Les Théorèmes de Sylow

Arthur Garnier

15 avril 2016

Table des matières

Introduction

Le but de ces notes est d'exposer plusieurs démonstrations différentes des trois théorèmes de Sylow, dont notamment celles de Lang, Wielandt, Rotman et Sylow lui-même. Certaines d'entre elles utilisent le théorème de Cauchy, dont nous donnerons deux démonstrations. Nous étudierons ensuite quelques conséquences de ces résultats, dont l'argument de Frattini, utilisé dans le théorème de Schur-Zassenhaus. On verra aussi que tout groupe dont l'ordre et produit de deux nombres premiers et résoluble. Enfin, nous appliquerons les résultats de Sylow à quelques questions plus concrètes, comme la détermination des sous-groupes distingués de $\mathfrak{A}_4$, ou encore le fait que tout groupe d'ordre 35 est cyclique.

Nous supposons le lecteur familier avec les fondements de Théorie des Groupes, notamment avec la notion d'action de groupes.

Avant toute chose, rappelons la définition d'un sous-groupe de Sylow :

Définition 1. Soient G un groupe fini et p un nombre premier divisant l'ordre de G. Si l'on écrit $|G| = np^k$, avec $p \nmid n$, alors un sous-groupe de G d'ordre p^k est appelé un p-sous-groupe de Sylow de G. De plus, on note $\mathrm{Syl}_p(G)$ l'ensemble des p-sous-groupes de Sylow de G.

Remarque 1. Dans [8], un p-sous-groupe de Sylow de G est par définition un p-sous-groupe maximal de G. Cette approche permet de donner un sens à la notion de sous-groupe de Sylow dans un groupe infini. De plus, nous montrerons, dans la quatrième preuve du premier théorème, que ceci est équivalent à la définition donnée ci-dessus, dans le cas où G est fini.

Dans ce cas, on peut énoncer les théorèmes de Sylow comme suit :

Théorème 0. *Soient G un groupe fini, p un nombre premier divisant l'ordre de G et notons $|G| = np^k$ avec $p \nmid n$. Alors*

1. *G admet un p-sous-groupe de Sylow.*
2. *Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G. De plus, tous les p-sous-groupes de Sylow sont conjugués.*
3. *Le nombre de p-sous-groupes de Sylow de G est congru à 1 modulo p et divise n.*

Première partie
Premier théorème de Sylow

Théorème 1. *Soit G un groupe fini et soit p un nombre premier divisant l'ordre de G. Alors, il existe un p-sous-groupe de Sylow de G.*

1.1 Première démonstration

Voir [6], section 1.6.

Nous aurons besoin du lemme suivant, qui est en fait le théorème de Cauchy dans le cas abélien.

Lemme 1. *Supposons que G soit un groupe abélien d'ordre m et soit p un nombre premier divisant m. Alors, G admet un élément d'ordre p.*

Démonstration. Nous prouvons tout d'abord par récurrence que si G a un exposant n, alors l'ordre de G divise une puissance de n. Soient $b \in G$, avec $b \neq 1$ et $H := \langle b \rangle$ le sous-groupe cyclique engendré par b. Alors, l'ordre de H divise n car $b^n = 1$. Par ailleurs, n est un exposant de G/H. Par hypothèse de récurrence, l'ordre de G/H divise une puissance de n et il en est de même de l'ordre de G, parce que

$$|G| = [G : H]|H|.$$

Supposons ensuite que p divise l'ordre de G. Alors il existe un élément x dans G d'ordre divisible par p. En effet, supposons que tout élément de G ait un ordre premier à p. Alors, G a un exposant n premier à p et d'après ce qui précède, ceci montre que $|G|$ divise une certaine puissance de n, donc p divise cette même puissance, contredisant le fait que n et p soient premiers entre eux. Donc il existe $x \in G$ dont l'ordre est divisible par p. Soit ps l'ordre de x. Alors $x^s \neq 1$ et x^s est clairement d'ordre p, d'où le résultat. □

Pour démontrer le théorème 1, on procède par récurrence sur l'ordre de G. Si l'ordre de G est un nombre premier, notre assertion est évidente. Un groupe fini G étant donné, supposons le théorème démontré pour tous les groupes d'ordre plus petit que celui de G. S'il existe un sous-groupe propre H de G dont l'indice est premier à p, alors un p-sous-groupe de Sylow pour H l'est également pour G, et le résultat en découle par hypothèse de récurrence. Nous pouvons par conséquent supposer que tout sous-groupe propre a un indice divisible par p. Considérons maintenant G opérant sur lui-même par conjugaison. La formule des classes donne

$$|G| = |Z| + \sum [G : G_x],$$

Z étant le centre de G. Le terme $|Z|$ correspond aux orbites à un seul élément, à savoir, aux éléments de Z. La somme de droite s'étend sur toutes les autres orbites, chaque indice

$[G : G_x]$ étant > 1, donc divisible par p. Comme p divise l'ordre de G, il s'ensuit que p divise l'ordre de Z, donc en particulier que G a un centre non trivial.
Soit a un élément d'ordre p dans Z et soit H le groupe cyclique engendré par a. Comme H est contenu dans Z, il est distingué. Soit $f : G \twoheadrightarrow {}^{G}/_{H}$ la projection canonique et supposons que p^k soit la plus grande puissance de p divisant l'ordre de G. Alors, p^{k-1} divise l'ordre de ${}^{G}/_{H}$. Soit K' un p-sous-groupe de Sylow de ${}^{G}/_{H}$, qui existe par hypothèse de récurrence, et posons $K := f^{-1}(K')$. On a $K \supset H$ et f applique K sur K', il existe donc un isomorphisme ${}^{K}/_{H} \simeq K'$. Par conséquent, l'ordre de K est $p^{k-1}p = p^k$. □

1.2 Deuxième démonstration

Voir [4], page 4 et [8], theorem 4.2. On utilisera ici le théorème de Cauchy :

Lemme 2. *Soit p premier divisant l'ordre de G. Alors, G admet un élément d'ordre p.*

