Thm de Lagrange :

Si $H \leq G$ alors $|H| \mid |G|$.

Q : Soit m un diviseur de $|G|$.

existe-t-il un $H \leq G$ t.q. $|H| = m$.

R : D'une manière générale non.

Mais : si $m = p^k$, p premier

oui.

Ce que nous allons démontrer :

Soit p^k une puissance maximale de p divisant $|G|$.

alors $\exists\ H \leq G$ t.q. $|H| = p^k$.

(et bien plus)

[p t.q. premier]

2 possibilités : 1. travailler dans $\mathbb{Z}[X]$ modulo p.
2. travailler directement dans $\mathbb{F}_p[X]$
où $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$

Chapitre VI

Théorèmes de Sylow

1. Un exercice préliminaire de combinatoire

Avant de parler des Théorème de Sylow, faisons un petit calcul. Considérons $\mathbf{Z}[X]$, l'ensemble des polynômes à coefficients entiers en l'inconnu X. La somme et le produit de deux polynômes dans $\mathbf{Z}[X]$ appartient encore à $\mathbf{Z}[X]$ (au fait, $(\mathbf{Z}[X], +, \cdot)$ est un anneau, voir la Définition I.5.1).

Si $P, Q \in \mathbf{Z}[X]$, on dit que P est Q cont **congru modulo** p, en symboles $P \equiv Q \mod p$, si $P - Q$ est divisible par p. Autrement dit, s'il existe $R \in \mathbf{Z}[X]$ tel que $P - Q = pR$. Dans la suite, nous allons omettre le mod p et noter la congruence modulo p par le symbole $\equiv$ seul.

Lemme VI.1.1. *La relation de congruence modulo p est une relation d'équivalence. Si $P_i \equiv Q_i$ pour $i = 1, 2$ alors*

$$P_1 + P_2 \equiv Q_1 + Q_2 \qquad \text{et} \qquad P_1 P_2 \equiv Q_1 Q_2.$$

$X + pX^2 = X$

Démonstration. Montrons que c'est une relation d'équivalence :
— Réflexive : $P - P = p \cdot 0$.
— Symétrique : si $P - Q = pR$, alors $Q - P = p(-R)$.
— Transitive : si $P - Q = pR$ et $Q - S = pT$ alors $P - S = p(R + T)$.
Pour la deuxième affirmation, on suppose que $P_i - Q_i = pR_i$ pour $i = 1, 2$. Alors :

$$(P_1 + P_2) - (Q_1 + Q_2) = p(R_1 + R_2)$$

et

$-Q_1P_2 + Q_1P_2$

$$(P_1 P_2) - (Q_1 Q_2) = (P_1 - Q_1)P_2 + Q_1(P_2 - Q_2) = p(R_1 P_2 + Q_1 R_2).$$

■

Lemme VI.1.2. *Soit $P, Q \in \mathbf{Z}[X]$. Alors pour tout $n \in \mathbf{N}$:*

$$(P + Q)^{p^n} \equiv P^{p^n} + Q^{p^n}.$$

mod p p premier

Démonstration. Montrons ça d'abord pour $n = 1$. Si $0 < k < p$, alors $p \mid \binom{p}{k}$. En effet, p divise le numérateur de $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ mais non le dénominateur (et p est premier). Par conséquent :

$$(P+Q)^p - P^p - Q^p = \sum_{0 \leq k \leq p} \binom{p}{k} P^k Q^{p-k} - P^p - Q^p = \sum_{0<k<p} \binom{p}{k} P^k Q^{p-k}$$

est divisible par p. Maintenant, on prouve par récurrence sur n. Pour $n = 0$ il n'y a rien à démontrer, puisque $p^n = 1$. À l'étape n on sait déjà que

$$(P+Q)^{p^n} \equiv P^{p^n} + Q^{p^n}.$$

D'où, d'après Lemme VI.1.1 :

$$(P+Q)^{p^{n+1}} = \left((P+Q)^{p^n}\right)^p \equiv \left(P^{p^n} + Q^{p^n}\right)^p \equiv P^{p^{n+1}} + Q^{p^{n+1}}. \qquad \blacksquare$$

