Exercice 22 : Soit p, q deux entiers premiers distincts. ①

a) Déterminer à isomorphisme près tous les groupes d'ordre pq.

b) Prouver qu'un groupe d'ordre p^2q n'est pas simple.

c) Un groupe d'ordre 45 est-il abélien ?

d) Un groupe d'ordre 225 est-il abélien ?

« N.B. Dans son livre " Cours d'Algèbre " Julien Queysé, édition 1976, Masson, à la page 27, l'exercice 27 : Montrer que tout groupe d'ordre 225 est commutatif. »

Preuve :

c) $o(G) = 45 = 3^2 \cdot 5$

Soit n_3 (resp. n_5) le nombre de 3 (resp. 5) S/g de Sylow de G. Donc on a :

· $\begin{cases} n_5 \equiv 1 \ [\mathrm{mod}\ 5] \\ n_5 / 9 \end{cases}$ ① et $\begin{cases} n_3 \equiv 1 \ [\mathrm{mod}\ 3] \\ n_3 / 5 \end{cases}$ ②.

D'où $n_3 = 1$ et $n_5 = 1$:

Soit H (resp. K) un 3-Sg de Sylow (resp. un 5-Sg de Sylow) de G, alors $H \triangleleft G$ et $K \triangleleft G$.

$o(H \cap K) \,/\, o(H)$ et $o(K)$ or $o(H) \wedge o(K) = 9 \wedge 5 = 1$

donc $o(H \cap K) = 1$ (ie) $H \cap K = \{e\}$, et

$$o(HK) = \frac{o(H).o(K)}{o(H \cap K)} = \frac{9.5}{1} = 45$$ d'où

$G = HK$.

Comme $K \simeq \mathbb{Z}/5\mathbb{Z}$ abélien et

$H \simeq \mathbb{Z}/9\mathbb{Z}$ or bien $H \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

donc H est aussi abélien, et comme

$\forall (h,k) \in H \times K$: $\underbrace{hkh^{-1}}_{\in K} \underbrace{k^{-1}}_{\in K} \in K$

et $\underbrace{h}_{\in H} \underbrace{kh^{-1}k^{-1}}_{\in H} \in H$ (ie) $hkh^{-1}k^{-1} \in H \cap K$

19

(ie) $hkh^{-1}k^{-1} = e$ (ie) $hk = kh$

donc G est abélien. ③

b) ≪ Un groupe $G \neq \{e\}$ est dit simple si ses seuls s/g distingués sont $\{e\}$ et G.

Exples : . $\mathbb{Z}/n\mathbb{Z}$ simple $\Leftrightarrow$ n premier.

. $\forall n \geq 5$: A_n est simple ≫.

$o(G) = p^2 q$. Comme $p \neq q$ donc $q < p$ ou bien $p < q$.

1er cas : $q < p$.

Soit P un p s/g de Sylow de G (donc $o(P) = p^2$)

Soit n_p le nombre de p s/g de Sylow de G.

On a alors $\begin{cases} n_p \equiv 1 \ [\text{mod } p] \\ n_p / q \end{cases}$ (ie) $n_p = 1$ ou bien $n_p = q$).

Si $n_p = q$ alors p divise $q - 1$, donc

$p \leq q - 1 < q < p$, absurde. Donc

$n_p = 1$ et $P \lhd G$.

2ème cas: $p<q$.

Soit n_q le nombre de q-s/g de Sylow de G. Donc $\begin{cases} n_q \equiv 1 \ [\text{mod. } q] \\ n_q / p^2 \end{cases}$ (ie) $n_q \in \{1, p, p^2\}$ (4)

Si $n_q = 1$, alors l'unique q-s/g de Sylow de G est distingué et donc G n'est pas simple.

Si $n_q = p$, alors $p \equiv 1 \ [q]$ (ie) q divise $p-1$, donc $q \leqslant p-1 < p < q$ absurde (Donc $n_q \neq p$).

Si $n_q = p^2$

Soit $H_1, \dots, H_{p^2}$ tous les q-s/g de Sylow de G. $\forall i \neq j$ dans $\{1, \dots, p^2\}$: $H_i \cap H_j = \{e\}$ (car $H_i \simeq \mathbb{Z}/q\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ est simple !).

. De plus, $\forall x \in H_i - \{e\}$: x est un générateur du groupe cyclique $H_i \simeq \mathbb{Z}/q\mathbb{Z}$ (i.e) $o(x) = q$; donc $\text{card}(\bigcup_{i=1}^{p^2} H_i - \{e\}) = \underbrace{(q-1)+\dots+(q-1)}_{p^2 \text{ fois}} =$

$= p^2(q-1)$. ⑤

Soit P un p/g de Sylow de G, donc $o(P) = p^2$. $\forall y \in P$: $o(y) \in \{1, p, p^2\}$ et alors $o(y) \neq q$. Donc

$\text{card}(\bigcup_{i=1}^{p^2} H_i \cup P) = p^2(q-1) + p^2 = p^2 q =$

$= o(G)$. De là on peut dire que P est l'unique p/g de Sylow de G (car si P_1 est un autre p/g de Sylow de G, $\exists x \in P_1 - P$ et alors $x \in \bigcup_{i=1}^{p^2} H_i$ (i.e) $o(x) = q$, mais $o(x) \in \{1, p, p^2\}$ absurde)). Donc G n'est pas simple.

