CM du 3 décembre.

Rappel : G groupe fini, p premier.

p^k : puissance maximale de p divisant $|G|$;

$|G| = p^k \cdot m$, $p \nmid m$.

Un p-Sylow : $H \leq G$ t.q. $|H| = p^k$.

Thms de Sylow : 1. G admet un p-Sylow.

2. Tous les p-Sylow de G sont conjugués

3. Soit N_p le # des p-Sylow.
alors $N_p \equiv 1 \mod p$
et $N_p \mid m$.

Applications :

Thm : Soit G un groupe fini et p diviseur premier de $|G|$. alors $\exists x \in G$ t.q. $\mathrm{ord}(x) = p$.

(déjà vu en TD, avec une autre preuve)

preuve utilisant le 1er thm de Sylow :

On sait que G admet au moins un p-Sylow.

Soit $H \leq G$ un p-Sylow : $|H| = p^k$ où

p^k est la + grande puissance de p divisant $|G|$.

par hypothèse : $p \mid |G| \Rightarrow k \geq 1 \Rightarrow H \neq \{e\}$.

$\Rightarrow \exists x \in H - \{e\}$. On choisit un tel x.

- $x \neq e \Rightarrow \mathrm{ord}(x) > 1$
- D'après Lagrange : $\mathrm{ord}(x) \mid \underbrace{|H|}_{p^k} \Rightarrow \mathrm{ord}(x) = p^l$

et sachant : $l \geq 1$.

Posons $y = x^{p^{l-1}} \neq e$ (car $y^p = e$) $\Rightarrow \mathrm{ord}(y) = p$.

$y^p = \left(x^{p^{l-1}}\right)^p = x^{p^{l-1} \cdot p} = x^{p^l} = e$.

VII

Groupes simples etc...

§1. Groupes simples :

Rque ! : Soit G un groupe. Alors :

$$G \trianglelefteq G \quad \text{et} \quad \{e\} \trianglelefteq G$$

[On notera le groupe trivial $\{e\}$ par 1 :

$$1 \trianglelefteq G$$

]

Donc tout groupe G admet au moins 2 ss-gpes distingués, pourvu que $G \neq 1$.

Définition : Un groupe G est dit **simple** s'il admet exactement deux sous-groupes distingués $1 (= \{e\})$ et G lui-même

En particulier un groupe simple n'est pas trivial.

Exm Groupes simples abéliens :
Tout groupe d'ordre premier ($\Rightarrow$ forcément cyclique) est simple (et abélien).

En effet : soit p premier, $|G| = p$.

Si $H \trianglelefteq G$ alors $|H| \mid p$

$\Rightarrow |H| = p$ ou 1

$\Rightarrow H = G$ ou $H = 1$.

Proposition : Les groupes simples abéliens sont exactement les groupes (cycliques) d'ordre premier.

preuve Il reste à montrer que si G est simple et abélien alors $|G|$ est premier.

Soit G simple et abélien : $G \neq 1 \Rightarrow |G| > 1$

$\Rightarrow \exists$ premier p tq $p \mid |G|$

$\Rightarrow \exists x \in G$ tq $\operatorname{ord}(x) = p$

$\|$

$|\langle x \rangle|$

Soit $H = \langle x \rangle$: $|H| = p$. $\therefore H \neq \{1\}$.

$H \leq G$ $\overset{G \text{ est abélien}}{\Longrightarrow}$ $H \trianglelefteq G$, G est simple

$\Rightarrow H = G$

$\Rightarrow |G| = p$.

Groupes simples abéliens $\Rightarrow C_p$, p premier

trop facile.

Groupes simples non abéliens : En existe-il ?

(Non) Exemples : D_n S_n. pour $n \geq 3$

En effet : $D_n = \{\text{rotations}, \text{réflexions}\}$ $(n \geq 3)$

$= \underbrace{\{\text{rotations}\}}_{R} \rtimes \langle s \rangle$

où s est n'importe quelle réflexion.

