est distingué.

II) Cas des groupes finis abéliens.

~~Déf~~ 1) Groupes cycliques

Déf 26 : On dit qu'un groupe G est cyclique lorsqu'il est monogène et fini. Tout élément a de G tel que $\langle a \rangle = G$ est appelé un générateur de G.

Ex 27 : $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n et engendré par $\bar{1}$

$\mathbb{U}_n$ est cyclique d'ordre n et engendré par $e^{\frac{2i\pi}{n}}$

Prop 28 : Soit G un groupe cyclique d'ordre n et a un générateur de G alors pour $k \in \mathbb{Z}$ l'ordre de a^k est $\frac{n}{n \wedge k}$

a^k est un générateur ssi $n \wedge k = 1$.

Il existe donc $\varphi(n)$ générateurs distincts dans G.

[COR] p59-62

Ex 29 : Les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont $\bar{1}, \bar{5}, \bar{7}, \overline{11}$

les générateurs de $\mathbb{U}_{18}$ sont $\zeta, \zeta^5, \zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{17}$ avec $\zeta = e^{\frac{2i\pi}{18}}$

Coro 30 : Deux groupes cycliques G et G' sont cycliques ssi ils ont le même ordre.

Coro 31 : Soit G cyclique d'ordre n. Le groupe $\mathrm{Aut}(G)$ est d'ordre $\varphi(n)$ et ses éléments sont les applications

$\alpha_k : x \mapsto x^k$, $k \in [\![0, n-1]\!]$ $k \wedge n = 1$

Prop 32 Soit G cyclique d'ordre n, a un générateur de G. Tout sous-groupe de G est cyclique et pour tout diviseur d de n il existe un unique sous-groupe H_d de G d'ordre d.

Ex 33 : Sous-groupes de $\mathbb{Z}/20\mathbb{Z}$

- Éléments d'ordre 6 dans $\mathbb{U}_{30}$

[COR] p62-65

Déf 34 : G est simple si $\{e\}$ et G sont les seuls sous-groupes distingués de G.

Prop 35 : G est d'ordre premier ssi G est cyclique et simple.

Coro 36 : Si G est d'ordre p^2 alors G est abélien.

[ULM] p64

Coro 37 : Un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

[COR] p63

Prop 38 : G_1 et G_2 sont cycliques d'ordres premiers entre eux ssi $G_1 \times G_2$ est cyclique. Dans ce cas, (a,b) est un générateur de $G_1 \times G_2$ ssi a et b sont des générateurs de G_1 et de G_2.

2) Décomposition en facteurs invariants. [COR] p66-68

Prop 39 Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe des entiers $q_1, q_2, \dots, q_k$ tels que $q_1 \geq 2$ et $q_1 | q_2 | \dots | q_k$ uniques tels que G soit isomorphe à $\mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_k\mathbb{Z}$.

Déf 40 : Cette suite $q_1, \dots, q_k$ est appelée la suite des invariants de G.

Coro 41 : Soit G un groupe abélien d'ordre p^n. Il existe une unique suite $r_1 \leq \dots \leq r_k$ dans $\mathbb{N}^*$ telle que $G \simeq \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_k}\mathbb{Z}$

Coro 42 : Soit G un groupe abélien et $|G| = n = p_1^{k_1} \dots p_r^{k_r}$. Pour tout diviseur d de l'ordre n de G, il existe un sous-groupe de G d'ordre d.

Ex 43 : Décomposition de $G = (\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z})$ en $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/60\mathbb{Z})$

- Structure d'un groupe abélien d'ordre 600.

III) Groupes finis non abéliens

1) Théorème de Sylow, un outil pour l'étude [ULM] p85-88

Déf 44 : Soit p un nombre premier et G un groupe fini. Un p-sous-groupe de G qui est maximal pour l'inclusion des p-sous-groupes de G est appelé un p-Sylow de G.

