Exemples de sous-groupes distingués et de groupes quotients.

I. Sous-groupes distingués :

def : si H est un sous-groupe d'un groupe G, on note G/H l'ensemble des classes à droite de G relativement à H : $\{gH, g \in G\}$.

def : • un sous-groupe H de G est dit distingué dans G si $\forall g \in G$, $gHg^{-1} = H$

• H est dit caractéristique dans G si $\forall \varphi \in \mathrm{Aut}\, G$, $\varphi(H) = H$.

ex : $\{1\}$ et G sont caractéristiques, donc distingués dans G.

prop : si H est distingué dans G (on note $H \lhd G$), il existe une unique structure de groupe sur G/H tq $\pi : G \to G/H$ soit un morphisme de groupes.

prop : • si $f : G \to G'$ est un morphisme de groupes, et $N' \lhd G'$, alors $f^{-1}(N') \lhd G$. ($\mathrm{Ker} f \lhd G$).

• si $H \lhd G$, il existe $f : G \to G'$ tq $H = \mathrm{Ker} f$.

ex : • un sous-groupe d'un groupe abélien est distingué dans ce groupe.

• si G un groupe, $Z(G) := \{g \in G : \forall h \in G, gh = hg\}$, centre de G, est distingué dans G. ex : • $\forall n \geq 3$, $Z(\mathfrak{S}_n) = \{id\}$

• $\forall n \geq 1$, $Z(GL_n(K)) = \{\lambda . Id : \lambda \in K^\times\}$, $Z(SL_n(K)) = \{\lambda Id : \lambda^n = 1\}$

• le centre d'un p-groupe non trivial est $\neq \{1\}$.

• groupe dérivé : on note $D(G)$ le sous-groupe de G engendré par les commutateurs $[a,b] = aba^{-1}b^{-1}$, $a, b \in G$. Alors $D(G)$ est caractéristique dans G, et si $N \lhd G$, G/N abélien $\Leftrightarrow$ $D(G) \subseteq N$.

ex : $D(\mathfrak{S}_n) = \mathfrak{A}_n$, $D(\mathfrak{A}_n) = \mathfrak{A}_n$, $\forall n \geq 5$, $D(SL_n(K)) = SL_n(K)$ si $n \geq 3$ et K corps fini.

• normalisateur :

si H est un sous-groupe de G, $N_G(H) := \{g \in G : gHg^{-1} = H\}$. Alors $N_G(H)$ est le plus grand sous-groupe K de G tq $H \lhd K$.

• G groupe fini. On note p le plus petit facteur premier de $\# G$. Alors tout sous-groupe de G d'indice p est distingué dans G.

def-prop : si S est une partie de G, l'intersection des sous-groupes distingués de G contenant S est un sous-groupe distingué de S, appelé clôture normale de S.

rq : le groupe $\mathbb{H}$ des quaternions vérifie : tous les sous groupes de $\mathbb{H}$ sont distingués, mais $\mathbb{H}$ n'est pas abélien.

def : un groupe G est dit simple s'il n'admet pas de sous-groupe distingué non trivial.

ex : • un groupe abélien est simple ssi il est cyclique d'ordre premier.

Dev^t A. • $\forall n \neq 4$, $\mathfrak{A}_n$ est simple. Application : $\forall n \neq 6$, $\mathrm{Aut}(\mathfrak{S}_n) \simeq \mathfrak{S}_n$.

• $PSL(n, k)$ est simple pour k corps fini, sauf $n = 2$ et $k = \mathbb{F}_2$ ou $\mathbb{F}_3$.

• $PSO(n, \mathbb{R})$ est simple pour $n \geq 5$.

