

## Théorème :

Soit  $G = \langle a \rangle$  monogène.

1<sup>re</sup> cas :  $\text{card } G = n < \infty$ , alors.

$G$  est isomorphe à  $\mathbb{Z}/n\mathbb{Z}$ .

avec  $\varphi: \mathbb{Z}/n\mathbb{Z} \rightarrow G$

et un isomorphisme  $\bar{k} \mapsto \varphi(\bar{k}) = a^k$ .

2<sup>de</sup> cas :  $G$  infini, alors  $G$  est isomorphe à  $\mathbb{Z}$ .

$\varphi: \mathbb{Z} \rightarrow G$

$k \mapsto \varphi(k) = a^k$

isomorphisme.

## Preuve :

1<sup>re</sup>  $G = \langle a \rangle = \text{cyclique}$ ,  $\text{card } G = n$

1<sup>re</sup>  $\varphi: (\mathbb{Z}/n\mathbb{Z}, +) \rightarrow (G, \cdot)$  est un isomorphisme.

$$\bar{k} \mapsto \varphi(\bar{k}) = a^k$$

1<sup>re</sup>  $\varphi$  est bien définie.

•  $\forall \bar{k} \in \mathbb{Z}/n\mathbb{Z} : \varphi(\bar{k}) = a^k \in G$ .

• Si  $\bar{k}, \bar{k}' \in \mathbb{Z}/n\mathbb{Z}$  et  $\bar{k} = \bar{k}'$ , alors  $\varphi(\bar{k}) = \varphi(\bar{k}')$ .

On a  $\bar{k} = \bar{k}' \Leftrightarrow k \equiv k' (n) \Leftrightarrow n \mid k - k'$ .

$\varphi(\bar{k}) = a^k = a^{np+k'} = (a^n)^p \cdot a^{k'} = 1^p \cdot a^{k'} = a^{k'} = \varphi(\bar{k}')$

$\Rightarrow \varphi$  est bien définie.

$\star \overline{k}, \overline{k'} \in \mathbb{Z}/n\mathbb{Z}$   
 $\varphi(\overline{k+k'}) = \varphi(\overline{k+k'}) = a^{k+k'} = a^k \cdot a^{k'}$   
 $= \varphi(\overline{k}) \cdot \varphi(\overline{k'})$   
 $\Rightarrow \varphi$  est un morphisme de groupes  
 $\bullet \overline{k} \in \ker \varphi \Leftrightarrow \varphi(\overline{k}) = e \Leftrightarrow a^k = e$   
 $\Leftrightarrow \text{ord}(a) = n \mid k \Rightarrow \overline{k} = \overline{0}$   
 $\Rightarrow \ker \varphi = \{\overline{0}\} \Rightarrow \varphi$  est injective  
 et on a  $\text{Card}(G) = \text{Card}(\mathbb{Z}/n\mathbb{Z}) = n < \infty$   
 Donc  $\varphi$  est bijective  
 Ainsi  $\varphi$  est un isomorphisme de groupes.

e) G infini

Req.  $\varphi: (\mathbb{Z}, +) \rightarrow (G, \cdot)$  est un isomorphisme  
 $k \mapsto a^k$

$\varphi$  est un morphisme de groupes.

$\forall y \in G, \langle a \rangle: \exists k \in \mathbb{Z} \text{ tq } y = a^k = \varphi(k)$

$\Rightarrow \varphi$  est surjective

$\bullet \ker \varphi = \{k \in \mathbb{Z} \text{ tq } a^k = e\}$

$\text{Supp } \exists k \in \mathbb{Z}^* \text{ tq } a^k = e$

$\Downarrow$   
 $\exists p \in \mathbb{N}^* \text{ tq } a^p = e$   
 $(p = k_0 \text{ car } p = k_0)$

$\Rightarrow a$  d'ordre fini.

$\text{Card}(\langle a \rangle) = n < \infty$  absurde  
 $\Rightarrow \ker \varphi = \{0\}$   
 $\Rightarrow \varphi$  injective.