Thm 45 : Soit p un nombre premier et G un groupe fini $|G| = p^{\alpha} m$ avec $p \nmid m$, alors :

1) Les p-Sylow de G sont les sous groupes d'ordre p^{α} de G
2) Il existe un p-Sylow de G
3) Les p-Sylow sont conjugués et leur nombre $n_p \mid |G|$
4) $n_p \mid m$ et $n_p \equiv 1 [p]$. (DVP)

Prop 46 : Un p-Sylow de G est distingué ssi $n_p = 1$

Appli 47 : Un groupe d'ordre 15 est cyclique, isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

[Com] p53

Appli 48 : Structure d'un groupe fini d'ordre 153.

2) Groupe symétrique. [ULM] p 27 - 53

Déf 49 Soit X un ensemble. Alors l'ensemble $\mathfrak{S}(X)$ des bijections de X dans X, muni de la composition des applications est un groupe appelé groupe symétrique de X d'ordre $|X|!$

à mettre avant Thm Sylow car il sert à le demontrer

Thm 50 : Tout groupe fini G d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$ (Cayley).

Déf 51 : Soit $1 \leq l \in \mathbb{N}$ et $i_1, \dots, i_l$ des éléments de $[\![1, n]\!]$. La permutation $\gamma \in \mathfrak{S}_n$ définie par $\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_l\} \\ i_{k+1} & \text{si } j = i_k, k \neq l \\ i_1 & \text{si } j = i_l \end{cases}$ et notée $(i_1, \dots, i_l)$

est appelée cycle de longueur l. Un cycle de longueur 2 est appelé transposition.

Thm 52 : Tout $\sigma \in \mathfrak{S}_n$ s'écrit comme produit de cycles de longueur ≥ 2 à supports disjoints avec unicité de la décomposition à ordre près.

Déf 53 : Soit $\sigma \in \mathfrak{S}_n$. On appelle signature de $\sigma \in \mathfrak{S}_n$ et on note $\varepsilon(\sigma)$ le nombre $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$

Prop 54 : $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un morphisme de groupe et si $\#(\sigma)$ désigne un nombre de transposition qui apparait dans une décomposition de σ alors $\varepsilon(\sigma) = (-1)^{\#(\sigma)}$

Prop 55 : $\mathfrak{S}_n$ est engendré par les $(1, i)$ avec $i \in [\![2, n]\!]$.

Déf 56 : Le noyau de $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un sous groupe distingué de $\mathfrak{S}_n$, noté A_n et appelé groupe alterné.

Prop 57 : A_n est engendré par les cycles $(1, i, j)$ avec i, j distincts dans $[\![2, n]\!]$. En particulier A_n est engendré par les 3-cycles de $\mathfrak{S}_n$.

3) Groupe diédral. [ULM] p 8-9

Déf 58 : Soit $n \in \mathbb{N}$, $n \geq 3$. Dans le plan complexe $\mathbb{C}$ identifié à $\mathbb{R}^2$ on considère P_n le polygone régulier à n sommets formés par les racines n-ièmes de l'unité $\omega_k = e^{\frac{2ik\pi}{n}}$ ($k \in [\![0, n-1]\!]$). Le groupe diédral D_n est le sous groupe des isométrie du plan affine qui laisse P_n invariant.

Prop 59 : Pour un entier $n \geq 3$, le groupe diédral D_n est d'ordre $2n$ et il est engendré par la symétrie axiale s et la rotation r d'angle $\theta = \frac{2\pi}{n}$ définie par $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $r = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Ces générateurs satisfont aux relations : $r^n = s^2 = e$, $srs = r^{-1}$ et $D_n = \{e, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}$. Le sous groupe $\langle r \rangle < D_n$ est un sous groupe distingué de D_n d'ordre n.

IV) Application à la théorie des représentations [ULM] p 144 - 159

Déf 60 : Soit V un $\mathbb{C}$-ev de dim finie. On appelle représentation linéaire sur $\mathbb{C}$ du groupe G tout morphisme $\rho : G \to GL(V)$, c'est le morphisme structurel de l'action de G sur V.

