TD 4/12 — Fiche 8 Plus sur les thms de Sylow

Exo 1 Soit G - groupe fini.

Pour chaque p premier divisant $|G|$:
on choisit un p-Sylow $G_p \leq G$.

Mq : $\boxed{S = \bigcup_p G_p}$ engendre G.

Indication Soit $H = \langle S \rangle$ le ss-gr engendré : que peut-on dire de $|H|$?

— $\forall p$: $G_p \subseteq H \Rightarrow |G_p| \leq |H|$.

Mieux : $G_p \leq H \Rightarrow |G_p| \mid |H|$

— Factorisons : $|G| = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$

$$\Rightarrow |G_{p_i}| = p_i^{k_i}$$

$$\Rightarrow p_i^{k_i} \mid |H| \quad \forall i = 1 \ldots \ell$$

$$\Rightarrow \left(\prod_{i=1}^{\ell} p_i^{k}\right) \Bigg| \; |H|$$

$$\Rightarrow |G| \mid |H|$$

Or $|H| \leq |G| \Rightarrow |H| = |G|$

$$\Rightarrow H = G.$$

Exo 6. Mq A_5 est simple en utilisant Sylow.

1. Identifier les éls d'ordre 3. Les compter, compter les 3-Sylows.

De manière générale : si p est premier : un $\sigma \in S_n$ est d'ordre $p \Leftrightarrow$ c'est un pr. de 1 ou plus p-cycles disjoints

$\Rightarrow$ Une permutation $\sigma \in S_5$ est d'ordre 3
$\Leftrightarrow$ c'est un 3-cycle.

tout 3-cycle $\in A_5$

$\Rightarrow$ $\boxed{\text{les éls de } A_5 \text{ d'ordre 3 sont les 3-cycles.}}$

Comptons-les : $(i\ j\ k) = (j\ k\ i) = (k\ i\ j)$

$$\frac{5 \cdot 4 \cdot 3}{3} = 20.$$

Combien de 3 Sylow ?

$|A_5| = \frac{|S_5|}{2} = 60$ la plus g^de puissance de 3 divisant $60 = 3$.

$A_5 = \ker(\mathrm{sgn})$ où : $\mathrm{sgn} : S_5 \to \{\pm 1\}$

$\Rightarrow A_5 \trianglelefteq S_5$

$S_5 / A_5 \simeq \{\pm 1\}$

$= |S_5|/|A_5|$

$\Rightarrow [S_5 : A_5] = 2$

$\Rightarrow |A_5| = \frac{|S_5|}{2}$

Un 3-Sylow a ordre 3

$\Rightarrow$ — $= \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$

3-cycle

puisque 3 est premier : 2 ss-groupes d'ordre 3 distincts s'intersectent en $\{e\}$.

$\Rightarrow$ 2 éls ~~non identité~~ d'ordre 3 pour chaque 3-Sylow.

$\Rightarrow N_3 = \frac{20}{2} = 10$ 3-Sylow.

[est-ce bien compatible avec le 3e thm ?

$10 \equiv 1 \quad (3)$ ✓

$10 \mid \frac{|A_5|}{3}$ càd $10 \mid 20$ ✓]

2. pareil pour $p = 5$

Quels sont les élts d'ordre 5 de A_5 (S_5) ?

Comme Ht à l'hr. $\sigma \in S_5$ est d'ordre 5

$\Leftrightarrow$ c'est un 5-cycle

[$\mathrm{sgn}(k\text{-cycle}) = (-1)^{k-1} \Rightarrow$ tout 5-cycle est pair]

$\therefore$ les élts d'ordre 5 de A_5 sont les 5-cycles

Combien ? $(a_1\ a_2\ a_3\ a_4\ a_5) = (a_2 \cdots a_5\ a_1) = (a_3\ a_4\ a_5\ a_1\ a_2)$
$= \cdots$

$$\frac{\underbrace{5 \cdot 4 \cdots 1}_{5}}{} = \frac{5!}{5} = 24.$$

$N_5 = ?$ $\quad 60 = 5 \cdot \boxed{12} \Rightarrow$ Un 5-Sylow est d'ordre 5.

