<u>Exo 11</u> Mettre en évidence les inclusions de sous-groupe dans l'exo 5.

$SL(n,\mathbb{R}) := \{A \in M_{n,n}(\mathbb{R}) \mid \det A = 1\}$

$$\underbrace{U_n}_{=\{z\in\mathbb{C} \mid z^n=1\}} \subset \underbrace{U}_{=\{z\in\mathbb{C} \mid |z|=1\}} \subset \mathbb{C}^*$$

$$SL(n,\mathbb{R}) \subset GL(n,\mathbb{R})$$

sous-groupe normal

$Iso(X) \subset S(X)$, où $(X,d)$ est un espace métrique

le groupe des isométries de $(X,d)$

le groupe symétrique de $X$

À continuer !

$$\{\pm 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$$

<u>Exo 12</u> $(G,\cdot)$ groupe, $A, B \subset G$ sous-groupes.

$A\cdot B := \{a\cdot b \mid a\in A,\ b\in B\}$

1 M.q $A\cdot B$ est un sous-groupe de $G$ ssi $A\cdot B = B\cdot A$

1a) $A\cdot B = B\cdot A \implies A\cdot B$ est un sous-groupe.

Supposons $\boxed{A\cdot B = B\cdot A}$ et m.q. $A\cdot B$ est un sous-groupe :

1. M.q. $e \in A\cdot B$ :

On a $e\in A$, $e\in B$, donc $e = \overset{\in A}{e}\cdot \overset{\in B}{e} \in A\cdot B$

2. M.q $\forall x,y \in A\cdot B$, $x\cdot y \in A\cdot B$

Soient $x,y \in A\cdot B$.

$x \in A\cdot B \implies \exists (a,b)\in A\times B,\ x = a\cdot b$

$y \in A\cdot B \implies \exists (\alpha,\beta)\in A\times B,\ y = \alpha\cdot\beta$

Mais $A\cdot B = B\cdot A$ donc $\exists (\alpha_1,\beta_1) \in A\times B,\ \alpha\cdot\beta = \beta_1\cdot\alpha_1$

$$x \cdot y = (a \cdot b) \cdot (\beta_1 \cdot \alpha_1) = a \cdot \underbrace{(b \cdot \beta_1)}_{\substack{\| \\ b_1 \in B}} \cdot \alpha_1 = a \cdot \underbrace{(b_1 \cdot \alpha_1)}_{\substack{\cap \\ B \cdot A = A \cdot B}}$$

$$\exists (\alpha_2, \beta_2) \in A \times B \quad t.q \quad b_1 \cdot \alpha_1 = \alpha_2 \cdot \beta_2$$

$$x \cdot y = \underbrace{(a \cdot \alpha_2)}_{\substack{\cap \\ A}} \cdot \underbrace{\beta_2}_{\substack{\cap \\ B}} \in A \cdot B$$

3. $\forall\, x \in A \cdot B,\ x^{-1} \in A \cdot B$

$$x \in A \cdot B \implies \exists (a, b) \in A \times B,\ x = a \cdot b$$

$$x^{-1} = \underbrace{b^{-1}}_{\substack{\cap \\ B}} \cdot \underbrace{a^{-1}}_{\substack{\cap \\ A}} \in B \cdot A = A \cdot B$$

$\longrightarrow$

1.b Réciproquement supposons que $A \cdot B$ est un sous-groupe.

Mq. $A \cdot B = B \cdot A$ c'est à dire $A \cdot B \subset B \cdot A$ et $B \cdot A \subset A \cdot B$

$B \cdot A \subset A \cdot B$ : Soit $x \in B \cdot A$, i.e $\exists (a, b) \in A \times B$, $x = b \cdot a$

$$\left.\begin{array}{l} \left.\begin{array}{l} a \in A \\ A \text{ sous-groupe} \end{array}\right\} \Rightarrow a^{-1} \in A \\ \left.\begin{array}{l} b \in B \\ B \text{ sous-groupe} \end{array}\right\} \Rightarrow b^{-1} \in B \end{array}\right\} \Rightarrow \left.\begin{array}{l} a^{-1} \cdot b^{-1} \in A \cdot B \\ A \cdot B \text{ sous-groupe} \end{array}\right\} \Rightarrow$$

$$\Rightarrow \underbrace{(a^{-1} \cdot b^{-1})^{-1}}_{\substack{\parallel \\ x = b \cdot a}} \in A \cdot B$$

$A \cdot B \subset B \cdot A$ :

Soit $x \in A \cdot B$, i.e.