Démonstration. On raisonne par récurrence sur l'ordre de G, en remarquant que si $|G|$ est premier, le résultat est alors trivial. D'après le Lemme 1, il suffit de montrer le résultat dans le cas où G n'est pas abélien. Soit $Z = Z(G)$ le centre de G. Si p divise $|Z|$, alors Z contient un élément d'ordre p d'après le cas abélien, et cet élément est aussi d'ordre p dans G. On peut donc supposer que p ne divise pas l'ordre de Z. Comme p divise $|G|$, la formule des classes montre qu'il existe une classe de conjugaison d'un élément non central g dont la taille n'est pas divisible par p. Mais, en vertu du lemme des orbites, cette taille vaut $[G : C_G(g)]$ (où $C_G(g)$ est le centralisateur de g), donc p divise l'ordre de $C_G(g)$, qui est un sous-groupe propre puisque g est non central. Par hypothèse de récurrence, ce sous-groupe contient un élément d'ordre p, d'où le résultat. □

Lemme 3. *Soit H un p-groupe opérant sur un ensemble fini S. Alors, en notant*

$$\mathrm{Fix}_H(S) := \{s \in S \ ; \ h \cdot s = s, \ \forall h \in H\}$$

l'ensemble des points fixes du H-ensemble S, on a

$$|S| \equiv |\mathrm{Fix}_H(S)| \pmod{p}.$$

Démonstration. On utilise la formule des orbites

$$|S| = \sum_i [H : H_{s_i}].$$

Pour chaque point fixe s_i, on a $H_{s_i} := \mathrm{Stab}_H(s_i) = H$. Si s_i n'est pas un point fixe, l'indice $[H : H_{s_i}]$ est divisible par p et le résultat en découle immédiatement. □

Soit p^k la plus grande puissance de p divisant l'ordre de G. Si $k = 0$, il n'y a rien à démontrer. On suppose donc que $k \geq 1$, et alors $p \mid |G|$. On va montrer le résultat plus fort suivant :

$$\text{Pour tout } 0 \leq i \leq k, \text{ il existe un sous-groupe } H \text{ d'ordre } p^i.$$

Plus spécifiquement, si $|H| = p^i$ avec $i < k$, on va montrer qu'il existe $H' \geq H$ tel que $[H' : H] = p$ (et on aura $|H'| = p^{i+1}$). Ainsi, en démarrant avec $H = 1$, on peut répéter ce processus pour obtenir une tour de groupes

$$1 = H_0 \leq H_1 \leq H_2 \leq \cdots$$

avec $|H_i| = p^i$ et après k étapes, on obtient $H_k \in \mathrm{Syl}_p(G)$ et le résultat sera acquis.

On considère donc l'action par translation à gauche de H sur ${}^{G}/_{H}$. Par le Lemme 3, on a

$$\left|{}^{G}/_{H}\right| \equiv \left|\mathrm{Fix}_H\left({}^{G}/_{H}\right)\right| \pmod{p}. \tag{1}$$

Si $x = gH \in {}^{G}/_{H}$, alors on observe que

$$gH \in \mathrm{Fix}_H\left({}^{G}/_{H}\right) \Leftrightarrow \forall h \in H,\ hgH = gH \Leftrightarrow \forall h \in H,\ hg \in gH$$

$$\Leftrightarrow \forall h \in H,\ g^{-1}hg \in H \Leftrightarrow g^{-1}Hg \subset H \Leftrightarrow g^{-1}Hg = H \Leftrightarrow g \in N_G(H),$$

où $N_G(H)$ est le normalisateur de H dans G. On en déduit que

$$\mathrm{Fix}_H\left({}^{G}/_{H}\right) = {}^{N_G(H)}/_{H}$$

et (1) devient

$$[G : H] \equiv [N_G(H) : H] \pmod{p}$$

et comme $H \trianglelefteq N_G(H)$, on a que ${}^{N_G(H)}/_{H}$ est un groupe. De plus, $|H| = p^i$ et $i < k$ donc p divise $[G : H]$ et donc p divise $[N_G(H) : H]$ et le Théorème de Cauchy implique que ${}^{N_G(H)}/_{H}$ admette un sous-groupe d'ordre p. Tous les sous-groupes de ${}^{N_G(H)}/_{H}$ sont de la forme ${}^{H'}/_{H}$ avec $H \leq H' \leq N_G(H)$. Ainsi, un sous-groupe d'ordre p de ${}^{N_G(H)}/_{H}$ est un ${}^{H'}/_{H}$ tel que $[H' : H] = p$ et donc $|H'| = p|H| = p^{i+1}$. □

1.3 Troisième démonstration

Voir [2], section 8 et [3], page 27. On commence par un résultat important de stabilité :

Lemme 4. *Si G admet un p-Sylow et si H est un sous-groupe de G dont l'ordre est divisible par p, alors H admet également un p-Sylow.*

Démonstration. On écrit $|G| = np^k$ et $|H| = mp^l$ avec $p \nmid n$ et $p \nmid m$. Soit $P \in \mathrm{Syl}_p(G)$, ainsi que $X := {}^{G}/_{P}$. On a $|X| = n$ et en particulier, $|X| \not\equiv 0 \pmod{p}$. Il existe alors une orbite sous l'action par translation de H sur X dont la taille n'est pas divisible par p. Soit $\mathcal{O}$ une telle orbite et soit $Q := \mathrm{Stab}_H(x)$, où $x \in \mathcal{O}$. Alors, on a

$$|\mathcal{O}| = \frac{|H|}{|Q|}$$

donc p^l divise $|Q|$. Mais on a, en écrivant $x = gP$,

$$Q = \{h \in H \ ; \ hgP = gP\} = \{h \in H \ ; \ g^{-1}hg \in P\} = gPg^{-1} \cap H$$

donc Q est un p-groupe et donc $|Q| = p^l$, d'où $Q \in \mathrm{Syl}_p(H)$. □

Ensuite, d'après le théorème de Cayley, il existe un monomorphisme

$$G \hookrightarrow GL_r(\mathbb{F}_p),$$

où $r := |G|$ et d'après le Lemme 4, trouver un p-Sylow de $GL_r(\mathbb{F}_p)$ donnera un p-Sylow de G. Considérons le sous-groupe

$$S := \left\{ \begin{pmatrix} 1 & x_1^1 & x_2^1 & \cdots & x_{r-1}^1 \\ 0 & 1 & x_2^2 & \cdots & x_{r-1}^2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & x_{r-1}^{r-1} \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}, \ x_j^i \in \mathbb{F}_p \right\} \leq GL_r(\mathbb{F}_p)$$

Par des arguments élémentaires de combinatoire et d'algèbre linéaire, on obtient

$$|GL_r(\mathbb{F}_p)| = (p^r - 1)(p^r - p) \cdots (p^r - p^{r-1}) = p^{\frac{r(r-1)}{2}}(p^r - 1) \cdots (p - 1),$$

et

$$|S| = p \times p^2 \times \cdots \times p^{r-1} = p^{\sum_{i=0}^{r-1} i} = p^{\frac{r(r-1)}{2}}.$$

Ainsi, par définition, on a $S \in \mathrm{Syl}_p(GL_r(\mathbb{F}_p))$, comme voulu. □

1.4 Quatrième démonstration

Voir [8], theorem 4.14.