Déf 61 : Soit $\rho : G \to GL(V)$ une représentation linéaire. Le caractère de ρ est la fonction $\chi_\rho : \begin{array}{l} G \longrightarrow \mathbb{C} \\ g \longmapsto \mathrm{tr}(\rho(g)) \end{array}$. Le degré du caractère $\deg(\chi) = \chi(e)$ est la dimension de V.

Appli 62 : Table de $\mathfrak{S}_4$

Coro 63 : Un groupe fini G est simple ssi tout caractère irréductible non trivial de G a un noyau trivial ie $\{g \in G \mid \chi(g) = \chi(e)\} = e$.

Références:

[ULM] : Félix Ulmer "Théorie des groupes"

[COM] : François Combes "Algèbre et géométrie"

[FGN] : Francinou, Gianella, Nicolas "Oraux X-ENS Alg 2"

Réf. FGN All2
p 171 + 177

Théorème de Burnside

Théorème

Soit G un sous groupe de $GL_n(\mathbb{C})$ d'exposant fini (càd tq $\exists N \in \mathbb{N}^*$ tq $A^N = I$ $\forall A \in G$) alors G est fini.

Démonstration

Étapes 1) Si $A \in M_n(\mathbb{C})$ tq $\operatorname{tr}(A^k) = 0$ $\forall k \in \mathbb{N}^*$ alors A est nilpotente.

2) Soit $G < GL_n(\mathbb{C})$, $(M_i)_{1 \leq i \leq m} \in G^m$ une base de $\operatorname{Vect}(G)$ et

$$f : \begin{array}{l} G \to \mathbb{C}^m \\ A \mapsto (\operatorname{Tr}(AM_i))_{1 \leq i \leq m} \end{array}$$

Alors si $f(A) = f(B)$ alors $AB^{-1} - I$ est nilpotente.

3) Si toutes les matrices de G sont diagonalisables alors f est injective.

4) Conclusion

1) Le polynôme caractéristique de A est scindé sur $\mathbb{C}$. Supposons A non nilpotente. Alors A a des valeurs propres non nulles. Soient $\lambda_1, \dots, \lambda_r$ ces valeurs propres et $m_1, \dots, m_r$ leurs multiplicités respectives. Donc $\forall k \geq 1$, on a :

$$\operatorname{Tr}(A^k) = m_1 \lambda_1^k + \dots + m_r \lambda_r^k = 0.$$

Si on écrit ces relations pour k variant de 1 à r, on obtient que $(m_1, \dots, m_r)$ est solution du système linéaire :

$$V(\lambda_1, \dots, \lambda_r) \left\{ \begin{pmatrix} \lambda_1 & \lambda_2 & \dots & \lambda_r \\ \lambda_1^2 & \lambda_2^2 & \dots & \lambda_r^2 \\ \vdots & & & \vdots \\ \lambda_1^r & \lambda_2^r & \dots & \lambda_r^r \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} \right.$$

Or $\det V(\lambda_1, \dots, \lambda_r) \neq 0$

Lemme $\det V(\lambda_1, \dots, \lambda_r) = \lambda_1 \dots \lambda_r \prod_{1 \leq i < j \leq r} (\lambda_j - \lambda_i)$

Démo Lemme :

$$\begin{vmatrix} \lambda_1 & \lambda_2 & \dots & \lambda_r \\ \lambda_1^2 & \lambda_2^2 & \dots & \lambda_r^2 \\ \vdots & & & \vdots \\ \lambda_1^r & \lambda_2^r & \dots & \lambda_r^r \end{vmatrix} = \lambda_1 \lambda_2 \dots \lambda_r \begin{vmatrix} 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_2 & \dots & \lambda_r \\ \vdots & & & \vdots \\ \lambda_1^{r-1} & \lambda_2^{r-1} & \dots & \lambda_r^{r-1} \end{vmatrix}$$