- un outil pour montrer qu'un groupe n'est pas simple : les théorèmes de Sylow :
Soit G un groupe fini d'ordre $n = p^\alpha m$, $p \nmid m$, p premier.
Alors G admet un sous-groupe d'ordre p^α. (appelé un p-Sylow de G)
De plus, • tous les p-Sylow de G sont conjugués.
• le nombre k de p-Sylow de G vérifie $k \equiv 1\ [p]$ et $k \mid m$.
Ainsi, si $k = 1$, le p-Sylow est distingué dans G.
- rq : la relation $\triangleleft$ "n'est pas transitive" : $\{1, (12)(34)\} \triangleleft \{1, (12)(34), (13)(24), (14)(23)\} \triangleleft \mathfrak{A}_4$
- Thm (Feit–Thompson) : Tout groupe fini simple non-cyclique est d'ordre pair.
- groupes simples d'ordre ≤ 600 : $\mathfrak{A}_5$ (60), $PSL_2(\mathbb{F}_7)$ (168), $\mathfrak{A}_6$ (360), $PSL_2(\mathbb{F}_{11})$ (504)
non cycliques.

II. Groupes quotients :

- ex : $PGL_n(K) := GL_n(K)/K^\times$, $PSL_n(K) := SL_n(K)/\mu_n(K)$, $\mathbb{T}^n := \mathbb{R}^n/\mathbb{Z}^n$
- théorèmes d'isomorphisme :
  1) $f : G \to G'$ morphisme. Alors $\mathrm{Im} f \simeq G/\mathrm{Ker} f$. ex : $GL_n(K)/SL_n(K) \simeq K^\times$
  2) $K \subset H \subset G$, $K \triangleleft G$, $H \triangleleft G$.
  Alors $H/K \triangleleft G/K$ et $G/H \simeq (G/K)/(H/K)$
  3) H, K deux sous-groupes de G.
  si $H \triangleleft G$, alors HK est un sous-groupe et $K/H\cap K \simeq HK/H$.
  ex : si tout élément de k admet une racine n-ième, $PSL_n(k) \simeq PGL_n(k)$.
- sous groupes : G groupe, $H \triangleleft G$.
On a une bijection : $\{$ss-groupes de G contenant $H\} \xrightarrow{\sim} \{$ss-groupes de $G/H\}$
$K \longmapsto K/H$.
- théorème de factorisation : $f : G \to G'$ morphisme, $H \triangleleft G$. si $H \subseteq \mathrm{Ker} f$,
il existe un unique morphisme $\bar{f} : G/H \to G'$ tq
$$\begin{tikzcd} G \arrow[r] \arrow[dr, "f"'] & G/H \arrow[d, "\bar{f}"] \\ & G' \end{tikzcd}$$
commute.
- suite exacte courte : si $H \triangleleft G$, on a la suite exacte $1 \to H \to G \to G/H \to 1$
- produit semi-direct :
  * def : N, H deux groupes, $\varphi : H \to \mathrm{Aut}\, N$ morphisme.
  on définit le produit semi-direct $G := N \rtimes_\varphi H$ comme le groupe d'ensemble de base $N \times H$ et de loi : $(n, h).(n', h') := (n.\varphi(h)n', hh')$
  * prop : on a $N \triangleleft G$ et $1 \to N \to G \rightleftarrows H \to 1$ suite exacte scindée.
  * caractérisations :
  ① N, H sous-groupes de G. Si $N \cap H = \{1\}$, $NH = G$ et $N \triangleleft G$, alors $G \simeq N \rtimes H$
  ② si on a une suite exacte scindée $1 \to N \to G \to H \to 1$, alors $G \simeq N \rtimes H$
  * ex : $\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$
  $GL_n(K) \simeq SL_n(K) \rtimes K^\times$
  $\mathbb{D}_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ (groupe diédral).

$\boxed{\text{Dév}^t\ B}$ [* classification des groupes d'ordre 8
* classification des groupes d'ordre pq

• groupe défini par générateurs et relations:

On note $\mathcal{L}$ un alphabet non-vide et $\hat{\mathcal{L}}$ le groupe libre construit sur $\mathcal{L}$.
On se donne $\mathcal{G} \subseteq \hat{\mathcal{L}}$, un ensemble de "relations" entre les lettres de $\mathcal{L}$. On note $\overline{\mathcal{G}}$ la clôture normale de $\mathcal{G}$ dans $\hat{\mathcal{L}}$.