Donnons une autre preuve du théorème de Cauchy, due à McKay (voir [7]).

Lemme 5. *Si p est un nombre premier divisant l'ordre de G, alors G admet un élément d'ordre p.*

Démonstration. Il s'agit de montrer qu'il existe un élément non trivial de G dont la $p^{\text{ième}}$ puissance est triviale. L'ensemble

$$E := \{(g) = (g_1, \ldots, g_p) \in G^p \ ; \ g_1 g_2 \cdots g_p = 1\}$$

est stable par la permutation circulaire

$$(g_1, \ldots, g_p) \mapsto (g_2, \ldots, g_p, g_1).$$

On peut donc faire agir le groupe cyclique $\mathbb{Z}/p\mathbb{Z}$ sur E via

$$\overline{m} \cdot (g_1, \ldots, g_p) := (g_{1+m \pmod p}, \ldots, g_{p+m \pmod p}).$$

De plus, E est en bijection avec G^{p-1} puisqu'on peut choisir $p-1$ éléments librement, le dernier devant être l'inverse du produit (ordonné) des $p-1$ premiers éléments. En notant a le nombre d'orbites réduites à un élément et b celui des orbites à p éléments, alors on a

$$a + pb = |E| = |G|^{p-1}.$$

Par suite, p divise a, donc $a > 1$. Il existe donc dans E un p-uplet $(h_1, \ldots, h_p) \neq (1, \ldots, 1)$ tel que

$$(h_1, \ldots, h_p) = (h_2, \ldots, h_1) = \cdots = (h_p, \ldots, h_{p-1})$$

c'est-à-dire que

$$h_1 = h_2 = \cdots = h_p.$$

Finalement,

$$1 = h_1 \cdots h_p = h_1^p,$$

et ceci achève la preuve. □

Remarque 2. En fait, l'égalité

$$a + pb = |E| = |G|^{p-1}$$

montre mieux : si l'on note q le nombre d'éléments d'ordre p, on a $a = 1 + q$ et de l'égalité ci-dessus, on déduit que le nombre d'éléments d'ordre p est congru à -1 modulo p.

En utilisant le même argument que dans la première partie de la première démonstration du second théorème (voir ci-après), on voit que tout p-sous-groupe maximal est un p-sous-groupe de Sylow de G. De plus, si $S \in \mathrm{Syl}_p(G)$ et si Q est un p-groupe, disons $|Q| = p^l$, avec $S \leq Q$, alors $p^k | p^l$ et $k \leq l$ mais $|Q|$ divise $|G|$ donc $p^l | np^k$ et n étant premier à p, on obtient $p^l | p^k$ d'où $l \leq k$ et donc $l = k$. Ceci implique que $S = Q$ et S est donc maximal.

Ainsi, les p-sous-groupes de Sylow sont exactement les p-sous-groupes maximaux de G. Enfin, l'ensemble des p-sous-groupes de G n'est pas vide d'après le Théorème de Cauchy et est fini, donc il admet un élément maximal, qui est alors un p-Sylow. (Notons que l'on peut aussi utiliser le lemme de Zorn, mais ce n'est pas utile ici car l'ensemble est fini). □

1.5 Cinquième démonstration

Voir [12].

Lemme 6. *Si p est un nombre premier et si $a, b \in \mathbb{N}^*$ avec $a \leq b$, alors on a*

$$\binom{pb}{pa} \equiv \binom{b}{a} \pmod p.$$

Démonstration. En effet, dans $\mathbb{F}_p[X]$, on a l'égalité

$$\sum_{k=0}^{pb} \binom{pb}{k} X^k = (1+X)^{pb} = (1+X^p)^b = \sum_{k=0}^{b} \binom{b}{k} X^{pk}$$

et l'égalité des coefficients du monôme X^{pa} donne le résultat. □

Écrivons $|G| = np^k$ et posons

$$\Omega := \{X \subseteq G \ ; \ |X| = p^k\}.$$

G agit sur Ω par translation à gauche. D'après le Lemme 6, on a

$$|\Omega| = \binom{np^k}{p^k} \equiv n \pmod{p}.$$

Ainsi, p ne divise pas $|\Omega|$ et Ω a une orbite $\mathcal{O}$ dont la taille n'est pas divisible par p. Soit $X \in \mathcal{O}$ et soit $H := \mathrm{Stab}_G(X)$. D'après le Lemme des orbites, on a $[G : H] = |\mathcal{O}|$, donc p^k divise $|H|$ et en particulier, on a $p^k \leq |H|$. D'autre part, pour $x \in X$, on a $Hx \subseteq X$, d'où

$$|H| = |Hx| \leq |X| = p^k,$$

et donc H est un p-Sylow de G. □

1.6 Sixième démonstration

Voir [11].

Soit p un nombre premier divisant l'ordre de G. Par le Théorème de Cauchy, il existe un p-sous-groupe maximal P de G. Il s'agit de montrer que

$$[G : P] \not\equiv 0 \pmod{p}.$$

Soit $N := N_G(P)$. Alors, tout élément de N d'ordre une puissance de p est dans P. En effet, un tel élément qui ne serait pas dans P donnerait un élément non trivial d'ordre une puissance de p dans N/P. On pourrait alors considérer la préimage par la projection naturelle $N \to N/P$ pour obtenir un p-sous-groupe H tel que $P \subsetneq H \leq N$ et ceci contredirait la maximalité de P.

Comme il n'existe pas d'élément non trivial d'ordre une puissance de p dans N/P, le Théorème de Cauchy implique que $[N : P] \not\equiv 0 \pmod{p}$.

Maintenant, P agit sur G/N par translation à gauche. Comme $P \subset N$, on a $tN = N$ pour tout $t \in P$, donc N est un point fixe pour cette action ; montrons qu'il est unique. Soit donc gN un point fixe quelconque. Pour tout $t \in P$, on a $tgN = gN$, d'où $g^{-1}tg \in N$ et donc $g^{-1}Pg \subset N$. Puisque $g^{-1}Pg$ est un p-groupe et comme tout élément d'ordre une puissance de p de N est dans P, il vient $g^{-1}Pg \subset P$, donc $g^{-1}Pg = P$ et donc $g \in N_G(P) = N$. Ceci implique que $gN = N$ comme souhaité.