En particulier, avec $m, n \in \mathbf{N}$ quelconques :

$$(1+X)^{mp^n} = \left((1+X)^{p^n}\right)^m \equiv (1+X^{p^n})^m.$$

À gauche, le coefficient de X^{p^n} est $\binom{mp^n}{p^n}$, et à droite m, d'où :

$$\boxed{\binom{mp^n}{p^n} \equiv m \mod p.}$$

Pour un argument plus calculatoire démontrant le même énoncé, voir l'Exercice VI.1.

2. Les trois théorèmes de Sylow

Soit G un groupe fini, p premier, et $k \in \mathbf{N}$. Sous quelles conditions existe-t-il un sous-groupe $H \leq G$ tel que $|H| = p^k$? D'après Lagrange, on a une condition nécessaire : il faut que $p^k \mid |G|$. Nous allons montrer que c'est aussi une condition suffisante. Concentrons-nous d'abord sur le cas où k est maximal.

Définition VI.2.1. Soit G un groupe fini et p premier. Soit p^n la puissance maximale de p qui divise $|G|$. Un sous-groupe $H \leq G$ d'ordre p^n s'appelle un ***p*-sous-groupe de Sylow** de G, ou simplement un ***p*-Sylow** de G.

$$X = \{ S \subseteq G \ : \ |S| = p^n \}$$

$S \in X$, $g \in G \Rightarrow gS = \{gh : h \in S\}$.

$h \mapsto gh$ est bijective
$G \to G$

$\Rightarrow |gS| = |S| = p^n \Rightarrow gS \in X$

$eS = S$, $g_1(g_2 S) = (g_1 g_2) S$

$\Rightarrow$ c'est une action $G \curvearrowright X$

Fixons quelques conventions. Nous gardons l'hypothèse que G est un groupe fini et p un nombre premier. Nous fixons le n maximal tel que $p^n \mid |G|$, et $m = |G|/p^n$. Ainsi :

$$|G| = mp^n, \qquad p \nmid m.$$

Avant d'énoncer et de démontrer les trois théorème de Sylow, démontons un lemme. Posons $|G| = mp^n$, où $p \nmid m$, et $X = \{S \subseteq G : |S| = p^n\}$. Si $g \in G$ et $S \in X$, alors $gS = \{gh : h \in S\} \in X$ également. Ceci définit une action $G \curvearrowright X$, que nous proposons d'étudier.

Lemme VI.2.2. *Soit O une orbite de cette action $G \curvearrowright X$, et supposons que $p \nmid |O|$. Alors il existe un p-Sylow $H \leq G$ tel que*

$$O = \{gH : g \in G\} = G/H.$$

Démonstration. Si $S \in O$ et $g \in S$, alors $e \in g^{-1}S \in O$. Ainsi nous pouvons choisir $S \in O$ tel que $e \in S$.

Soit $H = G_S$ son stabilisateur. Si $h \in H$ alors $h = he \in hS = S$, donc $H \subseteq S$. En particulier $|H| \leq p^n$. Par contre,

$$|O||H| = [G : H]|H| = |G| = mp^n.$$

Puisque $p \nmid |O|$, forcément $p^n \mid |H|$. Il en suit que $|H| = p^n$, c'est donc un p-Sylow. Puisque $H \subseteq S$, on a forcément $H = S$, donc $O = O_H$ Donc H est un p-Sylow, $H = S$, et $O = O_H = \{gH : g \in G\} = G/H$. ∎

Théorème VI.2.3 (Premier théorème de Sylow)**.** *Soit G un groupe fini et p premier. Alors G admet un p-Sylow.*