$= \langle \sigma \rangle = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4\}$

5-cycle

5-cycles qui engendre $\langle \sigma \rangle$.

$\Rightarrow$ si H, K sont 2 5-Sylow distincts : $H \cap K = \{e\}$.

$\Rightarrow$ 4 5-cycles pour chaque 5-Sylow

$\Rightarrow n_5 = \frac{24}{4} = 6$ 5-Sylow.

[$6 \equiv 1 \ (5)$ ✓

$6 \mid \underbrace{\frac{|A_5|}{5}}_{24}$ ✓]

Désormais : Soit $H \trianglelefteq A_5$.

3. Supposons que H contient un élt d'ordre 3 [ou d'ordre 5]. Mq $30 \mid |H|$.

puis que $H = A_5$.

Soit $\sigma \in H$ d'ordre 3.
alors $K = \langle \sigma \rangle \leq H$ et $|K| = 3$, $K \leq A_5$
$\Rightarrow K$ est un 3-Sylow de A_5

Si $K' \leq A_5$ est un autre 3-Sylow :
D'après le 2e thm : $\exists \tau \in A_5$ tq
$K' = \tau K \tau^{-1} \leq \tau H \tau^{-1} = H$

$\therefore$ H contient <u>tous</u> les 3-Sylow de A_5.
$3 \mid |H|$ (Lagrange) or $9 \nmid |H|$
car $|H| \mid 60$ $(H \leq A_5)$
$\Rightarrow$ un 3-Sylow de H est un ss-groupe de H d'ordre 3

$\therefore$ Les 3-Sylows de A_5 sont exactement les 3-Sylows de H.

$|H| = 3 \cdot m$, $m = \frac{|H|}{3}$ $3 \nmid m$.

3e thm de Sylow :

$\#\{3\text{-Sylow de } H\} \mid m$

$\#\{3\text{-Sylow de } A_5\}$ $\shortparallel$

$= 10$

$\therefore$ $10 \mid m$

$30 \mid |H|$.

Soit K un 3-Sylow de A_5

$\Rightarrow K \leq H \Rightarrow K$ est un 3-Sylow de H.

Soit K un 3-Sylow de $H \leq A_5$

$\Rightarrow K \leq A_5 \Rightarrow$ ——— A_5

On a démontré que si $H \trianglelefteq A_5$ et H contient un élt d'ordre 3 alors $30 \mid |H|$.

Pareil pour 5 :

On suppose que H contient un σ d'ordre 5. $\Rightarrow \langle\sigma\rangle \leq H \leq A_5 \Rightarrow$ c'est un 5-Sylow de A_5.

Si K est un 5-Sylow de A_5 ;

$K \overset{\text{thm}}{=} \tau \langle\sigma\rangle \tau^{-1} \leq \tau H \tau^{-1} = H$

$\Rightarrow$ tout 5-Sylow de A_5 est un ss-grp de H

...... $\Rightarrow$ les 5-Sylow de H

sont exactement les 5-Sylow de A_5.

Il y en a 6.

$|H| = 5 \cdot m$ (5 $\nmid$ m)

$6 \mid m$ (3^e thm) $\Rightarrow$ $30 \mid |H|$. $\Rightarrow |H| = 30$ ou 60

Or : $3 \mid 30$ et $5 \mid 30$.

donc : si $30 \mid |H| \Rightarrow 3 \mid |H|$ et $5 \mid |H|$

$\Rightarrow$ H contient et un él^t d'ordre 3
et ——— 5

Si H contient un él^t d'ordre 3 ou 5 $\Rightarrow 30 \mid |H|$

$\Rightarrow$ H contient un él^t d'ordre 3
et ——— 5

$\Rightarrow$ H contient tous les 3-Sylow
et 5-Sylow de A_5.

$\Rightarrow$ H contient tous les él^{ts} de A_5
d'ordre 3 ou 5.

Il y en a : $20 + 24 = 44 > 30$

$\Rightarrow |H| = 60$ $H = A_5$.

4. reste à considérer : $H \trianglelefteq A_5$

mais H ne contient aucun él d'ordre 3 ni 5.