## Autrevent

C'est un morphisme de groupes

⇒ Kerf. d. Abb. d.  $\mathbb{Z}_6$

$$\Rightarrow \exists n \in \mathbb{N} \text{ by } \text{Arch} \text{ s.t. } n \geq \frac{1}{\epsilon}$$

Supp  $\eta \neq 0$

on pose.  $f: (Z/nZ, +) \rightarrow (G, \cdot)$

$$T_k \rightarrow ah.$$

- $f$  est un morphisme  $E \rightarrow G/H$ .
- $f$  est surjectif.

1st Subjective

$$\begin{aligned} k \in \ker f &\Leftrightarrow f(k) = e \Leftrightarrow a^k = e \\ &\Leftrightarrow k \in \ker \varphi = n\mathbb{Z} \Rightarrow k = \frac{n}{h} \cdot e \\ &\Rightarrow \ker f = \left\{ 0 \right\} \Rightarrow f \text{ is injective} \end{aligned}$$

$\Rightarrow \ker f = \{0\} \Rightarrow f$  injective.  
 $\Rightarrow f$  bijective.

$\Rightarrow f$  bijective.  $\Rightarrow$   $f$  injective.

$$\begin{aligned} \text{absorb} & \Rightarrow \text{Card } \mathcal{G} = \text{Card } \mathcal{U} / n = n \sqrt{q} \\ \text{absorb} & \Rightarrow \text{Card } \mathcal{G} = \text{Card } \mathcal{U} / n = n \sqrt{q} \end{aligned}$$

## Exercício 5.

Exercice 5 :  
(G, .) groupe fini, card G = n  $\in \mathbb{N}^*$ .

Hsgb.G.

$$xRy \Leftrightarrow xy^{-1} \in H.$$

2a1.  $R$ : reflexive;  $x x^{-1} = e \in H$ .

R: Symmetric;  $\Leftrightarrow xRy \Leftrightarrow xy^{-1} \in H$ .

$$yRx \Leftarrow (xy^{-1})^{-1} = yx^{-1} \in H$$

$R$ : transitive; s.t.  $x R y \Leftrightarrow (x y^{-1})^{-1} = y x^{-1} \in H$ ,  
 $\Downarrow$   
 $x^{-1} y \in H$ .

$$xy^{-1} \in H \text{ and } yz^{-1} \in H.$$
$$\Rightarrow xz^{-1} = xy^{-1} \cdot yz^{-1} \in H.$$

$\Rightarrow R$ : relation d'équivalence.

$$b) a \in G, \mathcal{C}_R(a) = \{x \in G \mid xRa\} \\ = \{x \in G \mid x a^{-1} \in H\} \\ \begin{matrix} a \\ x a^{-1} = h \in H \\ x = h a \end{matrix}$$

$$\mathcal{C}_R(a) = H \cdot a$$

$$c) f_a: H \rightarrow \mathcal{C}_R(a) \\ x \mapsto x \cdot a$$

$$\forall y \in \mathcal{C}_R(a) = H \cdot a, \exists x \in H \text{ s.t. } y = x a \\ \Rightarrow f_a \text{ est surjective.}$$

$$\text{Soit } x, x' \in H \text{ s.t. } f_a(x) = f_a(x') \\ \Leftrightarrow x a = x' a$$

$$\Leftrightarrow x a a^{-1} = x' a a^{-1} \Rightarrow x = x'$$

$$\Rightarrow f_a \text{ est injective.}$$

$$\text{Donc } f_a \text{ est bijective.}$$

on a:  $R$ : relation d'équivalence.

