② Groupe cyclique, ordre d'éléments, Lagrange

$(G,\times)$ $e_G = 1$ $\#(G) < +\infty$.

- $\theta(x) = ?$. c'est le plus petit entier m / $x^m = 1$
  - $\varphi : \mathbb{Z} \to G$, $k \mapsto x^k$ $\quad \operatorname{Ker}\varphi = \{k \,/\, x^k = 1\} = m\mathbb{Z}$ (sous-groupe de $\mathbb{Z}$)

    $(m \neq 0)$
  - $\theta(x) = \#(\langle x \rangle)$
- G cyclique $\Leftrightarrow$ monogène et fini $\Leftrightarrow \left| \exists x \,/\, G = \langle x \rangle \right.$, $\theta(x) = n$

  Exemples $\left(\mathbb{Z}/n\mathbb{Z}, +\right)\left(\mathbb{U}_n, \times\right)$
- si $p \in \mathcal{P}$, $\#(G) = p$ alors G est cyclique.

  Corollaire d'1 Thm fondamental Lagrange ($\forall x$, $\theta(x) \,/\, \#(G)$)

  Preuve.

  $x \neq 1$ $\theta(x)/p$ et $p \in \mathcal{P}$ donc $\theta(x) = p$ ($\in G$)!

- Ex 2 1) ....

2) $\theta(x) = m$ $\quad O(\alpha_g(x)) = k$, on veut montrer $m = k$

- $(\alpha_g(x))^m = \alpha_g(x^m) = \alpha_g(1) = 1$ donc k/m.
- $\alpha_{g^{-1}}(\alpha_g(x)) = x$ donc si $k = \theta(\alpha_g(x))$, m/k

  car $x^k = \left(\alpha_{g^{-1}}(\alpha_g(x))\right)^k = \alpha_{g^{-1}}\left(\alpha_g(x)^k\right) = \alpha_{g^{-1}}(1) = 1$.

3) z est le seul élément d'ordre 2, comme $\forall g \in G$ $\alpha_g(z)$ est d'ordre 2

cela signifie $gzg^{-1} = z$ $\forall g \in G$ donc $gz = zg$ $\forall g \in G$

et z est dans le centre.

$\#(G) = 15$ $\quad x \in G \,/\, \theta(x) = 1, 3, 5, 15$

① $\exists x$ $\sigma(x) = 15$ $\quad G = \langle x \rangle$ $\quad G \simeq \left(\mathbb{Z}/15\mathbb{Z}, +\right)$ ou $\left(\mathbb{U}_{15}, \times\right)$

② $\exists x$ $\sigma(x) = 3$ en effet $\boxed{\text{Thm Cauchy } p \in \mathcal{P}\ p \,/\, \#(G) \quad \exists x \,/\, \sigma(x) = p}$ Revoir Ex. groupe d'ordre p et 1 ensemble.

$\exists y$ $\sigma(y) = 5$

$\langle x \rangle = K$ $\quad \langle y \rangle = H$

$K \cap H < H$ donc $\#(K \cap H) / 5$ $\quad$ donc $\boxed{\#(K \cap H) = 1}$

$\phantom{K \cap H <{}} K$ $ \#(K \cap H) / 3$

On démontre via les actions de groupes que H est distingué dans G

(cf pb B2)

$\mathbb{U}(\mathbb{Z}/n\mathbb{Z}) = ?$ $\qquad \mathbb{U}(A) = \{ z \in A \,/\, z \text{ inversible} \}$

$\longrightarrow$ On sait $(\mathbb{U}(A), \times)$ groupe multiplicatif (par ex. $(\mathbb{C}^*, \times)$ ds $\mathbb{C}$, $(\{\pm 1\}, \times$ ds $\mathbb{Z})$)

$$GL_n(K) = \mathbb{U}(M_n(K))$$

$\mathbb{U}(\mathbb{Z}/n\mathbb{Z}) = \{ \bar{z} \in \mathbb{Z}/n\mathbb{Z} \,/\, \bar{z} \text{ inversible} \}$

Révision $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$

$\bar{z}$ inv $\iff \exists \bar{z}' \in \mathbb{Z}/n \,/\, \bar{z}\bar{z}' = \bar{1}$

$\iff \exists k \,/\, zz' + kn = 1$ ds $\mathbb{Z}$

$\iff (z, n) = 1$ Bézout.

$\#(\mathbb{U}(\mathbb{Z}/n\mathbb{Z})) = \varphi(n) \xrightarrow[\text{déc}]{\text{thm}} \varphi(n) = \prod \varphi(p_i^{\alpha_i})$

$\varphi(p_i^{\alpha}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i - 1}(p_i - 1)$

par ex. $\varphi(15) = \varphi(3)\varphi(5) = 8$. $\qquad \mathbb{U}(\mathbb{Z}/15\mathbb{Z}) = \{ \bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14} \}$

$\mathrm{Aut}((\mathbb{Z}/5\mathbb{Z}, +)) = \{ \varphi$ morphisme bijectif de $(\mathbb{Z}/5\mathbb{Z}, +) \to (\mathbb{Z}/5\mathbb{Z}, +) \}$

φ est déterminé par $\varphi(\bar{1})$ car $\mathbb{Z}/5\mathbb{Z} = \langle \bar{1} \rangle = \{ k.\bar{1}, k \in \mathbb{Z} \}$

$\varphi(\mathbb{Z}/5\mathbb{Z}) = \{ k\,\varphi(\bar{1}), k \in \mathbb{Z} \} = \langle \varphi(\bar{1}) \rangle$

$\triangle$ $+$

donc φ bijectif $\iff \varphi(\bar{1})$ engendre $\mathbb{Z}/5\mathbb{Z}$ ie $\iff \varphi(\bar{1}) \in \mathbb{U}(\mathbb{Z}/5\mathbb{Z}) = (\mathbb{Z}/5\mathbb{Z})^*$

car $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ corps $p \in \mathcal{P}$.

$\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}, +) \simeq \mathbb{U}(\mathbb{Z}/5\mathbb{Z})$

$\varphi \longrightarrow \varphi(\bar{1})$

donc $o(\varphi) \,/\, \#\mathrm{Aut}(\;) = 4$.

$\varphi^3 = \mathrm{Id}$ impossible sauf à ce que $\varphi = \mathrm{Id}$!

On revient à exo 7 B 3)

$k \in K \to \alpha_k$

$K \longrightarrow \mathrm{Aut}(H) \simeq \mathbb{U}(\mathbb{Z}/5\mathbb{Z})$

$\alpha_k = \mathrm{Id}$ ce qui dit que $\forall k \in K\ \forall h \in H\ \ khk^{-1} = h$ $\qquad kh = hk$ (*)

4). $\theta(h,k) = hk$ $\qquad \mathrm{Im}(\theta) = HK$

$\theta(hh', kk') = hh'kk' \overset{(*)}{=} hk\,h'k'$

. $\theta(h,k) = \theta(h',k') \iff hk = h'k' \iff \underbrace{h'^{-1}h}_{\in H} = \underbrace{k'k^{-1}}_{\in K} = e$.

donc $h = h'$ et $k = k'$

Donc $\underbrace{H \times K}_{\text{card}=15} \simeq \underbrace{HK}_{\text{Card } 15} \subset \underline{G}$ $\quad$ Card 15 $\qquad G = HK \simeq H \times K$

$\simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$\simeq \mathbb{Z}/15\mathbb{Z}$ cyclique