En particulier : $R \trianglelefteq D_n$, $R \simeq C_n \simeq \mathbb{Z}/n\mathbb{Z}$

et $1 \neq R \neq D_n$

$\Rightarrow$ D_n n'est pas simple

(plus simple et direct : $R = \{\text{rotations}\}$ est un ss-groupe d'indice $2 = \frac{|D_n|}{|R|} = \frac{2n}{n}$. $\Rightarrow R \trianglelefteq D_n$

$\Rightarrow D_n$ n'est pas simple)

S_n : $n = 1$ $S_1 : 1$ n'est pas simple

$n = 2$ $S_2 \simeq C_2$ est simple mais abélien.

$n \geq 3$:

Rappel : La signature est un morphisme de groupes

$\text{sgn} : S_n \to \{\pm 1\}$

$\mathrm{sgn}\,\sigma = 1 \iff \sigma =$ produit de n transpositions, n pair

"σ est pair"

$\mathrm{sgn}\,\sigma = -1 \iff \sigma =$ ~~~~~~~~~~ n impair.

"σ est impair"

On pose $A_n = \ker(\mathrm{sgn})$

$= \{\sigma \in S_n : \mathrm{sgn}(\sigma) = 1\}$.

$\Rightarrow A_n \trianglelefteq S_n$

pour $n \geq 2$: $A_n \neq S_n$ $\left((12) \notin A_n \right)$

pour $n \geq 3$: $A_n \neq 1$ $\left((1\,2\,3) \in A_n \right)$

$\Rightarrow$ pour $n \geq 3$: $1 < A_n \triangleleft S_n \Rightarrow S_n$ n'est pas simple.

Exo : $[S_n : A_n] = 2$. (pour $n \geq 2$)

Le groupe A_n s'appelle le groupe alterné

Résumé ! Pour $n \geq 3$: on trouve dans D_n et dans S_n un ss-groupe (distingué) d'indice 2. $\Rightarrow$ ni S_n ni D_n ne sont simples

Regardons ces ss-groupes d'indice 2 :

— Dans le cas de D_n, c'est $R = \{\text{rotations}\}$ $\simeq C_n$. simple $\iff$ n premier

tjs abélien.

pas de grp simple non abélien ici ...

— Dans le cas de S_n, ce ss. groupe est A_n, le groupe alterné.

Cas :

$n=1$: $A_1 = S_1 - \{e\} = 1$ (ici : $[S_1 : A_1] = 1$ et non 2...)

$n=2$: $S_2 \simeq C_2$, $A_2 = 1$ pas simple.

$n=3$ $|S_3| = 6 \Rightarrow |A_3| = 3 = \frac{6}{2} \Rightarrow A_3 \simeq C_3$

simple, mais abélien.

$n=4$ A_4 n'est pas abélien.

Rappel :

$$\tau\,(a_1\ a_2\ a_3\ \dots)\,\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \tau(a_3)\ \dots)$$

$\sigma = (1\ 2\ 3) \in A_n$ $(\forall\ n \geq 4)$

$\tau = (2\ 3\ 4) \in A_n$, $n \geq 4$

$\Rightarrow \tau\sigma\tau^{-1} = (1\ 3\ 4) \neq \sigma$

$\tau\sigma \neq \sigma\tau$. $\Rightarrow A_n$, $n \geq 4$ n'est pas abélien.

Soit $n=4$:

Or : Soit $H = \{ e,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3) \}$.

I. $H \subset A_4$.

II. $e \in H$, si $\sigma \in H$ alors $\sigma^{-1} = \sigma \in H$.

et : si $\sigma, \tau \in H$.

si $\sigma = e$: $\sigma\tau = \tau \in H$

$\tau = e$ $\sigma\tau = \sigma \in H$.

$\tau = \sigma$ $\sigma\tau = \sigma^2 = e \in H$.

reste : $\sigma \neq \tau \neq e$ p.e : $(1\,2)(3\,4)(1\,3)(2\,4)$

$= (1\,4)(2\,3) \in H$

le autre cas. pareil.

Conclusion : $\forall \sigma, \tau \in H$: $\sigma\tau \in H$ $\left(\text{Ex20 : } H \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^2\right)$

i.e. $H \leq A_4$

$\forall\ \sigma \in H \qquad \forall\ \tau \in A_n$ (voire $\tau \in S_n$) :

si $\sigma = e$: $\tau\sigma\tau^{-1} = e \in H$.