Ainsi, $N \in G/N$ est l'unique point fixe de l'action, donc toute autre orbite de P dans G/N a une taille divisible par p, donc d'après le Lemme 3 il vient $[G : N] \equiv 1 \pmod{p}$. Il s'ensuit que

$$[G : P] = [G : N][N : P] \equiv [N : P] \not\equiv 0 \pmod{p},$$

d'où le résultat. □

Deuxième partie

Second théorème de Sylow

Théorème 2. *Soient G un groupe fini et p un nombre premier divisant l'ordre de G. Alors,*

1. *Tout p-sous-groupe de G est contenu dans un p-Sylow de G.*
2. *Tous les p-Sylow sont conjugués*

2.1 Première démonstration

Voir [6], théorème 1.6.4

1. Soient P un p-Sylow de G et H un p-sous-groupe de G. Supposons d'abord que H soit contenu dans le normalisateur $N_G(P)$ de P. On va montrer que $H \subset P$. En effet, dans ce cas, HP est un sous-groupe du normalisateur et P est distingué dans HP. Or,

$$[HP : P] = [H : H \cap P],$$

si bien que si $HP \neq P$, alors l'ordre de HP est une puissance de p et cet ordre est strictement plus grand que $|P|$, contrairement à l'hypothèse selon laquelle P est un p-sous-groupe de Sylow. Par conséquent, $HP = P$ et $H \subset P$.
Soit maintenant S l'ensemble de tous les conjugués de P dans G et considérons G opérant sur S par conjugaison. Comme le normalisateur de P contient P, et a ainsi un indice premier à p, il s'ensuit que $|S|$ n'est pas divisible par p. Soit H un p-sous-groupe quelconque ; alors H opère aussi sur S par conjugaison. D'après le Lemme 3, on sait que H admet au moins un point fixe. Si Q est un tel point fixe, alors, par définition, H est contenu dans le normalisateur de Q. D'après la première partie de la preuve, cela entraîne $H \subset Q$, ce qui prouve 1.
2. Ceci est une conséquence du point précédent, en prenant pour H un p-sous-groupe de Sylow, de sorte que $|H| = |Q|$, d'où $H = Q$.

□

2.2 Deuxième démonstration

Voir [10], theorem 1.11.6 et [5], theorem 6.3.3.

1. En fait, nous avons déjà justifié ceci dans la seconde démonstration du premier théorème.
2. Nous commençons par un lemme :

Lemme 7. *Soient $H, K \leq G$ et $x \in G$. L'ensemble*

$$HxK := \{hxk,\ h \in H,\ k \in K\},$$

appelé la double classe de x modulo H et K, vérifie

$$|HxK| = \frac{|H||K|}{|H \cap xKx^{-1}|}.$$

Démonstration. Le produit direct $H \times K$ agit sur HxK par

$$(h,k) \cdot y = hyk^{-1},\ y \in HxK.$$

Calculons $\mathrm{Stab}_{H\times K}(x)$. On a

$$(h,k) \in \mathrm{Stab}_{H\times K}(x) \ \Leftrightarrow\ hxk^{-1} = x \ \Leftrightarrow\ h = xkx^{-1}.$$

Ainsi, $\mathrm{Stab}_{H\times K}(x)$ est le sous-groupe formé des $(h,k) \in H \times K$ tels que $h = xkx^{-1}$. Ce sous-groupe a le même ordre que $H \cap xKx^{-1}$. Par le lemme des orbites, comme l'orbite de x est HxK, on obtient

$$|HxK| = \frac{|H \times K|}{|\mathrm{Stab}_{H\times K}(x)|} = \frac{|H||K|}{|H \cap xKx^{-1}|}.$$

□

Maintenant, pour $H, K \in \mathrm{Syl}_p(G)$ et $g \in G$, on a $p^{k+1} \nmid |HgK|$ si et seulement si $|H \cap gKg^{-1}| \geq p^k$, ou bien $H = gKg^{-1}$; c'est-à-dire si et seulement si $H = gKg^{-1}$. Si cette dernière égalité n'arrive jamais, alors toute classe double a un cardinal divisible par p^{k+1} et les doubles classes étant des classes d'équivalence, on en déduit que p^{k+1} divise $|G|$, ce qui n'est pas.

□

Troisième partie

Troisième théorème de Sylow

Théorème 3. *Soient G un groupe fini et p un nombre premier divisant l'ordre de G. En écrivant $|G| = np^k$ avec $p \nmid n$ et $n_p := |\mathrm{Syl}_p(G)|$, on a*

1. *n_p est congru à 1 modulo p.*
2. *n_p divise n.*

3.1 Première démonstration

Voir [6] théorème 1.6.4.

1. On reprend les notations de la première démonstration du second Théorème. Si P et H sont des p-Sylow de G, et si Q est un point fixe sous l'action par conjugaison de H sur l'ensemble S des conjugués de P dans G, alors on a montré que $H = Q$. En particulier, H n'a qu'un seul point fixe. D'après le Lemme 3, on en déduit que

$$|S| \equiv 1 \pmod{p}.$$

   Or, d'après le second Théorème, tous les p-Sylow sont conjugués et donc $S = \mathrm{Syl}_p(G)$, d'où le résultat.

2. Considérons l'action par conjugaison de G sur $\mathrm{Syl}_p(G)$. D'après le second Théorème, cette action est transitive et donc n_p divise $|G|$ par le lemme des orbites. Comme $n_p \equiv 1 \pmod{p}$, n_p est premier à p et donc $n_p | n$.

□

3.2 Deuxième démonstration

Voir [4], page 5.

1. Considérons l'action d'un p-Sylow S sur $\mathrm{Syl}_p(G)$ par conjugaison. D'après le Lemme 3, on a

$$n_p \equiv |\mathrm{Fix}_S(\mathrm{Syl}_p(G))| \pmod{p}.$$

   Les points fixes sont les $T \in \mathrm{Syl}_p(G)$ tel que $gTg^{-1} = T$ pour tout $g \in S$. On observe que S nous fournit un exemple d'un tel T. De plus, pour tout tel T, on a $S \leq N_G(T)$. On a aussi $T \leq N_G(T)$ et donc S et T sont des p-sous-groupes de Sylow de $N_G(T)$. D'après le second Théorème, S et T sont conjugués dans $N_G(T)$. Comme $T \trianglelefteq N_G(T)$, le seul sous-groupe de $N_G(T)$ conjugué à T est T, d'où $S = T$. Ainsi, S est l'unique point fixe et $n_p \equiv 1 \pmod{p}$. (Cet argument est à rapprocher du précédent.)

