Planche TD3

Exo 1 Donner la liste des sous-groupes de S_3 en précisant les sous-groupes normaux.

Soit $H \subset S_3$ sous-groupe. D'après le 1er corollaire au th. de Lagrange, $|H|$ est un diviseur de $|S_3| = 6$, donc

$$|H| \in \{1, 2, 3, 6\}$$

Cas 1) $|H| = 1$. Dans ce cas $H = \{e\}$

Cas 2) $|H| = 6$. Dans ce cas $H = S_3$

Cas 3) $\left.\begin{array}{l} |H| = 2 \\ 2 \text{ est un nombre premier} \end{array}\right\} \xrightarrow[\text{corollaire}]{3me}$ H est un sous-groupe cyclique d'ordre 2,

donc $H = \langle \sigma \rangle$ où $ord(\sigma) = 2$, donc $\sigma \in \{(1\,2), (1\,3), (2\,3)\}$

$(1\,2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\langle (1\,2) \rangle = \{ id, (1\,2) \}$

$\langle (2,3) \rangle = \{ id, (2\,3) \}$

$\langle (1\,3) \rangle = \{ id, (1\,3) \}$

des sous-groupes d'ordre 2 sont

$\{ id, (1\,2) \}$

$\{ id, (2\,3) \}$

$\{ id, (1\,3) \}$

Cas 4) $\left.\begin{array}{l} |H| = 3 \\ 3 \text{ nombre premier} \end{array}\right\} \xrightarrow[\text{corollaire}]{\text{3me}}$ H est cyclique d'ordre 3,

donc $H = \langle \sigma \rangle$, où $\sigma \in S_3$ est un élément d'ordre 3

Donc $\sigma \in \{ (1\,2\,3), (1\,3\,2) \}$

$\langle (1\,2\,3) \rangle = \{ id, (1\,2\,3), (1\,3\,2) \} = \langle (1\,3\,2) \rangle$

$$(1\,2\,3)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2)$$

$\langle 1\,3\,2 \rangle = \{ id, (1\,3\,2), (1\,2\,3) \}$

S_3 admet un seul sous-groupe d'ordre 3, à savoir $\{ id, (1\,2\,3), (1\,3\,2) \}$

on a utilisé:

$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad , \quad (1\ 2\ 3)^2 = (1\ 3\ 2)$$

$$(1\ 3\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad (1\ 3\ 2)^2 = (1\ 2\ 3)$$

$\{id\}$, S_3 sont normaux.

$\{id, (1\ 2\ 3), (1\ 3\ 2)\} = A_3$ sous-groupe normal, d'après le cours.

$$A_n := \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\} = \ker(\varepsilon : S_n \longrightarrow \{\pm 1\})$$

les sous-groupes d'ordre 2 ne sont pas normaux. En effet, par exemple soit $H = \langle (1\ 2) \rangle = \{id, (1\ 2)\}$

$$(1\ 3)(1\ 2)(1\ 3)^{-1} = (1\ 3)(1\ 2)(1\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3) \notin H$$

$h = (1\ 2) \in H$ Donc H n'est pas normal

$x = (1\ 3) \in S_3$ De même pour les autres sous-groupes d'ordre 2

Exo 2 Soit $H \subset \mathbb{Z}$ un sous-groupe nontrivial, i.e. $H \neq \{0\}$

1. M.q. $H \cap \mathbb{N}^* \neq \emptyset$

$\{0\} \subsetneq H \Longrightarrow \exists k \in H$ t.q $k \neq 0$.

inclusion stricte

Cas a) $k > 0$. Alors $k \in \mathbb{N}^*$ et $k \in H$ donc $k \in H \cap \mathbb{N}^*$

Cas b) $k < 0$.