Sinon : $\sigma = (ij)(k\ell)$ $i\ j\ k\ \ell$ distincts

$$\tau\sigma\tau^{-1} = \tau(ij)(k\ell)\tau^{-1}$$
$$= \tau(ij)\tau^{-1}\tau(k\ell)\tau^{-1}$$
$$= (\tau(i)\ \tau(j))\,(\tau(k)\ \tau(\ell)) \in H.$$

$\Rightarrow \quad \tau H \tau^{-1} \subseteq H \qquad \forall\ \tau \in A_n$

$\Rightarrow \quad H \trianglelefteq A_n$.

$1 \neq H \trianglelefteq A_n$ (car $(123) \in A_n$, $\notin H$)

$\therefore$ A_n n'est pas simple.

Thm A_n est simple $\forall\ n \geq 5$.

pause $\Rightarrow$ 10h30.

Remarque $(ij)(jk)$ $i\ j\ k$ distincts

$= (ijk)$. $\Rightarrow$ $(ijk) \in A_n$.

Lemme toute permutation paire est produit de 3-cycles.

preuve : Rappel : pour $\sigma \in S_n$:

$$\mathrm{supp}(\sigma) = \{1 \leq i \leq n : \sigma(i) \neq i\}.$$

On fait la preuve par réc. sur $|\mathrm{supp}(\sigma)|$ (pour $\sigma \in A_n$)

$|\mathrm{supp}(\sigma)| = 0$: $\sigma = e$ = pr. de 0 3-cycles.

$|\mathrm{supp}(\sigma)| = 1$ impossible.

$|\mathrm{supp}(\sigma)| = 2$: $\sigma = (i\,j)$ où $\mathrm{supp}(\sigma) = \{i, j\}$.

$\Rightarrow \sigma \notin A_n$ impossible

($|\mathrm{supp}(\sigma)| = 3$: $\sigma = (i\,j\,k)$ ✓.)

$|\mathrm{supp}(\sigma)| \geq 3$: Soit $i \in \mathrm{supp}\,\sigma$.

Soit $j = \sigma(i) \Rightarrow j \in \mathrm{supp}(\sigma)$ et $j \neq i$

Soit $k \in \mathrm{supp}(\sigma)$, $k \neq i, j$.

Posons $\tau = (i\,j\,k)$.

$\rho = \sigma\tau^{-1}$

$\mathrm{supp}(\tau) \subseteq \mathrm{supp}(\sigma)$

alors $\Rightarrow \mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$

$\rho(j) = \sigma\tau^{-1}(j) = \sigma(i) = j \Rightarrow j \notin \mathrm{supp}(\rho)$

$\Rightarrow \mathrm{supp}(\rho) \subsetneq \mathrm{supp}(\sigma)$

$\Rightarrow |\mathrm{supp}(\rho)| < |\mathrm{supp}(\sigma)|$

or $\sigma, \tau \in A_n \Rightarrow \rho \in A_n$

par hyp de réc : ρ = pr de 3-cycles

$\Rightarrow \sigma = \rho\,\underbrace{\tau}_{\text{3-cycle}}$ = pr de 3-cycles.

Lemme. Soit $n \geq 5$. Soit $1 \neq H \trianglelefteq A_n$

I. H contient un 3-cycle.

II. H contient tous les 3-cycles.

III. $H = A_n$

preuve.

I. $H \neq 1 \Rightarrow |H| > 1 \Rightarrow \exists$ premier p tq $p \mid |H|$

$\Rightarrow \exists \sigma \in H$ tq $\mathrm{ord}(\sigma) = p$.

$\Rightarrow$ σ = produit de $k \geq 1$ p-cycles disjoints.

Cas facile : $p \geq 3$

$\sigma = (a_1\ a_2\ a_3\ \dots\ a_p)\ \tau_2$ (le produit des $k-1$ autres p-cycles)

Soit $\tau = (a_1\ a_2\ a_3) \in A_n$.

