DM Correction

Exercice 3

5) Prenons $p=2$, $q=3$

$(\mathfrak{S}_3, \circ)$ groupe de cardinal 2×3

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

$$(1\,3)\circ(1\,2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$ Donc G non-commutatif

6) Soit G un groupe d'ordre $p\times q$ (p, q premiers distincts) commutatif.

Théorème de Cauchy : $\exists (x,y) \in G$ tel que $\mathrm{ord}(x)=p$, $\mathrm{ord}(y)=q$

Montrons que $\mathrm{ord}(x*y)=pq$

$$(x*y)^{pq} = \underbrace{(x^p)^q}_{e_G} * \underbrace{(y^q)^p}_{e_G} = e_G \text{, donc } \mathrm{ord}(x*y) \mid pq$$

~~Soit $n\in\mathbb{N}^*$ tel que $(x*y)^n = e_G$. $n \mid q$~~

i.e $\mathrm{ord}(x*y) \in \{1, p, q, pq\}$

• Supposons $\mathrm{ord}(x*y)=1$:

$$x*y=e_G \Rightarrow x^p * y^p = e_G \Rightarrow q \mid p \quad \lightning$$

- Supposons $(x*y)^p = e_G$ ($\text{ord}(x*y)=p$)

$\Rightarrow y^p = e_G$, m̂ contradiction

- Supposons $(x*y)^q = e_G$

De même.

$\boxed{\text{Conclusion : } \text{ord}(x*y) = pq}$

2e solution :

- $(x*y)^{pq} = e_G$.
- Soit $d = \text{ord}(x*y)$, on a $d \mid pq$.

$(x*y)^d = e_G \Leftrightarrow x^d = (y^{-1})^d$

D'où $x^{dq} = (y^q)^{-d}$

Donc $p \mid dq$, or $p \wedge q = 1$ donc $p \mid d$ (Gauß)

De même, $q \mid d$.

Donc, comme $p \wedge q = 1$, $pq \mid d$

$\boxed{\text{Conclusion : } \text{ord}(x*y) = pq}$

$\boxed{\text{Ainsi } \underbrace{\langle xy \rangle}_{\text{card } pq} \subset \underbrace{G}_{\text{card } pq} \text{, Donc } G \text{ est cyclique, } G \simeq \mathbb{Z}/pq\mathbb{Z}}$

7) G groupe de cardinal 35. Montrons que G a un élément d'ordre 5 et un élément d'ordre 7

1er cas G cyclique.

$$G \simeq \mathbb{Z}/35\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

théorème des restes chinois

$(\overline{1}^{[5]}, \overline{0}^{[7]})$ ordre 5
$(\overline{0}^{[5]}, \overline{1}^{[7]})$ ordre 7.

2e cas G non-cyclique, supposons que tous ses éléments sont d'ordre 1 ou 7 (par l'absurde, $\exists g \in G$ d'ordre 5)

$$G = \bigcup_{g \in G \setminus \{e_G\}} \langle g \rangle$$ — sous-groupe d'ordre 7.

Soit $\langle g_1 \rangle, \dots, \langle g_n \rangle$ la liste exhaustive et sans répétitions des $\langle g \rangle$ où $g \in G \setminus \{e_G\}$.

$$G = \bigcup_{i=1}^{n} \langle g_i \rangle = \{e_G\} \sqcup \left(\overset{(*)}{\bigsqcup_{i=1}^{n}} \langle g_i \rangle \setminus \{e_G\} \right)$$

Soient $i, j \in [\![1; n]\!]$ tq $(\langle g_i \rangle \setminus \{e_G\}) \cap (\langle g_j \rangle \setminus \{e_G\}) \neq \emptyset$.
Soit g dans cette intersection.

g élément d'ordre 7 de $\langle g_i \rangle$ de card 7.
Donc $\langle g \rangle = \langle g_i \rangle$ (7 premier)
De même, $\langle g \rangle = \langle g_j \rangle$
Donc $\langle g_i \rangle = \langle g_j \rangle$, d'où $i = j$. La réunion (*) est bien disjointe.

Donc $35 = 1 + 6n$
$\Rightarrow -1 \equiv 1 \ [6]$ ↯

En remplaçant 7 par 5 dans notre hypothèse, on obtient

$35 = 1 + 4m$
$\Rightarrow 3 = 1 [4]$ ↯.