Preuve du premier théorème de Sylow. On a $|X| = \binom{mp^n}{p^n} \equiv m \mod p$. Puisque $p \nmid m$, on a $p \nmid |X|$. En particulier, il existe une orbite O tel que $p \nmid |O|$. D'après le Lemme VI.2.2, il existe un p-Sylow $H \leq G$ tel que $O = G/H$. En particulier, un p-Sylow existe. ∎

Si $H \leq G$ est un p-Sylow, $g \in G$ et $K = gHg^{-1}$ alors, puisque la conjugaison par g est un automorphisme : $K \leq G$ et $|K| = |H|$. En particulier, K est aussi un p-Sylow. D'ailleurs, d'après Lagrange, l'ordre de tout sous-groupe de H est une puissance de p. La réciproque est aussi vraie :

Théorème VI.2.4 (Second théorème de Sylow)**.** *Soit G un groupe fini et p premier. Alors tous les p-Sylow de G sont conjugués. Autrement dit, si H et K sont des p-Sylow, alors il existe $g \in G$ tel que $gHg^{-1} = K$.*
De surcroît, tout sous-groupe de G dont l'ordre est une puissance de p est un sous-groupe d'un p-Sylow de G.

Démonstration. Soit $H \leq G$ un p-Sylow, et $K \leq G$ un sous-groupe d'ordre p^ℓ pour un certain ℓ. Considérons l'action $K \curvearrowright G/H$: c'est la restriction à K de l'action $G \curvearrowright G/H$, qui est elle-même une restriction de $G \curvearrowright X$ de tout à l'heure. On a $|G/H| = m$, et $p \nmid m$, donc cette action admet au moins une orbite O' telle que $p \nmid |O'|$.

Fixons $gH \in O' \subseteq G/H$. Alors $O' = K \cdot gH = \{kgH : k \in K\}$, et $|O'| = [K : K_{gH}] \mid p^\ell$. Puisque $p \nmid |O|'$, c'est que $|O'| = 1$. Autrement dit, $kgH = gH$ pour tout $k \in K$, donc $kg \in gH$ et $k \in gHg^{-1}$. Ainsi, $K \subseteq gHg^{-1}$, et gHg^{-1} est un p-Sylow.

$H = G_S = \{g \in G : gS = S\}$. Soit $S \in \mathcal{O}$

$X = \bigcup_{\mathcal{O} \in \Omega} \mathcal{O}$ (Ω : ensemble des orbites)

$\mathcal{O} \in \Omega$

↑ réunion disjointe. $\Rightarrow |X| = \sum_{\mathcal{O} \in \Omega} |\mathcal{O}|$

$X = \{S \subset G : |S| = p^n\}$, $|G| = m p^n$ $\Rightarrow |X| = \binom{|G|}{p^n} = \binom{m p^n}{p^n}$.

$K, H \leq G$, $|H| = p^n$ (H est un p-Sylow) $\Rightarrow \ell \leq n$

$|K| = p^\ell$

$K \curvearrowright G/H$:

$gH \in G/H$, $f \in K$

$\Rightarrow f(gH) = (fg)H \in G/H$.

Résumé Si : $H, K \leq G$

H p-Sylow, $|K| = p^\ell$.

$\Rightarrow \exists g \in G$ tq $K \subseteq gHg^{-1}$.

gHg^{-1} p-Sylow aussi.

$\Rightarrow$ (1) $K \subseteq$ un p-Sylow

(2) Si K est aussi un p-Sylow

alors : $|K| = p^n = |H| = |gHg^{-1}|$

$\Rightarrow K = gHg^{-1}$. ∎

3e thm de Sylow :
Contraintes sur le nombre N_p de p-Sylow de G.

$S = S_p = \{p\text{-Sylows de } G\}$. $|S| = N_p$.

Soit $H \in S$.