$\Rightarrow 3 \nmid |H|$ et $5 \nmid |H|$ (contraposée du théo de Cauchy)

$\Rightarrow |H| = 2^\ell$. $(\Leftrightarrow \forall \sigma \in H$, $ord(\sigma)$ = puissance de 2

1, 2 ou 4 $(8 \nmid 60)$

H est un 2-groupe

[Déf : H est un p-groupe si $\forall x \in H$, $ord(x) = p^?$

Si H est fini : $\Leftrightarrow |H| = p^?$]

Si $\sigma \in H$, $ord(\sigma) = 4$:

$\Rightarrow \sigma = 4$-cycle $\Rightarrow sgn(\sigma) = -1 \Rightarrow \sigma \notin A_5 \Rightarrow \sigma \notin H$

Si $\sigma \in H$, $ord(\sigma) = 2$:

$\Rightarrow \sigma = \begin{cases} \text{trans.} \quad \times & - \text{impair} \\ \text{pr. de 2 transp disjointes.} & - \text{pair} \end{cases}$

$\Rightarrow \sigma = (i\,j)(k\,\ell)$ 2 transp. disjointes

i, j, k, ℓ sont distincts, soit m distinct d'eux

$\tau = (i\,j\,m) \in A_5$.

$\Rightarrow \tau\sigma\tau^{-1} \in \tau H \tau^{-1} = H$

$\tau\sigma\tau^{-1} = (j\,m)(k\,\ell)$

$\therefore \sigma \cdot \tau\sigma\tau^{-1} \in H$

$\sigma \cdot \tau\sigma\tau^{-1} = (i\,j)(k\,\ell)(j\,m)(k\,\ell) = (i\,j\,m)$ d'ordre 3.

Contradiction avec l'hypothèse.

$\therefore \forall \sigma \in H$: $ord(\sigma) = 1$: $\sigma = e$.

$H = \{e\}$

On a montré :

$\forall\ H \trianglelefteq A_5$: $H = A_5$ ou $H = \{e\}$

Pause ; 15h45

$\therefore$ A_5 est simple.

Exo 5. 1. Mq si $G \leq K$ et K admet un p-Sylow alors G admet un p-Sylow

(Sans utiliser le 1er thm de Sylow !)

Soit $P \leq K$ un p-Sylow de K.

On a une action par translation

$$K \curvearrowright K/P$$
$$x \cdot kP = xkP.$$

On peut la restreindre en une action de G :

$$G \curvearrowright K/P$$
$$g \cdot kP = gkP \qquad (g \in G \quad k, gk \in K$$
$$kP, gkP \in K/P)$$

(i) Calculer G_{kP} = stabilisateur de kP :

$$G_{kP} = \{ g \in G : \underline{gkP = kP} \}$$
$$\Updownarrow$$
$$gkPk^{-1} = \underline{kPk^{-1}} \iff g \in kPk^{-1}.$$

Si $G \geq H$, $g \in G$:

$gH = H \iff g \in H$

$kPk^{-1} \leq K$ (c'est même un p-Sylow de K !)

$G_{kP} = (kPk^{-1}) \cap G$.

(ii) Utiliser la formule des classes pour mq.

$\exists k \in K$ tq $kPk^{-1} \cap G$ est un p-Sylow de G.

formule des classes :

$$|O_x| = [G : G_x]$$

Dans notre cas : $|O_{kP}| = [G : (kPk^{-1}) \cap G]$.

$|kPk^{-1}| = |P|$ = puissance de p

$G \cap kPk^{-1} \leq kPk^{-1} \Rightarrow |G \cap kPk^{-1}|$ = puissance de p.

$G \cap kPk^{-1}$ est un p-Sylow de G

$\Leftrightarrow |G \cap kPk^{-1}|$ = la plus g^d puissance de p divisant $|G|$

$\Leftrightarrow [G : G \cap kPk^{-1}] = \dfrac{|G|}{|G \cap kPk^{-1}|}$ n'est pas divisible par p.

$$|K/P| = \sum_{O \in \Omega} |O|$$ où Ω = l'ensemble des orbites de $G \curvearrowright K/P$.

__or :__ $|K/P| = \dfrac{|K|}{|P|}$

et $|P|$ = la plus gde puissance de p divisant $|K|$

$\Rightarrow p \nmid |K/P|$.