C.Q.F.D.

d) Soit $f : \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \longmapsto \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

$(\bar{x}, \bar{y}) \longmapsto (-\bar{y}, \bar{x}-\bar{y})$

Montrons que $f \in Aut(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$

((ie) f isomorphisme de $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \longmapsto \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$))

et que $o(f) = 3$:

(6)

- $f((\bar{x}, \bar{y}) + (\bar{x_1}, \bar{y_1})) = f(\overline{x+x_1}, \overline{y+y_1})$

$= (-(\overline{y+y_1}), \overline{x+x_1} - (\overline{y+y_1})) =$

$= (-\bar{y}, \bar{x} - \bar{y}) + (-\bar{y_1}, \bar{x_1} - \bar{y_1})$

$= f(\bar{x}, \bar{y}) + f(\bar{x_2}, \bar{y_2})$.

Donc f est un homomorphisme de groupes.

- $f(\bar{x}, \bar{y}) = (\bar{0}, \bar{0}) \Longleftrightarrow \begin{cases} -\bar{y} = 0 \\ \bar{x} - \bar{y} = \bar{0} \end{cases} \Longleftrightarrow$

$\Longleftrightarrow (\bar{x}, \bar{y}) = (\bar{0}, \bar{0})$.

Donc $f \in Aut(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$.

17.03.2005

- $f^2(\bar{x}, \bar{y}) = f(f(\bar{x}, \bar{y})) = f(-\bar{y}, \bar{x} - \bar{y})$

$= (-\bar{x} + \bar{y}, -\bar{y} - \bar{x} + \bar{y}) = (-\bar{x} + \bar{y}, -\bar{x})$

et $f^3(\bar{x},\bar{y}) = f(f^2(\bar{x},\bar{y})) =$

$= f(-\bar{x}+\bar{y}, -\bar{x}) = (-(-\bar{x}), -\bar{x}+\bar{y}-(-\bar{x}))$

$= (\bar{x},\bar{y})$. Donc $f \neq id_{\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}} = id$,

(7)

$f^2 \neq id_{\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}}$ et $f^3 = id_{\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}}$,

donc $o(f^3) = 3$.

- Soit $\varphi : \mathbb{Z}/3\mathbb{Z} \longmapsto Aut(\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z})$

$\bar{0} \longmapsto \varphi(\bar{0}) = id$

$\bar{1} \longmapsto \varphi(\bar{1}) = f$

$\bar{2} \longmapsto \varphi(\bar{2}) = f^2$

φ est alors un homomorphisme non trivial de groupes. Soit $G_1 = (\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}) \times_\varphi \mathbb{Z}/3\mathbb{Z}$, d'après f) l'ex 19, et comme φ est non trivial alors G_1 est non commutatif.

Soit $G = G_1 \times \mathbb{Z}/3\mathbb{Z}$ groupe non commutatif et $o(G) = o(G_1)\,o(\mathbb{Z}/3\mathbb{Z}) = 75.3 = 225$.

C.Q.F.D.

a) Comme $p \neq q$, on suppose (par exple) $p < q$.
(Soit G un groupe d'ordre pq. Soit n_q le nombre de q-s/g de Sylow de G ((donc $n_q \equiv 1 [q]$ et n_q / p (ie) $n_q = 1$ ou $n_q = p$)). (8)

Si $n_q = p$ alors $p \equiv 1 [q]$ (ie) $q / p-1$
donc $q \leqslant p-1 < p < q$, absurde. Donc
$n_q = 1$ et alors G admet un unique q-s/g de Sylow, qui on notera Q, on a alors $Q \triangleleft G$.

Soit P un p-s/g de Sylow de G, $P \cap Q$ est un s/g de P et de Q, donc $o(P \cap Q)$ divise $o(P) = p$ et $o(Q) = q$, or $p \wedge q = 1$ donc $o(P \cap Q) = 1$ (ie) $P \cap Q = \{e\}$.

D'où $G = P.Q$ et selon g)/2x19,
$G \simeq Q \rtimes_\varphi P$ où

. $\varphi : P \longmapsto Aut(Q)$

$h \longmapsto \varphi(h) : Q \longmapsto Q$

$x \longmapsto hxh^{-1}$

On a 2 cas possibles : ⑨

p ne divise pas $q-1$ ou bien

p divise $q-1$.