2. On procède de la même manière que dans la première démonstration.

□

3.3 Troisième démonstration

Voir [10], theorem 1.11.12.

On ne démontre que le premier point, le deuxième s'en déduisant par un argument donné plus haut.

Ici encore, on considère l'action par conjugaison de G sur $\mathrm{Syl}_p(G)$. Le stabilisateur de $S \in \mathrm{Syl}_p(G)$ est le normalisateur $N_G(S)$ et l'orbite de S est $\mathrm{Syl}_p(G)$, en vertu du second Théorème. Si $r := \frac{|N_G(S)|}{p^k}$, il s'agit de montrer que $n \equiv r \pmod{p}$. En effet, si c'est le cas, alors on aura

$$n_p = \frac{|G|}{|N_G(S)|} = \frac{|G|}{rp^k} = \frac{np^k}{rp^k} = \frac{n}{r} \equiv 1 \pmod{p}.$$

On a

$$|SgS| = \frac{p^{2k}}{|S \cap gSg^{-1}|},$$

et ce d'après le Lemme 7. Ainsi, p^{k+1} ne divise pas $|SgS|$ si et seulement si $g \in N_G(S)$. Soit s le nombre de telles doubles classes. Comme la somme des cardinaux des doubles classes égale $|G|$, on doit avoir

$$sp^k \equiv |G| \equiv np^k \pmod{p^{k+1}},$$

ce qui est équivalent à

$$s \equiv n \pmod{p}.$$

Mais $g \in N_G(S)$ si et seulement si $p^{k+1} \nmid |SgS|$, auquel cas on a $|SgS| = p^k$. Ainsi, l'union de toutes les doubles classes vérifiant ceci est égale à $N_G(S)$ et donc $sp^k = rp^k$, ce qui implique que

$$r \equiv s \equiv n \pmod{p}.$$

□

Quatrième partie

Preuve de Wielandt

Nous allons développer ici un peu plus profondément l'argument de la cinquième démonstration, et montrer le résultat suivant, qui implique directement le troisième théorème de Sylow et donc aussi le premier. Nous avons choisi de présenter cette démonstration pour son élégance et son efficacité.

Théorème 4. *Soient G un groupe fini et p un nombre premier tel que p^β divise $|G|$, où $\beta \geq 1$. Si n_p^β désigne le nombre de sous-groupes de G d'ordre p^β, alors on a*

$$n_p^\beta \equiv 1 \pmod{p}.$$

Démonstration. On écrit $|G| = tp^\alpha$ avec $p \nmid t$ et $\beta \leq \alpha$. Soit $\Omega := \{U \subseteq G \ ; \ |U| = p^\beta\}$. On a

$$|\Omega| = \binom{tp^\alpha}{p^\beta}.$$

G agit sur Ω par translation à gauche. Soit Γ une orbite. Si $T \in \Gamma$ et $x \in T$, alors $S := x^{-1}T \in \Gamma$ vérifie $1 \in S$. Si $g \in \mathrm{Stab}_G(S)$, alors $gS = S$ et $g = g \cdot 1 \in S$. Ainsi, $\mathrm{Stab}_G(S) \subseteq S$.

i) Supposons que $\mathrm{Stab}_G(S) = S$, alors $S \leq G$. Par le lemme des orbites, on a

$$|\Gamma| = \frac{|G|}{|\mathrm{Stab}_G(S)|} = \frac{|G|}{|S|} = \frac{tp^\alpha}{p^\beta} = tp^{\alpha-\beta}$$

et Γ est donc l'ensemble des classes à gauche modulo S. Ainsi, un seul élément de Γ est un sous-groupe de G. Réciproquement, si $T \leq G$ est d'ordre p^β, alors $G \cdot T \approx {}^G/_T$ donc $|G \cdot T| = tp^{\alpha-\beta}$. On en déduit qu'une orbite contient un (unique) sous-groupe d'ordre p^β si et seulement si elle est de taille $tp^{\alpha-\beta}$.

ii) Supposons que $\mathrm{Stab}_G(S) \neq S$. Alors $|S| > |\mathrm{Stab}_G(S)|$ et $|\Gamma| > tp^{\alpha-\beta}$. On voit ensuite, par récurrence descendante, que pour tout $1 \leq \beta \leq \alpha$, si $n > tp^{\alpha-\beta}$ et $n | tp^\alpha$, alors $p^{\alpha-\beta+1} | n$. Comme ici $|\Gamma|$ divise $|G| = tp^\alpha$, ceci implique que $p^{\alpha-\beta+1}$ divise $|\Gamma|$. D'après *i)*, aucun élément de Γ n'est un sous-groupe de G.

On déduit de ceci qu'il existe exactement n_p^β orbites dont le stabilisateur est d'ordre p^β et elles sont de taille $tp^{\alpha-\beta}$, tandis que les orbites dont le stabilisateur est d'ordre inférieur à p^β sont de tailles divisibles par $p^{\alpha-\beta+1}$.

Il existe donc un entier k tel que $|\Omega| = n_p^\beta tp^{\alpha-\beta} + kp^{\alpha-\beta+1}$ et on a alors

$$\frac{|\Omega|}{p^{\alpha-\beta}} = n_p^\beta t + kp \equiv n_p^\beta t \pmod{p}.$$

Comme $p \nmid t$, il existe un unique $u \in \{1, \ldots, p-1\}$ tel que $ut \equiv 1 \pmod{p}$, et alors

$$n_p^\beta \equiv \frac{|\Omega| u}{p^{\alpha-\beta}} \equiv \binom{tp^\alpha}{p^\beta} \frac{u}{p^{\alpha-\beta}} \pmod{p}.$$

Finalement, $n_p^\beta \pmod p$ ne dépend que de $|G|$ et de p^β, il ne dépend donc pas du groupe G tel que $|G| = tp^\alpha$. On peut donc déterminer $n_p^\beta \pmod p$ avec

$$G = \mathbb{Z} \big/ tp^\alpha \mathbb{Z}.$$

Or, dans ce cas, G admet un unique sous-groupe de chaque ordre divisant $|G| = tp^\alpha$ et donc

$$n_p^\beta \equiv 1 \pmod p,$$

d'où le résultat. □

On donne enfin la preuve de Wielandt, telle que l'on la trouve dans [13].