$\forall g \in G$: gHg^{-1} est un p-Sylow

$\Rightarrow gHg^{-1} \in S$

2e thm : Si $K \in S$ alors $\exists g \in G$ tq $K = gHg^{-1}$.

$\Rightarrow S = \{gHg^{-1} : g \in G\}$.

action par conjugaison :

$s \in G$ $K = gHg^{-1} \in S$

$G \curvearrowright S$: $s \cdot K = sKs^{-1}$

$= sgH(sg)^{-1}$.

S = orbite de H pour cette action.

(c'est une action transitive : une seule orbite.)

$S = \mathcal{O}_H$ $\quad (H \in S)$

$\Rightarrow |S| \cdot |\mathcal{O}_H| = [G : G_H]$.

où : $G_H = \{g \in G : gHg^{-1} = H\}$

$= N_G(H)$ le normalisateur de H dans G.

$\therefore N_p = |S| = [G : N_G(H)] = \dfrac{|G|}{|N_G(H)|}$

Or : $H \leq N_G(H)$ $\quad$ (t_j, pour tout ss-grp)

En effet : si $h \in H$

alors $hHh^{-1} = Hh^{-1} = H$.

$\Rightarrow |H| \mid |N_G(H)| \Rightarrow \dfrac{|G|}{|H|} = m$

$N_p = \dfrac{|G|}{|N_G(H)|}$

$\therefore N_p \mid m$.

Si K est un p-Sylow, c'est que $|K| = |H| = |gHg^{-1}| = p^n$, donc $K = gHg^{-1}$. Ceci prouve le deuxième théorème. ■

Maintenant, que nous savons que les p-Sylow existent et qu'ils sont tous conjugués, on peut se demander, combien il en existe exactement. Il n'est pas toujours possible d'y donner une réponse complète, mais nous pouvons établir au moins quelques contraintes.

Théorème VI.2.5 (Troisième théorème de Sylow)**.** *Soit G un groupe fini et p premier. Soit $|G| = p^n m$, où $p \nmid m$, et soit N_p le nombre des p-Sylow de G. Alors*

— $N_p \mid m$, *et*
— $N_p \equiv 1 \mod p$.

Démonstration. Soit $\mathfrak{S}$ l'ensemble des p-Sylows, de sorte que $N_p = |\mathfrak{S}|$. Si $H \in \mathfrak{S}$, alors $\mathfrak{S}$ est l'ensemble des conjugués de H, d'après le second théorème. Rappelons la conclusion de l'Exercice IV.17 : $|\mathfrak{S}| = [G : N_G(H)]$, et ceci divise $[G : H]$. Autrement dit, $N_p \mid m$.

Revenons maintenant à l'action $G \curvearrowright X$, et soit Ω l'ensemble de ses orbites. Nous pouvons le partitionner en :

$$\Omega_1 = \{O \in \Omega : p \nmid |O|\}, \qquad \Omega_2 = \Omega \setminus \Omega_1 = \{O \in \Omega : p \mid |O|\}.$$

Si $H \in \mathfrak{S}$, alors $H \in X$, et $O_H = G/H$ est de cardinal m, donc $G/H \in \Omega_1$. Ceci nous définit donc une application $\mathfrak{S} \to \Omega_1$, $H \mapsto G/H$.

Cette application est injective, car on peut retrouver H à partir de la famille $G/H = \{gH : g \in G\}$ (comment ?) D'après le Lemme VI.2.2, cette application est également surjective. Donc :

$$|X| = \sum_{O \in \Omega} |O| = \sum_{O \in \Omega_1} |O| + \sum_{O \in \Omega_2} |O| \equiv \sum_{H \in \mathfrak{S}} |G/H| = mN_p,$$

où $\equiv$ est la congruence modulo p. Nous avons aussi démontré plus tôt que

$$|X| = \binom{mp^n}{p^n} \equiv m.$$

Donc $mN_p \equiv m$, et puisque m est inversible modulo p, on a $N_p \equiv 1$, le tout modulo p. ■