$\exists (a, b) \in A \times B$, $x = a \cdot b$

$$\left.\begin{array}{l} b \in B \Rightarrow b^{-1} \in B \\ a \in A \Rightarrow a^{-1} \in A \end{array}\right| \Rightarrow b^{-1} \cdot a^{-1} \in B \cdot A$$

$\cap$

$A \cdot B$

Donc $b^{-1} \cdot a^{-1} \in B \cdot A \subset A \cdot B$

déjà démontrée

$\exists (\alpha, \beta) \in A \times B, \quad b^{-1} \cdot a^{-1} = \alpha \cdot \beta$

$\Downarrow$

$x = a \cdot b = \underbrace{\beta^{-1}}_{\in B} \cdot \underbrace{\alpha^{-1}}_{\in A} \in B \cdot A$

2. Supposons $A, B$ sont finis et $A \cap B = \{e\}$

M.q $A \cdot B$ est fini et $|A \cdot B| = |A| \cdot |B|$

Soit $f : A \times B \longrightarrow A \cdot B$, définie par $f(a, b) := a \cdot b$

$f$ est surjective. En effet, par la définition de $A \cdot B$, tout élément de $A \cdot B$ s'écrit sous la forme $\underset{\substack{\| \\ f(a,b)}}{a \cdot b}$

pour un couple $(\underset{\substack{\cap \\ A}}{a}, \underset{\substack{\cap \\ B}}{b}) \in A \times B$

M.q $f$ est injective : Soit $(a,b),(\alpha,\beta) \in A \times B$ t.q

$f(a,b) = f(\alpha,\beta)$ . À démontrer : $(a,b) = (\alpha,\beta)$

$$\Updownarrow$$

$$a \cdot b = \alpha \cdot \beta \underset{\beta^{-1}(\ )}{\Longrightarrow} \underbrace{\alpha^{-1}}(a \cdot b) = \beta \underset{(\ )b^{-1}}{\Longrightarrow} \underbrace{\alpha^{-1} \cdot a}_{\substack{\cap \\ A}} = \underbrace{\beta \cdot b^{-1}}_{\substack{\cap \\ B}}$$

Donc $\underset{\substack{\| \\ \beta \cdot b^{-1}}}{\alpha^{-1} \cdot a} \in A \cap B = \{e\}$

$\beta \cdot b^{-1} \in A \cap B = \{e\}$

Donc $\alpha^{-1} \cdot a = e \Rightarrow a = \alpha$

$\beta\, b^{-1} = e \Rightarrow \beta = b$

Conclusion : $(a,b) = (\alpha,\beta)$.

Donc $f$ est bijective, donc

$$|A \times B| = |A \cdot B|$$
$$\|$$
$$|A| \cdot |B|$$

3. Supposons : $G$ est abélien, $A \cap B = \{e\}$

Soit $f : A \times B \longrightarrow A \cdot B$, $f(a, b) = a \cdot b$

$f$ est un isomorphisme.

Il suffit de montrer que $f$ est un homomorphisme

Soient $(a, b), (\alpha, \beta) \in A \times B$.

$$f((a, b) \cdot (\alpha, \beta)) = f(a \cdot \alpha, b \cdot \beta) = a \cdot \alpha \cdot b \cdot \beta \underset{ab}{\overset{G \text{ est}}{=\!=}} \overbrace{a \cdot b}^{f(a,b)} \cdot \overbrace{\alpha \cdot \beta}^{f(\alpha,\beta)} =$$

$$= f(a, b) \cdot f(\alpha, \beta)$$

Exo 14. a) Déterminer $\mathbb{Z}_{10}^{\times}$ et écrire la table de ce groupe. b) Démontrer que $(\mathbb{Z}_{10}^{\times}, \cdot)$ est un groupe cyclique. c) Est-ce que $(\mathbb{Z}_{30}^{\times}, \cdot)$ est cyclique ?

a) $\mathbb{Z}_{10}^{\times} = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$

Rappel : Soit $k \in \mathbb{Z}$.
$[k]_n \in \mathbb{Z}_n^{\times} \Leftrightarrow \mathrm{pgcd}(k, n) = 1$

| $\cdot$ | $[1]$ | $[3]$ | $[7]$ | $[9]$ |
|---|---|---|---|---|
| $[1]$ | $[1]$ | $[3]$ | $[7]$ | $[9]$ |
| $[3]$ | $[3]$ | $[9]$ | $[1]$ | $[7]$ |
| $[7]$ | $[7]$ | $[1]$ | $[9]$ | $[3]$ |
| $[9]$ | $[9]$ | $[7]$ | $[3]$ | $[1]$ |

b) $\mathrm{ord}([1]) = 1 \qquad \langle [1] \rangle = \{[1]\}$

$\mathrm{ord}([3]) = 4 \qquad \langle [3] \rangle = \underbrace{\{[1], [3], [9], [7]\}}_{\mathbb{Z}_{10}^{\times}}$

$$\boxed{\text{Rappel. Si } \mathrm{ord}(x) = k \quad \langle x \rangle = \{e, x \ldots x^{k-1}\}}$$

$\mathbb{Z}_{10}^{\times}$ est cyclique, $[3]$ est un générateur de ce groupe.