$\left.\begin{array}{l} k \in H \\ H \text{ est un sous-groupe de } \mathbb{Z} \end{array}\right\} \Longrightarrow -k \in H$

$\left.\begin{array}{l} \text{Mais } -k \in \mathbb{N}^* \\ -k \in H \end{array}\right\} \Longrightarrow -k \in H \cap \mathbb{N}^*$

Dans les deux cas on obtient $H \cap \mathbb{N}^* \neq \emptyset$

2. En utilisant le TDE montrer que $H = d\mathbb{Z}$, où $d = \min(H \cap \mathbb{N}^*)$.

existe, parce que $H \cap \mathbb{N}^* \neq \emptyset$.

On va démontrer l'égalité $H = d\mathbb{Z}$ par double inclusion:

(i) M.q. $d\mathbb{Z} \subset H$. En effet $d \in H \cap \mathbb{N}^*$, donc $d \in H$

Puisque $d \in H$, tout élément de la forme kd (avec $k \in \mathbb{Z}$) sera élément de H. Donc $d\mathbb{Z} \subset H$

(ii) M.q. $H \subset d\mathbb{Z}$.

Soit $k \in H$. On va montrer que $k \in d\mathbb{Z}$. De manière équivalente on va montrer que le reste r de la DE de k par d est 0. Par l'absurde : supposons $r > 0$, donc $r \in \mathbb{N}^*$. Mais

$k = qd + r$ (où $q \in \mathbb{Z}$ et $r < d$), donc $r = k - qd \in H$ parce que $k \in H$ et $qd \in H$ (parce que $d \in H$).

En conclusion
$r \in H$, $r \in \mathbb{N}^*$ et $r < d$,
donc $r \in H \cap \mathbb{N}^*$ et $r < d$, ce qui contredit la définition de d.

Conclusion : le reste de la DE de k par d est 0, donc k est divisible par d, donc $k \in d\mathbb{Z}$.

En déduire :

<u>Proposition</u> : Tout sous-groupe de $\mathbb{Z}$ est cyclique.

<u>Dém.</u> Soit $H \subset \mathbb{Z}$ sous-groupe. Si $H \neq \{0\}$ alors $H = d\mathbb{Z}$, où $d := \min(H \cap \mathbb{N}^*)$ d'après Q2.

$$d\mathbb{Z} = \langle d \rangle$$

Si $H = \{0\}$, alors $H = \langle 0 \rangle$.

<u>Exo 3.</u> Soient $(G, \cdot)$ un groupe, $H, H' \subset G$ sous-groupes

1. M. q. $H \cap H'$ est un sous-groupe de G.

1. M. q. $e \in H \cap H'$. En effet

$$\left.\begin{array}{l} H \subset G \text{ sous-groupe} \Longrightarrow e \in H \\ H' \subset G \text{ sous-groupe} \Longrightarrow e \in H' \end{array}\right\} \Longrightarrow e \in H \cap H'$$

2. M.q. $(x \in H \cap H') \wedge (y \in H \cap H') \Longrightarrow x \cdot y \in H \cap H'$

Soient $x \in H \cap H'$, $y \in H \cap H'$. On a donc

$x \in H$ et $y \in H$, donc (H sous-groupe) $x \cdot y \in H$

$x \in H'$ et $y \in H'$, donc (H' sous-groupe) $x \cdot y \in H'$

Conclusion $x \cdot y \in H \cap H'$

3. M.q $(x \in H \cap H') \Longrightarrow x^{-1} \in H \cap H'$.

Exercice.

2. Soit $(A,+)$ un groupe abélien, $H, H' \subset A$ sous-groupes

M.q. $H + H' := \{x + x' \mid x \in H, x' \in H'\}$ est un sous-groupe de A

On peut utiliser l'exo 12 de la planche TD2

Puisque $(A,+)$ est abélien, on a $H+H' = H'+H$, donc, d'après l'exo 12 TD2, $H+H'$ est un sous-groupe.

Démonstration directe :

1. $e \in H+H'$: $\left.\begin{array}{l} e\in H \\ e \in H' \end{array}\right\} \Longrightarrow e = e+e \in H+H'$

2. $x, y \in H+H' \Longrightarrow x+y \in H+H'$.