1er cas : p ne divise pas $q-1$.

<< Rappel $\forall n \geq 2$:

$Aut(\mathbb{Z}/n\mathbb{Z}) \simeq U(\mathbb{Z}/n\mathbb{Z})$

et si n premier $U(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/(n-1)\mathbb{Z}$ >>

Si $\varphi : \mathbb{Z}/p\mathbb{Z} \longmapsto \mathbb{Z}/(q-1)\mathbb{Z}$ est un

homomorphisme non trivial alors

φ est injectif et $Im(\varphi)$ est un s/g d'ordre

p de $\mathbb{Z}/(q-1)\mathbb{Z}$, donc p divise $q-1$, absurde.

Donc tout homomorphisme de $P \longrightarrow Aut(Q)$ est trivial et dans ce cas

$$G \simeq Q \rtimes_\varphi P = Q \times P \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq$$

e) 2×19

$$\simeq \mathbb{Z}/pq\mathbb{Z}$$ et G est cyclique. (10)

2ème cas: p divise $q-1$.

Si φ est trivial, $G \simeq P \rtimes_\varphi Q \simeq P \times Q$

$$\simeq \mathbb{Z}/pq\mathbb{Z}$$

On suppose alors que φ est non trivial

(donc G n'est pas commutatif).

or $P \simeq \mathbb{Z}/p\mathbb{Z}$ et $Q \simeq \mathbb{Z}/q\mathbb{Z}$

« Rappel: si $G_1 \simeq G_2$

alors $Aut(G_1) \simeq Aut(G_2)$ »

donc $\exists \varphi_1$ homomorphisme non trivial

de $\mathbb{Z}/p\mathbb{Z} \longmapsto \mathbb{Z}/(q-1)\mathbb{Z}$ tel que

$G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_1} \mathbb{Z}/p\mathbb{Z}$

(11)

Si G' est un groupe non abélien d'ordre pq (avec p divise $q-1$), donc

$\exists \varphi_1' : \mathbb{Z}/p\mathbb{Z} \longmapsto \mathbb{Z}/(q-1)\mathbb{Z}$ homomorphisme non trivial tel que $G' \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_1'} \mathbb{Z}/p\mathbb{Z}$

Montrons que $G \simeq G'$ (ie) que

$\mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_1} \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_1'} \mathbb{Z}/p\mathbb{Z}$

et pour cela, et selon h) Tx19, il suffit de prouver l'existence d'un isomorphisme $\alpha : \mathbb{Z}/p\mathbb{Z} \longmapsto \mathbb{Z}/p\mathbb{Z}$ tel que

$\varphi_1' \circ \alpha = \varphi_1$:

Comme φ_1 et φ_1' ne sont pas triviaux, alors $Im(\varphi_1)$ et $Im(\varphi_1')$ sont des $\mathbb{Z}/q$

d'ordre p du groupe cyclique $\mathbb{Z}/(q-1)\mathbb{Z}$
(ou si d/n, $\exists!$ s/g de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d),
donc $Im(\varphi_1) = Im(\varphi_1')$. • (12)

Soit $\dot{a} = \varphi_1(\bar{1}) \in Im(\varphi_1) = Im(\varphi_1')$,
$\exists! \bar{b} \in \mathbb{Z}/p\mathbb{Z}$ tel que $\varphi_1'(\bar{b}) = \dot{a}$,

on pose alors $\alpha : \mathbb{Z}/p\mathbb{Z} \longmapsto \mathbb{Z}/p\mathbb{Z}$

$\bar{1} \longmapsto \bar{b}$

$\bar{c} \longmapsto \overline{cb}$

$\bar{0} \longmapsto \bar{0}$

donc α est un isomorphisme de $\mathbb{Z}/p\mathbb{Z} \longmapsto \mathbb{Z}/p\mathbb{Z}$
et $(\varphi_1' \circ \alpha)(\bar{1}) = \varphi_1'(\alpha(\bar{1})) = \varphi_1'(\bar{b}) =$
$= \dot{a} = \varphi_1(\bar{1})$, d'où
$\varphi_1' \circ \alpha = \varphi_1$;
et alors comme conclusion:

Soit G un groupe d'ordre pq
où p et q sont premiers distincts

(on suppose, par exple, que $p<q$). Si (*)
p divise $q-1$ alors G est nonabélien
et $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ où φ est

n'importe quel homomorphisme non trivial
de $\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z}$ $(\simeq Aut(\mathbb{Z}/q\mathbb{Z}))$,

sinon G est abélien et dans ce cas cyclique $\simeq \mathbb{Z}/pq\mathbb{Z}$.
et Si p ne divise pas $q-1$ alors

(tout homomorphisme de $\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z} \simeq Aut(\mathbb{Z}/q\mathbb{Z})$
est trivial) G est cyclique
isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.

C.Q.F.D.