$\text{ord}([7]) = 4 \qquad \langle [7] \rangle = \langle [1], [7], \underset{[-1]}{\underset{\shortparallel}{[9]}}, [3] \rangle$

$[7]$ est un générateur de $\mathbb{Z}_{10}^{\times}$

$\text{ord}([9]) = 2 \qquad \langle [9] \rangle = \{ [1], [9] \}$

c) $\mathbb{Z}_{30}^{\times} = \{ [1], [7], [11], [13], [17], [19], [23], [29] \}$

Voir l'exo 2 pour la table de ce groupe.

$\langle [1] \rangle = \{ [1] \}$, $\langle [7] \rangle = \{ [1], [7], [19], [13] \}$, $\text{ord}([7]) = 4$

$\langle [11] \rangle = \{ [1], [11] \}$, $\text{ord}([11]) = 2$, $\langle [13] \rangle = \{ [1], [13], [19], [7] \}$

$[11]^2 = [121] = [1]$ $\qquad$ $\text{ord}([13]) = 4$

$\langle [17] \rangle = \{ [1], [17], [19], [23] \}$ $\qquad$ $\langle [19] \rangle = \{ [1], [19] \}$

$\text{ord}([17]) = 4$ $\qquad$ $\text{ord}[19] = 2$

$\langle [23] \rangle = \{[1], [23], [19], [17]\}$ $\quad \mathrm{ord}([23]) = 4$

$\langle [29] \rangle = \{[1], [29]\}$ $\quad \mathrm{ord}([29]) = 2$

$\mathbb{Z}_{30}^{\times}$ ne contient aucun élément d'ordre 8,
donc n'est pas un groupe cyclique

Autre argument : $\mathbb{Z}_{30}^{\times}$ ne coïncide avec aucun sous-groupe cyclique

Remarque $\quad 30 = 5 \cdot 6 \quad \mathrm{pgcd}(5,6) = 1$

D'après la version multiplicative du théorème
chinois nous avons un isomorphisme :

$\mathbb{Z}_{30}^{\times} \xrightarrow{h} \mathbb{Z}_5^{\times} \times \mathbb{Z}_6^{\times}$ donné par

$$h([k]_{30}) = ([k]_5, [k]_6) \in \underbrace{\mathbb{Z}_5^\times}_{\text{cyclique d'ordre 4}} \times \underbrace{\mathbb{Z}_6^\times}_{\text{cyclique d'ordre 2}}$$

$$\mathbb{Z}_5^\times = \{[1]_5, [2]_5, [3]_5, [4]_5\}$$

$$\mathbb{Z}_6^\times = \{[1]_6, [5]_6\}$$

$$(\mathbb{Z}_5^\times, \cdot) \simeq (\mathbb{Z}_4, +)$$

$$(\mathbb{Z}_6^\times, \cdot) \simeq (\mathbb{Z}_2, +)$$

$$\varphi : (\mathbb{Z}_4, +) \xrightarrow{\simeq} (\mathbb{Z}_5^\times, \cdot)$$

$$\psi : (\mathbb{Z}_2, +) \xrightarrow{\simeq} (\mathbb{Z}_6^\times, \cdot)$$

$$\begin{array}{ccc}
\boxed{\mathbb{Z}_{30}^\times} & & \\
\simeq \downarrow h & & \\
\mathbb{Z}_5^\times \times \mathbb{Z}_6^\times & \xleftarrow{\simeq} & \mathbb{Z}_4 \times \mathbb{Z}_2 \\
(\varphi([k]_4), \psi([\ell]_2)) & \longleftarrow & ([k]_4, [\ell]_2)
\end{array}$$

Rappel

Soit $x \in G$ un element d'ordre $n$

Alors $g_x : \mathbb{Z}_n \longrightarrow \langle x \rangle$ defini par

$g_x([k]_n) = x^k$ est un isomorphisme

Dans notre cas $[2]_5$ est un generateur de $\mathbb{Z}_5^{\times}$

en posant $x = [2]_5$ on obtient un

isomorphisme $\varphi = g_x : (\mathbb{Z}_4, +) \xrightarrow{\simeq} (\mathbb{Z}_5^{\times}, \cdot)$

$$\varphi([k]_4) = x^k = [2]_5^k = [2^k]_5 \quad 0 \leq k \leq 3$$

$$\psi([\ell]_2) = y^\ell = [5]_6^\ell = [5^\ell]_6 \quad 0 \leq \ell \leq 1$$