Alors l'ensemble des classes d'équivalence forment une partition de  $G$ .

$$G = \bigcup_{a \in G} \mathcal{C}_R(a)$$

$$\text{or } \text{Card } G < \infty \Rightarrow \exists p \text{ classe d'équiv. avec } p \leq n.$$

$$G = \bigcup_{k=1}^p \mathcal{C}_R(a_k)$$

$$\Rightarrow \text{Card } G = \sum_{k=1}^p \text{Card}(\mathcal{C}_R(a_k))$$

Donc par l'app.  $f_{a_k}$  est bijective.

$$\Rightarrow \text{Card}(\mathcal{C}_R(a_k)) = \text{Card}(H), \forall k \in \{1, \dots, p\}$$

$$\Rightarrow \text{Card } G = p \cdot \text{Card}(H)$$

$$\Rightarrow \boxed{\text{Card } H \mid \text{Card } G}$$

u) Si  $(G, \cdot)$  groupe.  
 $\text{Card}(G) = n$  et  $a \in G$ .

Soit  $H = \langle a \rangle$  s.g.d.  $G$ .

D'après 1.  $\text{Card } H \mid \text{Card } G = n$ .  
 $\text{ord}(a) \mid \text{Card } G$ .

$$\Rightarrow a^n = e.$$

5)  $n = ep + 1$  et  $m \mid ep$   $ep = mk$ .  
 a)  $\varphi: G \rightarrow G$  est bijective.  
 $x \mapsto x^m$ .

Soit  $x, y \in G$  t.p.  $f(x) = f(y)$   
 $\Leftrightarrow x^m = y^m \Leftrightarrow x^{mk} = y^{mk}$   
 $\Rightarrow x^{ep} = y^{ep}$   
 $\Rightarrow x^{-1} = y^{-1}$   
 $e = x^m y^{-1}$   
 $y = x^m$   
 $\Rightarrow x^{n-1} = y^{n-1}$   
 $(x = y = e)$

$\Rightarrow$  surjective.  
 et on a  $\text{Card } G \leq \infty \left\{ \begin{array}{l} \Rightarrow f \text{ surjective} \\ \Rightarrow f \text{ bijective} \end{array} \right.$

Exercice 7.

Soit  $G$  un groupe cyclique.  
 $G = \langle a \rangle$  et  $\text{Card } G = n$ .

1) Pq si  $H$  s.g.d.  $G$ , alors  $H$  est cyclique.  
 Si  $H = \{e\}$ .  
 Si  $H \neq \{e\} \Rightarrow \exists x \in H \setminus \{e\}$ .

Soit  $I = \{p \in \mathbb{N}^* \mid \exists k \in \mathbb{Z}^* \text{ t.p. } x = a^k \in H\}$   
 $I \neq \emptyset$  car  $k \in I \Leftrightarrow k \in I$   
 $I \subset \mathbb{N}^*$   
 Soit  $d' = \min I$ .  
 Pq  $H = \langle a^{d'} \rangle$ .

ma.  $d' \in \Sigma \Rightarrow a^{d'} \in H = \langle a \rangle$ .  
 $\Rightarrow \langle a^{d'} \rangle \subset H$ .  
 " soit  $y \in H \Rightarrow \exists n' \in \mathbb{Z} \text{ tq. } y = a^{n'}$ .  
 $n' = d \cdot d' + r$  avec  $0 \leq r < d'$ .

Supposons  $r \neq 0$   
 ma.  $a^{n'} = (a^{d'})^{d''} \cdot a^r$   
 $\Rightarrow a^{n'} = a^{n''} \cdot (a^{d'})^{d''}$   
 $\Rightarrow a^{n'} \in H \Rightarrow r \in \Sigma \Rightarrow n' \geq d$  absurde.  
 $\Rightarrow n' = d \cdot d' \Rightarrow y = (a^{d'})^{d''} \in \langle a^{d'} \rangle$

Arns.  
 $H = \langle a^{d'} \rangle$ .  
 e). Si  $d$  divise  $\text{card}(G)$   
 tq.  $\exists ! H$  s.g. de  $G$ .  
 $\text{card}(H) = d$ .