Théorème 5. *Si G est un groupe fini, et si p est un nombre premier divisant l'ordre de G, alors on a*

$$|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}.$$

Démonstration. On écrit $|G| = p^a n$ avec $p \nmid n$. Soit

$$\Omega := \{S \subseteq G \ ; \ |S| = p^a\}.$$

On a $|\Omega| = \binom{p^a n}{p^a}$. G agit sur Ω par $g \cdot S = \{gs, \ s \in S\}$. Ω est réunion disjointe des orbites T_i sous action :

$$|\Omega| = \sum_i |T_i|, \ |T_i| = [G : \underbrace{\mathrm{Stab}_G(S_i)}_{=:U_i}],$$

pour $S_i \in T_i$, $S_i \subseteq G$ et $|S_i| = p^a$. On a $U_i \cdot S_i = S_i$ puisque $U_i = \mathrm{Stab}_G(S_i)$. Donc U_i agit sur S_i et

$$S_i = \bigsqcup_{j=1}^{k_i} U_i \cdot g_{i,j} \tag{2}$$

pour certains $g_{i,j} \in G$. Ainsi, $|S_i| = p^a = k_i|U_i|$ et donc $|U_i| = p^{b_i}$ où $b_i \leq a$.

Si $|U_i| < p^a$ alors $|T_i| = \frac{|G|}{|U_i|} \equiv 0 \pmod{pn}$ et on a $|U_i| = p^a \ \Leftrightarrow \ |T_i| = n$, ainsi que

$$|\Omega| = \binom{p^a n}{p^a} \equiv \sum_{|T_i|=n} |T_i| \pmod{pn}.$$

Pour les T_i avec $|T_i| = n$, on a $|U_i| = p^a$ et $S_i = U_i \cdot s_i$ pour $s_i \in G$. En effet, on a $|T_i| = n$ si et seulement si $|U_i| = p^a$ ce qui implique d'après (2) que $p^a = |S_i| = \sum_{j=1}^{k_i} |U_i| = k_i|U_i| = k_i p^a$ d'où $k_i = 1$ et $S_i = U_i s_i$ avec $s_i = g_{i,1}$. Donc $s_i^{-1} S_i = s_i^{-1} U_i s_i =: V_i$ est un sous-groupe de G d'ordre p^a.

Inversement, si $U \in \mathrm{Syl}_p(G)$, alors $T := \{gU, \ g \in G\}$ est une orbite de longueur n car $|T||\mathrm{Stab}_G(U)| = |G|$ et $\mathrm{Stab}_G(U) = U$ car $U \leq G$ et donc $|T|p^a = np^a \ \Rightarrow \ |T| = n$. Deux sous-groupes U_1 et U_2 de G avec $|U_1| = |U_2| = p^a$ donnent deux orbites différentes puisque $gU_1 = U_2$ implique $1 = gu_1$ avec $u_1 \in U_1$ et donc $g = u_1^{-1} \in U_1 \ \Rightarrow \ U_1 = U_2$.

Donc, on a

$$\binom{np^a}{p^a} \equiv \sum_{|T_i|=n} |T_i| \equiv n|\mathrm{Syl}_p(G)| \pmod{pn}.$$

Que vaut $\binom{np^a}{p^a}$ modulo pn ?
On peut évaluer ceci de façon élémentaire ou de façon plus élégante ; n peut tester ce terme pour n'importe quel groupe G et si on arrive à l'évaluer pour un G particulier, ce terme est le même pour tous les autres groupes d'ordre $p^a n$. Soit donc $G = C_{p^a n}$ le groupe cyclique d'ordre np^a. Pour un groupe cyclique d'ordre n, il existe un unique sous-groupe d'ordre k pour tout $k|n$. En fait, si C_m est engendré par c, d'ordre m, alors le groupe engendré par $c^{\frac{m}{k}}$ est d'ordre k, et c'est le seul sous-groupe d'ordre k. En particulier, pour $G = C_{p^a n}$, on a un et un seul sous-groupe d'ordre p^a, d'où $|\mathrm{Syl}_p(C_{p^a n})| = 1$, donc $\binom{np^a}{p^a} \equiv n \pmod{pn}$ et donc

$$|\mathrm{Syl}_p(G)| \equiv \frac{1}{n}\binom{np^a}{p^a} \equiv 1 \pmod{pn} \equiv 1 \pmod{p}.$$

□

Cinquième partie
Applications

5.1 Quelques corollaires

Nous donnons à présent quelques conséquences des résultats précédemments établis. Nous commençons par un résultat de Frattini, utile par exemple dans la démonstration du théorème de Schur-Zassenhaus.

Mais avant toute chose, nous donnons une conséquence immédiate du travail effectué précédemment. Ce résultat est parfois appelé le "quatrième théorème de Sylow" (par exemple dans [4]).

Corollaire 1. *(Quatrième Théorème de Sylow)*
Soient G un groupe fini, p un nombre premier divisant l'ordre de G et S un p-Sylow de G. Alors, on a

$$|\mathrm{Syl}_p(G)| = [G : N_G(S)].$$

Démonstration. En effet, faisons agir G sur $\mathrm{Syl}_p(G)$ par conjugaison. L'action étant transitive d'après le second Théorème, le lemme des orbites montre que

$$|\mathrm{Syl}_p(G)| = \frac{|G|}{|\mathrm{Stab}_G(S)|}.$$

Mais comme

$$\mathrm{Stab}_G(S) = \{g \in G \ ; \ gSg^{-1} = S\} = N_G(S),$$

le résultat est prouvé. □

Corollaire 2. *(Argument de Frattini)*
Soient G un groupe fini, $N \trianglelefteq G$ un sous-groupe distingué et $S \in \mathrm{Syl}_p(N)$ un p-Sylow de N. Alors

$$G = N \cdot N_G(S).$$

Démonstration. Soit $g \in G$. Comme N est distingué, on a $gSg^{-1} \leq N$ donc gSg^{-1} est un p-Sylow de N. Par le second Théorème de Sylow, S et gSg^{-1} sont conjugués dans N et il existe alors $n \in N$ tel que $gSg^{-1} = nSn^{-1}$ et alors $n^{-1}gSg^{-1}n = S$ et donc $n^{-1}g \in N_G(S)$. Ceci montre que $g \in N \cdot N_G(S)$ et le résultat. □

Nous allons maintenant voir qu'un groupe dont l'ordre est produit de deux nombres premiers distincts est résoluble. Cette illustration provient de [6], lemme 1.6.7 et proposition 1.6.8.