$\Rightarrow \tau\sigma\tau^{-1} \in H$ (car $H = \tau H \tau^{-1}$).

$(a_2\ a_3\ a_4\ \dots\ a_p)\ \sigma$

$\tau[\sigma\tau^{-1}\sigma^{-1}] \in H$

$\tau^{-1} = (a_3\ a_2\ a_1)$

$\sigma\tau^{-1}\sigma^{-1} = (a_4\ a_3\ a_2)$

$\tau\sigma\tau^{-1}\sigma^{-1} = (a_1\ a_2\ a_3)(a_4\ a_3\ a_2)$

$= (a_1\ a_2\ a_4) \in H.$

Cas difficile : $p = 2$. $\Rightarrow \sigma$ est produit de k transp. à supp disj.

$\sigma = (a_1\ a_2)(a_3\ a_4)\ \underbrace{\dots}_{\tau^{-1}} \in H.$ $\Rightarrow k$ est pair $\Rightarrow k \geq 2$.

les autres $k-2$ transp.

soit $\tau = (a_1\ a_2\ a_3) \in A_n$.

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

$\tau\underbrace{\sigma\tau^{-1}\sigma^{-1}} \in H$

$\sigma(a_3\ a_2\ a_1)\sigma^{-1} = (a_4\ a_1\ a_2)$

$\tau\sigma\tau^{-1}\sigma^{-1} = (a_1\ a_2\ a_3)(a_4\ a_1\ a_2) =$

$(a_1\ a_3)(a_2\ a_4)$ = pr. de 2 transp. disj.

OPS : $(a_1\ a_2)(a_3\ a_4) \in H$, $a_1\ a_2\ a_3\ a_4$ distincts.

Puisque $n \geq 5$: soit $a_5 \neq a_1, a_2, a_3, a_4$.

Soit $\rho = (a_1\ a_2\ a_5) \in A_n$.

$\rho\sigma\rho^{-1} = (a_2\ a_5)(a_3\ a_4)$.
$\in H$

$\sigma\rho\sigma\rho^{-1} = (a_1\ a_2)(a_3\ a_4)(a_2\ a_5)(a_3\ a_4)$
$\in H$ $= (a_1\ a_2\ a_5)$

Dans un cas comme dans l'autre : H contient un 3-cycle.

II H contient tous les 3-cycles.

En effet : soit $(a_1\ a_2\ a_3) \in H$

et soit $(i\ j\ k)$ un 3-cycle quelconque.

On peut compléter l'application partielle

$$\begin{cases} a_1 \mapsto i \\ a_2 \mapsto j \\ a_3 \mapsto k \end{cases}$$

en une permutation $\tau \in S_n$.

1er cas : $\tau \in A_n$. $\underbrace{\tau(a_1\ a_2\ a_3)\tau^{-1}}_{\in H} = (i\ j\ k)$

2e cas : $\tau \notin A_n$: τ est impair

puisque $n \geq 5$: $\exists\ a_4 \neq a_5 \neq a_1, a_2, a_3$

Posons $\tau' = \tau(a_4\ a_5)$

τ' est pair : $\tau' \in A_n$.

et : $\tau' : \begin{cases} a_1 \longmapsto \tau(a_1) = i \\ a_2 \longmapsto j \\ a_3 \longmapsto k \\ m \longmapsto m \text{ on s'en fiche} \end{cases}$

$\Rightarrow \underbrace{\tau'(a_1\ a_2\ a_3)\tau'^{-1}}_{\in H} = (i\ j\ k)$.

Donc tout 3-cycle $(i\ j\ k)$ appartient à H.

II. $H = A_n$: puisque H contient tous les 3-cycles et toutes permutation paire est produit de 3-cycles. ∎

Thm : A_n est simple (et non abélien) pour tout $n \geq 5$.

preuve : Nous avons déjà montré que A_n est non abélien (même pour $n \geq 4$).

et que $\forall\ H \trianglelefteq A_n$, si $H \neq 1$ alors $H = A_n$.

∎

En fait : On peut démontrer que A_5 (groupe d'ordre $\frac{5!}{2} = 60$) est le plus petit groupe simple non abélien.