II soit  $H' = \langle a^{\frac{n}{d}} \rangle$ .  
 ma.  $o(a^{\frac{n}{d}}) = d \Rightarrow \text{card } H' = d$ .  
unicité.  
 soit  $H$  un s.g. de  $G$  tq  $\text{card } H = d$ .  
 d'après 1/  $H$  cyclique.  
 $\Rightarrow H = \langle a^k \rangle$ . et  $\text{card } H = d$ .  
 ma.  $(a^k)^d = e \Rightarrow a^{kd} = e$ .  
 $\Rightarrow n \mid kd$ . et  $d \mid n \Rightarrow n = d \cdot n'$ .  
 $\Rightarrow d \cdot n' \mid kd \Rightarrow n' \mid k$ .  
 $\Rightarrow k = k' \cdot n'$ .  
 $\Rightarrow a^k = (a^{\frac{n}{d}})^{k'} \Rightarrow a^k \in \langle a^{\frac{n}{d}} \rangle$ .  
 $\Rightarrow H \subset \langle a^{\frac{n}{d}} \rangle = H'$ .  
 et  $\text{card } H = \text{card } H' = d$   
 $\Rightarrow H = H'$ .

Exercise 66.  $H, K \leq G$  et  $K \trianglelefteq G$ .

$H \cdot K = \{xy, x \in H \text{ et } y \in K\}$

$\Rightarrow$   $H$  est distingué dans  $K$ :

$\forall h \in H; \forall x \in G, xhx^{-1} \in H$ .

Pq.  $H \cdot K$  est un  $\trianglelefteq G$ .

$\cdot H \cdot K \subset G$ .

$\cdot e = ee \in H \cdot K$ .

$\cdot \forall x, y \in H \cdot K, \text{ on a } xy^{-1} \in H \cdot K$ .

$x = h.k$  et  $y = h'.k', h, h' \in H$   
 $k, k' \in K$ .

$$\begin{aligned} xy^{-1} &= h.k.(h'.k')^{-1} \\ &= h.k.k'^{-1}.h'^{-1} \\ &= \underbrace{h.k.k'^{-1}}_{\substack{\in H \\ \leftarrow \\ \in H}} \cdot \underbrace{h'^{-1}}_{\substack{\in H \\ \leftarrow \\ \in H \text{ (distingué)}}} \cdot \underbrace{(k.k'^{-1})}_{k'' \in K} \end{aligned}$$

$$\begin{aligned} &= h''.k'' \in H \cdot K \\ \Rightarrow H \cdot K &\trianglelefteq G. \end{aligned}$$

## Rappel: "Anneau".

$(A, +, \times)$  est un anneau.  
 $\Leftrightarrow$

$(A, +)$  groupe abélien

$\exists 1_A$  pour la loi " $\times$ "

" $\times$ " associative.

" $\times$ " est dist.  $\% "$  " $+$ ".

### Exemples:

$(\mathbb{C}, +, \times)$ ;  $(\mathbb{R}, +, \times)$ ;  $(\mathbb{Q}, +, \times)$ ;  $(\mathbb{Z}, +, \times)$ .

$(K[x], +, \times)$ ;  $(K(x), +, \times)$ ;  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

sont des anneaux commutatifs.  $(\mathbb{R}(x), +, \times)$

\*  $(M_n(K), +, \times)$ ;  $(\mathcal{L}(E), +, \circ)$

sont des anneaux non commutatifs.

$U(A) = \{x \in A \mid \exists x^{-1} \text{ tel que } x \cdot x^{-1} = 1 \text{ pour la loi } \times\}$

Ex.  $U(\mathbb{Z}) = \{-1, 1\}$

$U(M_n(K)) = GL_n(K)$

$U(\mathbb{Z}/n\mathbb{Z}) = \{ \bar{a} \mid a \wedge n = 1 \}$

Dans  $\mathbb{Z}/12\mathbb{Z} \Rightarrow U(\mathbb{Z}/12\mathbb{Z}) = \{ \bar{1}, \bar{5} \}$

$\bar{3} \bar{3} = \bar{1} \Rightarrow (\bar{3})^{-1} = \bar{3}$

Prop.  $a \wedge n = 1 \Leftrightarrow \exists u, v \in \mathbb{Z} \text{ t.q. } au + vn = 1$   
 $\Rightarrow \overline{au + vn} = \bar{1} \Rightarrow \overline{au} = \bar{1} \Rightarrow \overline{a} \cdot \overline{u} = \bar{1}$

$\Rightarrow \bar{a}$  inv.