alors $\hat{\mathcal{L}}/\overline{\mathcal{G}}$ est appelé le groupe défini par les générateurs $g \in \mathcal{L}$ et les relations $\{\mu = e,\ \mu \in \mathcal{G}\}$.

ex: • $\mathcal{L} = \{a\}$, $\mathcal{G} = \{a^n\}$, alors on obtient le groupe cyclique d'ordre n.
• $\mathcal{L} = \{a, b\}$, $\mathcal{G} = \{a^n, b^2, (ab)^2\} \longrightarrow$ on obtient un groupe $\simeq D_n$.
• Présentation de $\mathfrak{S}_n$

• théorème (Burnside): G groupe fini, S un p-Sylow de G, contenu ds le centre de son normalisateur. Alors $\exists\ H \triangleleft G$ tq $S \simeq G/H$.

• application: G fini simple non-cyclique, d'ordre N. Alors soit $12 \mid N$, soit le plus petit facteur premier de N est au moins au cube.

• théorie de Galois:

* def: $K \subset L$ deux corps. $K \subset L$ est dite galoisienne si $K \subset L$ est finie, normale et séparable (i.e le polynôme minimal sur K de $x \in L$ est scindé à racines simples dans L).
On note $\mathrm{Gal}(L|K) := \{\sigma : L \to L$ morphisme de corps, $\sigma|_K = id_K\}$, d'ordre $[L:K]$.

* théorème: si $K \subset L$ est galoisienne, on a une bijection:

$$\{\text{extensions intermédiaires } K \subset F \subset L\} \xrightarrow{\sim} \{\text{ss groupes de } \mathrm{Gal}(L|K)\}$$
$$F \longmapsto \mathrm{Gal}(L|F)$$
$$L^H := \{x \in L : \sigma x = x, \forall \sigma \in H\} \longleftarrow H$$

* prop: $K \subset L \subset M$, $K \subset M$ galoisienne. $G := \mathrm{Gal}(M|K)$, $H := \mathrm{Gal}(M|L)$.
$L \subset M$ est galoisienne, et: $K \subset L$ galoisienne $\Leftrightarrow H \triangleleft G$ (auquel cas $\mathrm{Gal}(L|K) \simeq G/H$).

III. groupes résolubles, groupes nilpotents:

def: G groupe. Une suite de décomposition de G est une suite finie $(G_i)_{0 \le i \le n}$ de ss groupes tq: $G_0 = G \triangleright G_1 \triangleright \dots \triangleright G_n = \{1\}$. Les G_i/G_{i+1} sont appelés quotients de la suite.

def: G est dit résoluble si G admet une suite de composition à quotients abéliens.
G est dit nilpotent si G admet une telle suite, et $G_i \triangleleft G$, $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$ (i.e $[G_i, G] \subseteq G_{i+1}$).

def: G groupe. On note $D^n(G) = [D^{n-1}(G), D^{n-1}(G)]$ et $C^n(G) = [C^{n-1}(G), G]$, $C^1(G) = D(G)$

prop: G résoluble (resp. nilpotent) $\Leftrightarrow \exists n \geq 1$, $D^n(G) = \{1\}$ (resp $C^n(G) = \{1\}$).

prop: un p-groupe (fini) est nilpotent, et admet une suite de composition à quotient d'ordre p.

Thm: (Burnside) p, q premiers. Tout groupe d'ordre $p^\alpha q^\beta$ est résoluble.

ex: $\mathfrak{S}_3$ est résoluble, non nilpotent. Un groupe abélien est nilpotent.

Application: polygônes réguliers constructibles:

def: • $\alpha \in \mathbb{R}$ est dit constructible si c'est une coordonnées d'un point constructible.
• le polygône à n côtés est constructible si $\cos\left(\frac{2\pi}{n}\right)$ est constructible.

$\boxed{\text{Dev}^t\ C}$ Thm: le polygône régulier à n côtés est constructible ssi $n = 2^r p_1 \cdots p_s$, $p_i = 2^{2^{r_i}} + 1$ premiers distincts.