On pose $P(X) = \begin{vmatrix} 1 & \dots & 1 & 1 \\ \lambda_1 & \lambda_2 \dots & \lambda_{r-1} & X \\ \vdots & & & \vdots \\ \lambda_1^{r-1} & \lambda_2^{r-1} \dots & \lambda_{r-1}^{r-1} & X^{r-1} \end{vmatrix} = \det V(\lambda_1, \dots, \lambda_{r-1}, X)$

P est un polynôme de degré au plus $(n-1)$. De plus le coefficient en X^{n-1} est $\det V(\lambda_1,\dots,\lambda_{n-1})$ et si on substitue λ_i à X on a $P(\lambda_i)=0$. Donc P est divisible par $\prod_{i=1}^{n-1}(X-\lambda_i)$ qui est unitaire de degré $(n-1)$. Ainsi

$$P(X)=V(\lambda_1,\dots,\lambda_{n-1})\prod_{i=1}^{n-1}(X-\lambda_i) \Rightarrow P(\lambda_n)=V(\lambda_1,\dots,\lambda_{n-1})\prod_{i=1}^{n-1}(\lambda_n-\lambda_i)$$

D'où par récurrence

$$\det V(\lambda_1,\dots,\lambda_n)=\prod_{1\leq i<j\leq n}(\lambda_j-\lambda_i)\neq 0.$$

Donc $(m_1,\dots,m_n)=(0,\dots,0)$ contradiction.

Donc A est nilpotente ∎

2) Soit $D=AB^{-1}$. Par linéarité de la trace on a $Tr(AM)=Tr(BM)$ $\forall M\in Vect(G)$ et en particulier $\forall M\in G$. Soit $k\in\mathbb{N}^*$. On a

$$Tr(D^k)=Tr(AB^{-1}D^{k-1}) \quad / M=B^{-1}D^{k-1}$$
$$=Tr(BB^{-1}D^{k-1})$$
$$=Tr(D^{k-1})$$

Donc $\forall k\in\mathbb{N}$, $Tr(D^k)=Tr(I_n)=n$.

Donc $\forall k\geq 1$ $Tr(D-I_n)^k=Tr\left(\sum_{j=0}^{k}C_k^j(-1)^jD^{k-j}\right)=n\sum_{j=0}^{k}\binom{k}{j}(-1)^j=n(1-1)^k=0$

D'où le résultat d'après 1) ∎

3) Si les éléments de G sont diagonalisables, alors $D=AB^{-1}\in G$ donc est diagonalisable. Donc $D-I$ l'est aussi or elle est nilpotente elle est donc nulle. Donc $D=I$ et $A=B \Rightarrow f$ est injective.

4) Toute matrice A de G est annulée par X^N-I qui est scindé à racines simples donc A est diagonalisable $\forall A\in G$.

Ainsi f est injective. De plus l'image de f est incluse dans X^m où X est l'ensemble des traces des éléments de G.

Or X est fini car les vap des éléments de G appartiennent à l'ensemble fini des racines N-ième de l'unité.

Donc G est fini.

Réf. Perrin p78-79 A_8^4, 8

Théorème de Sylow

Théorème. Soit p premier, G groupe fini $|G| = p^\alpha m$ avec $p \wedge m = 1$

Alors
1) Il existe des p-Sylows
2) Si H est un p sous groupe de G, il existe un p-Sylow S avec $H \subset S$
3) Les p Sylows sont tous conjugués
4) Si n_p est le nombre de p-Sylow de G alors $n_p | m$ et $n_p \equiv 1\ [p]$

Démonstration

1) **Lemme 1** Soit G un groupe avec $|G| = p^\alpha m$ $p \nmid m$ et soit H un sous groupe de G. Soit S un p-Sylow de G. Alors $\exists a \in G$ tq $aSa^{-1} \cap H$ soit un p-Sylow de H