Lemme 8. *Soient G un groupe fini et p le plus petit diviseur premier de l'ordre de G. Si H est un sous-groupe d'indice p, alors H est distingué.*
En particulier, si G est d'ordre pair et si H est un sous-groupe d'indice 2, alors $H \trianglelefteq G$.

Démonstration. Notons $N := N_G(H)$ le normalisateur de H. On a alors $N = H$ ou $N = G$. Si $N = G$, il n'y a rien à démontrer et on peut supposer que $N = H$. Dans ce cas, l'orbite de H sous l'action par conjugaison possède $p = [G : H]$ éléments et la restriction de l'action de G sur cette orbite donne un homomorphisme $G \to \mathfrak{S}_p$. Soit K le noyau de ce morphisme. Alors, K est l'intersection des stabilisateurs. Le stabilisateur de H étant H par hypothèse, il s'ensuit que $K \subset H$.
On a que $[G : K]$ divise $p!$ et comme p est premier, seule sa première puissance divise $p!$. Si $H \neq K$, il existe un nombre premier q divisant $[H : K]$. De la formule

$$[G : K] = [G : H][H : K] = p[H : K],$$

on déduit que q divise $\frac{[G:K]}{p}$, donc divise $(p-1)!$ et on obtient alors l'inégalité $q < p$. Or, q divise l'ordre de G et comme $q < p$, ceci est absurde et donc $H = K \trianglelefteq G$. □

Corollaire 3. *Soient p, q deux nombres premiers distincts et G un groupe d'ordre pq. Alors G est résoluble.*

Démonstration. Supposons $p < q$ et soit Q un q-sous-groupe de Sylow de G. L'indice de Q est p, donc le Lemme 8 montre que Q est distingué et le groupe quotient est d'ordre p. Mais un groupe d'ordre premier est cyclique (donc abélien), d'où le résultat. □

Corollaire 4. *Soient p, q deux nombres premiers distincts et G un groupe d'ordre p^2q. Alors, G admet un p-Sylow ou un q-Sylow distingué.*
En particulier, G n'est pas simple.

Démonstration. Soient $n_p := |\mathrm{Syl}_p(G)|$ et $n_q := |\mathrm{Syl}_q(G)|$. Il s'agit de montrer que $n_p = 1$ ou $n_q = 1$. Par l'absurde supposons que $n_p, n_q > 1$. Comme n_p divise q (troisième Théorème) et comme q est premier, on a $n_p = q$. De la congruence fournie par le troisième Théorème

$$q = n_p \equiv 1 \pmod{p},$$

on obtient $p \leq q - 1$, donc $q > p$. D'autre part, n_q divise p^2, donc $n_q \in \{p, p^2\}$. $n_q = p$ est exclus car $n_q \equiv 1 \pmod{q}$ et $q > p$. Ainsi, $n_q = p^2$. Soient $S_1, S_2, \ldots, S_{p^2}$ les q-sous-groupes de Sylow de G. Un élément d'ordre q est un élément non trivial dans un des S_i, qui s'intersectent trivialement puisqu'ils sont d'ordre premier : $S_i \cap S_j = 1$, $\forall i \neq j$. Il vient alors

$$\{g \in G \ ; \ o(g) = q\} = \bigsqcup_{i=1}^{p^2} (S_i \setminus \{1\}),$$

ce qui montre que

$$|\{g \in G \ ; \ o(g) = q\}| = \sum_{i=1}^{p^2} |S_i \setminus \{1\}| = p^2(q-1).$$

Il y a donc $|G| - p^2(q-1) = p^2$ éléments dans $G \setminus \{g \in G \ ; \ o(g) = q\} = \{g \in G \ ; \ o(g) \neq q\}$. Soit S un p-Sylow de G. Alors $S \subseteq \{g \in G \ ; \ o(g) \neq q\}$ et comme ces deux ensembles ont le même cardinal p^2, on obtient

$$S = \{g \in G \ ; \ o(g) \neq q\}.$$

Ainsi, $\{g \in G \ ; \ o(g) \neq q\}$ est le seul p-Sylow de G et $n_p = 1$. Ceci est absurde. □

5.2 Exemples

Nous concluons notre étude par quelques applications "concrètes" plutôt surprenantes ; par exemple, tout groupe d'ordre 35 est cyclique !

Exemple 1. *(Voir [9], Applications of Sylow Theorems, Example 4)*
Un groupe d'ordre 28 ayant un sous-groupe distingué d'ordre 4 est abélien.

En effet, si $n_7 = |\mathrm{Syl}_7(G)|$, alors $n_7 \equiv 1 \pmod 7$ et $n_7|4$, d'après le troisième Théorème de Sylow. Ceci implique que $n_7 = 1$ et l'unique 7-Sylow de G est alors distingué. Si le 2-Sylow est également normal, alors G est isomorphe au produit direct de son 2-Sylow et de son 7-Sylow, et est alors abélien. En effet, dans ce cas, $N_G(T) = N_G(S) = G$, donc S et T se normalisent mutuellement et comme $T \cap S$ est un sous-groupe de S et de T, on en déduit que $T \cap S = 1$. Ceci implique que l'application

$$\begin{array}{rccc} f & : & T \times S & \to & G \\ & & (t,s) & \mapsto & ts \end{array}$$

est un morphisme de groupes car, si $t, t' \in T$ et $s, s' \in S$, on a $[t', s] = t'st'^{-1}s^{-1} \in T \cap S = 1$, donc $t's = st'$ et $f(tt', ss') = tt'ss' = tst's' = f(t,s)f(t',s')$, comme voulu. De plus, l'égalité $ts = f(t,s) = 1$ implique que $t \in T \cap S = 1$, donc $t = s = 1$ et f est injectif. Enfin, puisque $|T \times S| = 28 = |G|$, f est un isomorphisme, ce qui permet de conclure. □

Exemple 2. Un groupe d'ordre 340 n'est pas simple.

Soit en effet G un tel groupe. On a

$$|G| = 340 = 2^2 \cdot 5 \cdot 17.$$

Si $n_5 = |\mathrm{Syl}_5(G)|$, alors le troisième Théorème montre que n_5 divise $2^2 \cdot 17$ et est congru à 1 modulo 5. Donc $n_5 = 1$, comme on peut le voir en examinant chaque entier possible $n_5 \leq 2^2 \cdot 17 = 68$. □

Exemple 3. Un groupe G d'ordre 48 n'est pas simple.