$\Rightarrow \exists O \in \Omega$ tq : $p \nmid |O|$

$\exists k \in K$ tq: $kP \in \Theta$ $\quad$ Si $\Theta \in \Omega$: $\quad x \in \Theta \iff \Theta = \Theta_x$.

$\Theta = \Theta_{kP}$.

$\Rightarrow |\Theta| = |\Theta_{kP}| = [G : G_{kP}]$

$= [G : G \cap kPk^{-1}]$

$\therefore \quad p \nmid [G : G \cap kPk^{-1}]$

$\iff G \cap kPk^{-1}$ est un p-Sylow de G.

Résumé : On a $p \nmid |K/P|$ (car P est un p-Sylow de K)

$\Rightarrow \exists$ orbite Θ de $G \curvearrowright K/P$

t.q. $p \nmid |\Theta|$

$\Rightarrow$ $kPk^{-1} \cap G$ est un p-Sylow de G

$\forall kP \in \Theta$.

---

2. Thm de Cayley : Soit G un groupe d'ordre n alors G est isomorphe à un ss-groupe de S_n.

pq? On énumère ~~les~~ les élt de G :

$G = \{g_1, g_2, \ldots, g_n\}$

$\forall g \in G$: l'application $G \to G$
$h \mapsto gh$

est une bijection càd une permutation de G.

On peut définir $\sigma_g : \{1 - n\} \to \{1 - n\}$

par : $g \cdot g_i = g_{\sigma_g(i)}$.

alors on vérifie que 1. $\sigma_g \in S_n$.

2. $\Sigma : G \to S_n$
$g \mapsto \sigma_g$ est un morphisme injectif.

$$\Rightarrow \quad G \simeq \underbrace{\operatorname{img} \Sigma}_{H} \leq S_n.$$

Donc : G admet un p-Sylow $\Leftrightarrow$ H en admet un.

D'après la partie (i) : Si S_n admet un p-Sylow alors H en admet un, donc G aussi.
autrement dit : pour montrer que G admet un p-Sylow il suffit de montrer que S_n admet un p-Sylow

Soit k un corps.

Je veux montrer que G se plonge dans $GL_n(k)$. (i.e. $G \simeq$ ss-groupe de $GL_n(k)$)

$\Leftrightarrow$ $\exists$ $\underbrace{\text{morphisme injectif}}_{\text{plongement}}$ $G \hookrightarrow GL_n(k)$

On a déjà $G \hookrightarrow S_n$

il suffit de trouver $S_n \hookrightarrow GL_n(k)$.

(puis composer)

$$S_n \ni \sigma \longmapsto \underbrace{\begin{array}{c} \\ i \end{array}\!\!\left(\begin{array}{c} j \\ \delta_{i,\sigma(j)} \end{array} \right)}_{A_\sigma}$$

$\sigma = (124) \in S_4$

$$A_\sigma = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$(A_\sigma A_\tau)_{i,k} = \sum_j \overset{(A_\sigma)_{ij}}{\overset{\shortparallel}{\delta_{i\sigma(j)}}} \; \overset{(A_\tau)_{jk}}{\delta_{j\tau(k)}} = \begin{cases} 1 & \exists j \quad i = \sigma(j),\ j = \tau(k) \\ 0 & \text{sinon} \end{cases}$$

$$\Leftrightarrow \begin{cases} 1 & i = \sigma \circ \tau(k) \\ 0 & \text{sinon} \end{cases}$$

$$A_\sigma A_\tau = A_{\sigma\tau} \,. \quad (*)$$

$A_{id} = I_n$.

$\Rightarrow (A_\sigma)^{-1} = A_{\sigma^{-1}}$

$\Rightarrow \quad A_\sigma \in GL_n(K) \qquad \forall \sigma \in S_n.$

$\sigma \mapsto A_\sigma$ est un morphisme par $\circledast$.

$S_n \longrightarrow GL_n(K)$

si $\sigma \neq \tau$: $\exists j$ tq $\sigma(j) \neq \tau(j)$

$\Rightarrow$ la j^e colonne de A_σ

$\neq$ ——— A_τ.