\*  $(A, +, \times)$  est un corps  $\Leftrightarrow$   
 $(A, +, \times)$  anneau commutatif

$\& U(A) = A \setminus \{0\}$

$\mathbb{Z}/p\mathbb{Z}$  corps  $\Leftrightarrow p$  premier.

Sous anneau.

$$B \subset A;$$

$(B, +, \times)$  est un sous anneau  $\Leftrightarrow$

- $\left\{ \begin{array}{l} 1_A \in B \\ (B, +) \text{ i.g.d. } (A, +) : (x-y) \in B \\ \forall x, y \in B; x \cdot y \in B \end{array} \right.$

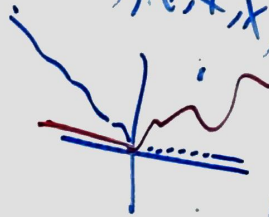
\*  $(A, +, \times)$  est un anneau intègre

si  $x, y \in A$  tq  $x \cdot y = 0 \Rightarrow x = 0$  ou  $y = 0$ .

Exemples

$(\mathbb{R}, +, \times), (\mathbb{C}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{Z}, +, \times)$  sont intègres.

\*  $(\prod_n (\mathbb{K}), +, \times), (\sqrt[n]{\mathbb{K}}, +, \times)$  ne sont intègres.



8.  $(A, +, \times)$  est un corps, alors intègre :

on  $x, y \in A$  tq  $x \cdot y = 0$

si  $x \neq 0 \Rightarrow x^{-1} \cdot y = 0 \Rightarrow y = 0$

$(\mathbb{Z}/p\mathbb{Z}, +, \times)$  est un corps  $\Leftrightarrow$  intègre  $\Leftrightarrow p$  premier.

(2)  $\Rightarrow$  (3)

hyp  $\mathbb{Z}/p\mathbb{Z}$  intègre, nq  $p$  premier. Supp  $p$  n'est pas premier.

$\Rightarrow \exists k, k' \in \mathbb{Z}, p \nmid k \text{ tq } k \cdot k' = p$

et  $\overline{k} \cdot \overline{k'} = \overline{p} = \overline{0}$ .  
ce qui est absurde car  $\mathbb{Z}/p\mathbb{Z}$  intègre.

Dans un anneau commutatif

$I \subset A$ ;  $I$  idéal

$$\Leftrightarrow \left\{ \begin{array}{l} \forall x, y \in I, x+y \in I \\ \forall a \in A, \forall x \in I, a \cdot x \in I \end{array} \right\} \quad (I, +) \text{ sgd } (A, +)$$

•  $I$  idéal  $\Rightarrow (I, +)$  sgd  $(A, +)$ .

Si  $I$  idéal

et  $1_A \in I \Rightarrow I = A$ .

\* Si  $I$  idéal et  $\exists x$  inversible  $x \in I$

$$\downarrow \\ 1_A = x \cdot x^{-1} \in I$$

\* Si  $I$  idéal d'un corps.  
Alors  $I = \{0\}$  ou  $I = A$ .

Dans  $K[X]$  les idéaux sont d.o.

la forme  $I = P \cdot K[X] : P \in K[X]$

$U \in \mathcal{U}(E)$ .

$$P(U) = \{ P \in K[X] \mid P(U) = 0 \} \\ = \text{idéal de } K[X]$$

Dans  $\mathbb{Z}$

Les idéaux de  $\mathbb{Z}$  sont  $n\mathbb{Z}$ ,  $n \in \mathbb{N}$ .

\* Dans  $(A, +, \cdot)$

$\forall a \in A, I = aA$  est un idéal de  $A$ .