En effet, on écrit

$$|G| = 48 = 2^4 \cdot 3.$$

D'après le troisième Théorème, $n_2 \equiv 1 \pmod 2$ et $n_2|3$ donc $n_2 \in \{1, 3\}$. Si $n_2 = 1$, le résultat est acquis. Supposons donc que $n_2 = 3$. En faisant agir G par conjugaison sur $\mathrm{Syl}_2(G)$, on obtient un morphisme

$$\varphi : G \to \mathfrak{S}_3.$$

D'après le second Théorème, tous les 2-Sylow sont conjugués, donc l'image de φ ne peut être triviale. Mais, dans ce cas, $\ker\varphi \trianglelefteq G$ et $\operatorname{im}\varphi \simeq {}^{G}/_{\ker\varphi}$ donc $\frac{|G|}{|\ker\varphi|} > 1$ et donc $\ker\varphi \neq G$. De plus, on ne peut avoir $\ker\varphi = 1$ car sinon, $G \simeq \operatorname{im}\varphi \leq \mathfrak{S}_3$ et alors $6 = |\mathfrak{S}_3|$ serait divisible par $|G| = 48$, ce qui serait absurde. $\ker\varphi$ est donc un sous-groupe distingué propre et non trivial. □

Exemple 4. *(Voir [1], page 5)*
Le groupe alterné $\mathfrak{A}_4$ admet un unique sous-groupe distingué propre K_4. Celui-ci est d'ordre 4 et est donné par

$$K_4 := \{id, (12)(34), (13)(24), (14)(23)\} \simeq {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}.$$

K_4 est appelé le groupe de Klein.

Les éléments du groupe alterné $\mathfrak{A}_4$ s'écrivent

$$\mathfrak{A}_4 = \{id, (234), (243), (12)(34), (123), (124), (132), (134), (13)(24), (142), (143), (14)(23)\}.$$

Tout d'abord, montrons que $\mathfrak{A}_4$ n'admet pas de sous-groupe distingué d'ordre 2 ou 6. En fait, il n'existe pas de sous-groupe d'ordre 6 dans $\mathfrak{A}_4$. Supposons en effet que $H \leq \mathfrak{A}_4$ soit un tel sous-groupe. Alors, $H \trianglelefteq \mathfrak{A}_4$ d'après le Lemme 8 puisque H est d'incide 2. De plus, on a

$$\mathfrak{A}_4 / H \simeq {}^{\mathbb{Z}}/_{2\mathbb{Z}},$$

donc, pour tout $\sigma \in \mathfrak{A}_4$, on a $\sigma^2 \in H$. Or, tout 3-cycle $\gamma \in \mathfrak{A}_4$ est un carré car $(\gamma^2)^2 = \gamma$, donc H contient tous les 3-cycles, qui sont en nombre plus grand que 6, et ceci est absurde.

Ensuite, on observe que les seuls éléments d'ordre 2 de $\mathfrak{A}_4$ sont les éléments non triviaux de K_4. Or, on a

$$\begin{cases} (123)(12)(34)(213) = (14)(23), \\ (123)(13)(24)(213) = (12)(34), \\ (123)(14)(23)(213) = (13)(24). \end{cases}$$

Ainsi, aucun sous-groupe d'ordre 2 n'est distingué.

D'autre part, on a

$$|\mathfrak{A}_4| = 12 = 2^2 \cdot 3.$$

Pour $S \in \mathrm{Syl}_3(G)$, $|S| = 3$ donc S est cyclique. Il y a 8 éléments d'ordre 3 dans $\mathfrak{A}_4$ qui s'arrangent par paires d'inverses, et il y a donc quatre 3-Sylow et aucun d'entre eux n'est distingué d'après le second Théorème.

Donc, d'après le Corollaire 4, il existe un unique 4-Sylow qui est distingué. Il s'agit donc de K_4. On conclut en remarquant qu'un sous-groupe de $\mathfrak{A}_4$ est d'ordre 1, 2, 3, 4, 6 ou 12. □

Exemple 5. *(Voir [6], Section 1.6)*
Tout groupe d'ordre 35 et cyclique.

On a $n_7 \equiv 1 \pmod 7$ et $n_7 | 5$ donc $n_7 = 1$ et soit H_7 l'unique 7-Sylow (distingué) de G. Soit aussi H_5 un 5-Sylow de G, d'ordre 5 donc. Alors H_5 opère par conjugaison sur H_7, donnant un homomorphisme

$$H_5 \to \mathrm{Aut}\,(H_7).$$

Étant donné que $\mathrm{Aut}\,(H_7) \simeq \mathrm{Aut}\left({}^{\mathbb{Z}}/_{7\mathbb{Z}}\right)$ est cyclique d'ordre 6, l'homorphisme précédent est trivial, de sorte que tout élément de H_5 commute avec les éléments de H_7. Si $H_5 = \langle x \rangle$ et $H_7 = \langle y \rangle$, alors x et y commutent entre eux, donc xy est d'ordre $7 \cdot 5 = 35$ et donc $G = \langle xy \rangle$, comme souhaité. □

Le même argument permet de montrer que tout groupe d'ordre 15 est également cyclique.

Références

[1] R. A. Bailey, *Sylow's Theorem*, Queen Mary University of London, 2006.

[2] Oleg Bogopolski, Introduction to Group Theory, EMS, 2002.

[3] Peter J. Cameron, *Notes on finite group theory*, 2013.

[4] Keith Conrad, *The Sylow Theorems*.

[5] Cyril F. Gardiner, A first course in group theory, Springer-Verlag, 1980.

[6] Serge Lang, Algèbre, Dunod, 2004.

[7] James H. McKay, *Another proof of Cauchy's Group Theorem*, Seattle University, 1959.

[8] Joseph J. Rotman, An introduction to the Theory of Groups, Springer-Verlag, New-York, 1995.

[9] Tara L. Smith, *The Sylow Theorems and Applications*.

[10] Victor P. Snaith, Groups, Rings and Galois Theory, World Scientific Publishing, 1998.

[11] Ludwig Sylow, *Théorèmes sur les groupes de substitutions*, Math. Ann, 1872.

[12] Helmut Wielandt, *Ein Beweis für die Existenz der Sylowgruppen*, Arch. Math., 1959.

[13] Alexander Zimmermann, *Algèbre Générale - Théorie des Groupes*, Cours de Licence 3, Université de Picardie Jules Verne, France, 2014.