$\Rightarrow$ c'est un morphisme injectif.

$$\begin{tikzcd} G \arrow[r, hook] \arrow[rr, hook, bend right] & S_n \arrow[r, hook] & GL_n(K) \end{tikzcd}$$

(Rmq / Ezo : $\operatorname{sgn} \sigma = \det A_\sigma$.)

$\therefore$ Pour montrer que G (d'ordre n) admet un p-Sylow il suffit de trouver un corps k tq $GL_n(k)$ soit fini et admette un p-Sylow.

Observation : si K est infini (et $n \geq 1$) alors $GL_n(K)$ est infini car contient

$\{ aI_n : a \in K \setminus \{0\} \}$. $\left(= Z(GL_n(K)) \right)$

2. ~~Soit p premier~~ On considère le corps fini à p élt : $\mathbb{F}_p = (\mathbb{Z}/_p\mathbb{Z}, +, \cdot)$

On étudiera le Groupe

$$G = GL_n(\mathbb{F}_p).$$

(i) $|G| = ?$

Combien de possibilités pour h

C_1 = 1ère colonne : $p^n - 1$ (n'importe quoi, sauf 0)

C_2 : 2e " : $p^n - p$ (" " , sauf multiple de C_1)

C_3 : $p^n - p^2$: (tout sauf Vect(C_1, C_2))

C_k : $p^n - p^{k-1}$ (tout sauf Vect$(C_1 \dots C_{k-1})$)

⋮

C_n $p^n - p^{n-1}$ $\dots \dots \Rightarrow (C_1 \dots C_n)$ est une famille libre.

$$|G| = \prod_{k=0}^{n-1} (p^n - p^k)$$

$$= \underbrace{\prod_{k=0}^{n-1} (p^{n-k} - 1)}_{m} \cdot \underbrace{\prod_{k=0}^{n-1} p^k}_{p^N}$$

$= \underbrace{M\ p^N}$, $p \nmid M$.

$\forall \ell \geq 1 \quad p \nmid p^\ell - 1$
$p^\ell - 1 \equiv -1\ (p)$.
$\Rightarrow \prod_{k=0}^{n-1} (p^{n-k}-1) \equiv (-1)^n\ (p)$

$N = 0 + \dots + (n-1) = \frac{n(n-1)}{2}$.

$\Rightarrow p^N$ est la plus gd puissance de p divisant $|G|$ puisque $p \nmid M$

$\therefore$ U_n p-Sylow de $G = GL_n(\mathbb{F}_p)$

est un ss-groupe d'ordre $p^{\frac{n(n-1)}{2}}$.

Soit $U_n(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in M_n(\mathbb{F}_p) \right\} \subseteq GL_n(\mathbb{F}_p)$.

= "matrices unipotentes triangulaires supérieures".

Exo
$I_n \in U_n(\mathbb{F}_p)$
$A, B \in U_n(\mathbb{F}_p) : AB \in U_n(\mathbb{F}_p)$
$A \in U_n(\mathbb{F}_p) : A^{-1} \in U_n(\mathbb{F}_p)$

Nous allons admettre.

$\Rightarrow U_n(\mathbb{F}_p) \leq GL_n(\mathbb{F}_p)$

(pareil pour n'importe quel corps :
$U_n(k) \leq GL_n(k)$)

$|U_n(\mathbb{F}_p)| = p^L$ où

L = nombre de coefficients à choisir dans le triangle

$\begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix}$

$1^{ère}$ ligne : $n-1$

2^e —— $n-2$

$\vdots$

$(n-1)^e$ — 1

n^e 0

$$L = 0 + 1 \cdots + \cdots + n-1 = \frac{n(n-1)}{2} = N$$

$\therefore$ $U_n(\mathbb{F}_p)$ est un p-Sylow de $GL_n(\mathbb{F}_p)$.

+ Exo 5 :

$\therefore$ $\forall n$, p premier :

Un groupe G d'ordre n admet un p-Sylow : puisqu'il se plonge dans $GL_n(\mathbb{F}_p)$ qui lui admet un p-Sylow

$\Rightarrow$ Autre démonstration du 1er thm de Sylow.