Corollaire VI.2.6. *Soit $p < q$ premiers, et G un groupe d'ordre pq. Alors*

(i) *Le groupe G admet un unique q-Sylow.*

(ii) *S'il est aussi vrai que G admet un unique p-Sylow, alors G est cyclique : $G \cong C_{pq}$.*

Démonstration. D'après le troisième théorème, $N_q \equiv 1 \mod q$ et $N_q \mid p$. En particulier, $N_q \leq p < q$, donc forcément $N_q = 1$.

Soit H l'unique q-Sylow, et supposons également que G admet un unique p-Sylow, appelons-le K. On a $|H \cup K| \leq p + q - 1 < pq$ (l'identité appartient au deux). Il existe donc $x \in G \setminus (H \cup K)$. D'un côté $o(x) | pq$. Quelles sont les possibilités pour $o(x)$?

$X = \{S \subset G : |S| = p^n\}$ $\quad G \curvearrowright X : (g, S) \mapsto gS.$

$\Omega = \{\text{orbites}\} = \Omega_1 \cup \Omega_2$

orbites de cardinal non divisible par p ↑ $\quad$ orbites de card. divisible par p ↖

Si H est un p-Sylow : $H \in X$

$\{p\text{-Sylow}\} \twoheadrightarrow$

$\mathcal{O}_H = \{gH : g \in G\} = G/H.$

$\Rightarrow$ application $\Omega \to \Omega_1$

$H \longmapsto \mathcal{O}_H.$

$|\mathcal{O}_H| = [G : H] = m$

$\neq 1 \bmod p$

appl. injective : H est l'unique membre de $\mathcal{O}_H$ qui contient e.

$= G/H$

$\Rightarrow$ si $K, H \in S$ et $\mathcal{O}_H = \mathcal{O}_K$ alors $H = K$. ✓

Surjectif : Notre 1er Lemme.

$\therefore N_p = |S| = |\Omega_1|.$

$$|X| = \binom{mp^n}{p^n} \equiv m.$$

$$|X| = \sum_{\theta \in \Omega} |\theta|$$

$$= \sum_{\theta \in \Omega_1} |\theta| + \sum_{\theta \in \Omega_2} |\theta|$$

divisible par p.

$$\equiv \sum_{\theta \in \Omega_1} |\theta|$$

$$= \sum_{H \in S} \underbrace{|G/H|}_{m} = \underbrace{|S|}_{N_p} \cdot m.$$

$$m \equiv N_p \, m \mod p.$$

or $p \nmid m \Rightarrow$ m est inversible mod p :

$\Rightarrow 1 \equiv N_p \mod p.$ $\exists \ell : m\ell \equiv 1$

— $\mathrm{ord}(x) = 1$: non, car $x \neq e$.
— $\mathrm{ord}(x) = p$: dans ce cas, $\langle x \rangle$ serait un p-Sylow, donc égal à K, or $x \neq K$, donc impossible.
— $\mathrm{ord}(x) = q$: impossible pour la même raison avec q et H au lieu de p et K.
— $\mathrm{ord}(x) = pq$: c'est l'unique possibilité qui reste !
Donc $\mathrm{ord}(x) = |G|$, d'où $G = \langle x \rangle$ est cyclique.
(On pourrait aussi appliquer l'Exercice VI.8 pour déduire que G est cyclique – mais dans notre cas la preuve directe est aussi facile.) ■

Corollaire VI.2.7. *Soit $p < q$ premiers, et G un groupe tel que $|G| = pq$. Si G est abélien, ou si $p \nmid (q-1)$, alors G est cyclique.*

Démonstration. Si G est abélien alors il admet un unique p-Sylow (car tous les p-Sylow sont conjugués). Supposons maintenant que $p \nmid q-1$. Autrement dit, $q \not\equiv 1 \mod p$. D'après le troisième théorème, on a $N_p \mid q$, donc $N_p \in \{1, q\}$, et $N_p \equiv 1 \mod p$, donc $N_p \neq q$. On en déduit que $N_p = 1$, il existe donc un unique p-Sylow. D'après le Corollaire VI.2.6, G est cyclique. ■

Exercices

Exercice VI.1. Soit p premier et $m, n \in \mathbf{N}$. Montrons que $m \equiv \binom{mp^n}{p^n} \mod p$ d'une autre manière.