Démo du Lemme: G opère sur G/S par translation à gauche et le stabilisateur de aS est aSa^{-1}. Mais H opère lui aussi sur G/S par restriction avec comme stabilisateur de aS : $aSa^{-1} \cap H$. Il reste donc à montrer que l'un des ces groupes est un Sylow de H. Ce sont des p groupes (car S l'est) il suffit donc de prouver que pour un $a \in G$, $|H/_{aSa^{-1}\cap H}|$ soit premier à p

Or $|H/_{aSa^{-1}\cap H}| = |\omega(aS)|$ le cardinal de l'orbite de aS dans G/S sous l'action de H. Or si tous ces nombres étaient divisibles par p il en serait de même de $|G/S|$ qui est la réunion de $\omega(aS)$. Mais ceci contredit le fait que S est un p-Sylow de G ∎

Ce lemme va nous permettre de prouver que G a au moins 1 p-Sylow. En effet $|G| = n$. Donc par Cayley on peut plonger G dans $\mathfrak{S}_n$ puis on plonge $\mathfrak{S}_n$ dans $GL_n(\mathbb{F}_p)$ avec $\sigma \in \mathfrak{S}_n \mapsto u_\sigma$ défini dans la base canonique par $u_\sigma(e_i) = e_{\sigma(i)}$

Ainsi on a réalisé G comme un sous-groupe de $GL_n(\mathbb{F}_p)$ qui possède un p-Sylow donc G aussi par le lemme 1 ∎

Lemme 2 : $GL_n(\mathbb{F}_p)$ possède un p-Sylow : $P = \{A = (a_{ij}) \mid a_{ij} = 0$ si $i > j$, $a_{ii} = 1\}$

$$A = \begin{pmatrix} 1 & * & \cdots & * \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Démo Lemme 2 $\quad |GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$

$$= 1 \times (p^n - 1)\, p(p^{n-1} - 1) \cdots p^{n-1}(p-1)$$

$$= p^{0+1+\cdots+(n-1)} (p^n - 1)(p^{n-1} - 1) \cdots (p-1) = p^{\frac{n(n-1)}{2}} m$$

avec $p \wedge m = 1$

Or $|P| = p \times p^2 \cdots p^{n-1} = p^{\frac{n(n-1)}{2}}$ car les a_{ij} sont qcq pour $i < j$. ■

2) et 3) Si H est un p-sous groupe de G et S un p-Sylow de G, il existe par le Lemme 1, $a \in G$ tq $aSa^{-1} \cap H$ soit un p-Sylow de H. Or H est un p-groupe donc $aSa^{-1} \cap H = H$

Donc $H \subset aSa^{-1}$ qui est un Sylow. Si de plus H est un Sylow par égalité des cardinaux on a $H = aSa^{-1}$ ■

4) Pour montrer ce point, on fait agir G par conjugaison sur l'ensemble X de ses p-Sylow. Soit $S \in X$, S opère lui aussi sur X et on a, comme S est un p-groupe ;

$$|X| \equiv |X^S| \; [p]$$

Il ne reste plus qu'à montrer que l'on a $|X^S| = 1$. Or si $s \in S$, on a $sSs^{-1} = S$ donc $S \in X^S$, on doit donc montrer qu'il n'y a que lui.

Soit $T \in X$ et $T \neq S$ et supposons que

$$\forall s \in S, \quad sTs^{-1} = T. \quad (T \text{ est normalisé par } S)$$

Soit le sous groupe N de G engendré par S et T. On a $S \subset N$ et $T \subset N$ et ce sont des p-Sylow de N. Mais comme S normalise T on a $T \triangleleft N$ donc T est l'unique p-Sylow de $N \Rightarrow S = T$ ↯

Donc $X^S = \{S\} \Rightarrow |X^S| = 1 \Rightarrow |X| \equiv 1 \; [p]$ ■

$|X|$ car G agit sur X par conjugaison et il y a une seule orbite donc $|X| \mid |G|$ or $|X| \wedge p = 1 \Rightarrow |X| \mid m$