$x \in H+H' \Longrightarrow \exists\, u \in H\ \exists\, u' \in H',\ x = u+u'$

$y \in H+H' \Longrightarrow \exists\, v \in H\ \exists\, v' \in H',\ y = v+v'$

$$x+y = (u+u')+(v+v') \underset{\text{comm}}{\overset{+\text{ est}}{=}} \underbrace{(u+v)}_{\in H} + \underbrace{(u'+v')}_{\in H'}$$

Donc $x+y \in H+H'$

3. Soit $x \in H+H'$. M.q $-x \in H+H'$

$x \in H+H' \Longrightarrow \exists u \in H \; \exists u' \in H', \; x = u+u'$

$-x = (-u') + (-u) \underset{\text{comm}}{\overset{+\text{est}}{=\!=}} \underbrace{(-u)}_{\underset{H}{\in}} + \underbrace{(-u')}_{\underset{H'}{\in}} \in H+H'.$

Rappel $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$

Exo 4 Soient $m, n \in \mathbb{N}^*$. M.q

1. $m\mathbb{Z} + n\mathbb{Z} = \text{pgcd}(m,n)\mathbb{Z}$.

Soit $d := \text{pgcd}(m,n)$. Posons $m' := \frac{m}{d}$, $n' := \frac{n}{d}$

On démontre par double inclusion $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$

(1) $m\mathbb{Z} + n\mathbb{Z} \subset d\mathbb{Z}$. Soit $k \in m\mathbb{Z} + n\mathbb{Z}$, i.e. $\exists u, v \in \mathbb{Z}$

t.q $k = um + vn = um'd + vn'd = (um' + vn')d \in d\mathbb{Z}$

(ii) $d\mathbb{Z} \subset m\mathbb{Z} + n\mathbb{Z}$

Soit $k \in d\mathbb{Z}$, donc $k = dl$ avec $l \in \mathbb{Z}$.

D'après l'égalité de Bézout, il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$,

$d = um + vn$. On a donc

$$k = (um + vn)l = \underbrace{(ul)m}_{\in m\mathbb{Z}} + \underbrace{(vl)n}_{\in n\mathbb{Z}} \in m\mathbb{Z} + n\mathbb{Z}$$

2. $m\mathbb{Z} \cap n\mathbb{Z} = \text{ppcm}(m, n)\mathbb{Z}$

Posons $\mu := \text{ppcm}(m, n)$. M.q. $m\mathbb{Z} \cap n\mathbb{Z} = \mu\mathbb{Z}$ par double inclusion. μ est multiple commun de m et n donc $\mu = am = bn$, où $a, b \in \mathbb{N}^*$

(i) $m\mathbb{Z} \cap n\mathbb{Z} \subset \mu\mathbb{Z}$. Soit $k \in m\mathbb{Z} \cap n\mathbb{Z}$. Donc k est un multiple de m et un multiple de n, donc

k est un multiple commun de m et n.

D'après le cours $\mu \mid k$, donc $k \in \mathbb{Z}\mu$

(ii) $\mu\mathbb{Z} \subset m\mathbb{Z} \cap n\mathbb{Z}$

Soit $k \in \mu\mathbb{Z}$, donc $k = \mu l$ avec $l \in \mathbb{Z}$. Mais $\mu = am = bn$, donc $k = (al)m \in m\mathbb{Z}$ et $k = (bl)n \in n\mathbb{Z}$, donc

$k \in m\mathbb{Z} \cap n\mathbb{Z}$

3. M.q $m\mathbb{Z} \subset n\mathbb{Z}$ ssi $n \mid m$ et, si c'est le cas

$$n\mathbb{Z}/_{m\mathbb{Z}} \simeq \mathbb{Z}_d, \text{ où } d = m/n$$

(i) M.q $m\mathbb{Z} \subset n\mathbb{Z} \Longrightarrow n \mid m$. Supposons $m\mathbb{Z} \subset n\mathbb{Z}$

Mais $\left.\begin{array}{l} m = m\cdot 1 \in m\mathbb{Z} \\ m\mathbb{Z} \subset n\mathbb{Z} \end{array}\right\} \Longrightarrow m \in n\mathbb{Z}$, donc m est un multiple de n.