(i) Montrer que si $0 < k < p^n$, alors $p \mid \binom{p^n}{k}$.

(ii) Montrer que

$$\binom{mp^n}{p^n} = \sum_{k_1+\cdots+k_m=p^n} \binom{p^n}{k_1} \cdots \binom{p^n}{k_m}.$$

(iii) En déduire que

$$\binom{mp^n}{p^n} \equiv m \mod p.$$

Exercice VI.2. On dit que G est un **p-groupe** si l'ordre de chaque élément de G est une puissance de p.
Montrer qu'un groupe fini est un p-groupe si et seulement si son ordre est une puissance de p.

Exercice VI.3. Soit G un groupe d'ordre p^n.

(i) Montrer que si $n > 1$, alors G admet un sous-groupe distingué d'ordre p^k avec $0 < k < n$.
Indication : il y a plusieurs cas à considérer, mais on pourrait commencer en regardant le Lemme IV.3.2.

(ii) Déduire que pour tout $0 \leq k \leq n$, G admet au moins un sous-groupe d'ordre p^k.

Exercice VI.4. Soit G un groupe d'ordre $p^n m$, où $p \nmid m$. Montrer que pour tout $0 \leq k \leq n$, G admet au moins un sous-groupe d'ordre p^k.

Exercice VI.5. Montrer, sans utiliser les théorèmes de Sylow, que le second théorème de Sylow est équivalent à l'affirmation suivante :

> Soit $H \leq G$ un p-Sylow, et $K \leq G$ un sous groupe dont l'ordre est une puissance de p. Alors il existe $g \in G$ tel que $gKg^{-1} \leq H$.

Exercice VI.6. Trouver les 2- et 3-Sylow des groupes symétriques S_3 et S_4. Vérifier les affirmations du second et du troisième théorème.

Exercice VI.7. Soit G un groupe d'ordre p^k avec p premier, admettant au plus un sous-groupe de chaque ordre. Montrer que G est monogène.
Indication : essayer de majorer le cardinal de $\{x \in G : \mathrm{ord}(x) < p^k\}$.

Exercice VI.8. Soit G un groupe d'ordre n (fini), admettant au plus un sous-groupe de chaque ordre. Soit $n = p_1^{k_1} \cdots p_m^{k_m}$ la factorisation de n en puissance de premiers.

(i) Montrer que pour chaque $1 \leq i \leq m$, G admet un sous-groupe H_i d'ordre $p_i^{k_i}$.

(ii) Montrer que chaque H_i est monogène (voir l'exercice précédent). Dans la suite, soit x_i un générateur de H_i.

(iii) Montrer que $H_i \trianglelefteq G$.

(iv) Montrer que $H_i \cap H_j = \varnothing$ pour $i \neq j$.

(v) Déduire que les x_i commutent entre eux (on pourrait s'inspirer de la preuve du Remarque V.1.8).

(vi) Déduire que $y = x_1 x_2 \cdots x_m$ est un générateur de G, qui est par conséquent monogène.

Exercice VI.9. Soit G un groupe fini d'ordre n. À de l'Exercice II.23 et de l'Exercice VI.8, montrer que sont équivalents :

(i) G est cyclique.

(ii) G admet exactement un sous-groupe d'ordre d pour chaque $d \mid n$.

(iii) G admet au plus un sous-groupe de chaque ordre.