(ii) $n \mid m \Longrightarrow m\mathbb{Z} \subset n\mathbb{Z}$.

Supposons $n \mid m$, donc il existe $k \in \mathbb{N}^*$, $m = kn$

M.q. $m\mathbb{Z} \subset n\mathbb{Z}$

Soit $x \in m\mathbb{Z}$. Il existe $\ell \in \mathbb{Z}$, $x = m\ell$.

Donc $x = kn\ell = \underbrace{(k\ell)}_{\in\mathbb{Z}} n \in n\mathbb{Z}$.

Supposons $n \mid m$ (c'est à dire $m\mathbb{Z} \subset n\mathbb{Z}$) et m.q.

$n\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_d$, où $d = \frac{m}{n}$.

Soit $F : \mathbb{Z} \longrightarrow n\mathbb{Z}$ définie par $F(x) = nx$

<u>Exercice</u> Mq. F est un isomorphisme de groupe.

Soit $q : n\mathbb{Z} \longrightarrow {}^{n\mathbb{Z}}/_{m\mathbb{Z}}$ l'<u>épimorphisme</u> canonique

et soit $f : q \circ F : \mathbb{Z} \longrightarrow {}^{n\mathbb{Z}}/_{m\mathbb{Z}}$

f est un épimorphisme (composition d'épimorphismes)

$$\ker(f) = \{x \in \mathbb{Z} \mid f(x) = \underbrace{[0]_{m\mathbb{Z}}}\} = \{x \in \mathbb{Z} \mid [nx]_{m\mathbb{Z}} = [0]_{m\mathbb{Z}}\} =$$

$$= \{x \in \mathbb{Z} \mid nx \in m\mathbb{Z}\} = \{x \in \mathbb{Z} \mid nx \in dn\mathbb{Z}\} =$$

$$= \{x \in \mathbb{Z} \mid x \in d\mathbb{Z}\} = d\mathbb{Z}$$

Le 1er th. d'isomorphisme nous donne un isomorphisme

$$\begin{array}{ccc} \mathbb{Z}/_{\ker f} & \xrightarrow{\varphi} & \mathrm{im}(f) \\ \| & & \| \\ \mathbb{Z}/d\mathbb{Z} & & n\mathbb{Z}/m\mathbb{Z} \\ \| & & \\ \mathbb{Z}_d & & \end{array}$$

donné par

$$\varphi([x]_d) = [f(x)]_{m\mathbb{Z}}$$

Exo 8 À étudier

Exo 11 À étudier.

Exo 13

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 2 & 1 \end{pmatrix} \in S_6.$$

1) Trouver une décomposition de σ en produit de cycles disjoints.

$\sigma = (1\ 3\ 6)(2\ 4\ 5)$

Decomposition de σ en produit de transpositions

$$(n_1\ n_2\ n_3) = (n_1\ n_3)(n_1\ n_2)$$

$$(1\ 3\ 6) = (1\ 6)(1\ 3)\ ;\quad (2\ 4\ 5) = (2\ 5)(2\ 4)$$

$$\sigma = (1\ 6)(1\ 3)(2\ 5)(2\ 4)$$

2. $\operatorname{sign}(\sigma) = \operatorname{sign}(1\ 3\ 6)\operatorname{sign}(2\ 4\ 5) = (-1)^{3-1}(-1)^{3-1} = 1$

$\operatorname{sign}(\sigma) = (-1)^4 = 1$

3. $\sigma = \underbrace{(1\ 3\ 6)}_{3\text{-cycle}}\ \underbrace{(2\ 4\ 5)}_{3\text{-cycle}}$ $\quad \operatorname{ord}(\sigma) = \operatorname{ppcm}(3,3) = 3$

$\sigma^2 = (1\ 3\ 6)^2(2\ 4\ 5)^2.$

$$\langle\sigma\rangle = \{id, \sigma, \sigma^2\} = \{id, \sigma, (1\ 6\ 3)(2\ 5\ 4)\}$$