

Ex 1:

A anneau commutatif ; $A \neq \{0\}$.

1) A intègre et fini $\Rightarrow A$ corps.

Soit $a \in A \setminus \{0\}$.

$$f: A \longrightarrow A \\ n \mapsto an.$$

Soit $(n, y) \in A^2$ $\neq$ $f(n) = f(y)$

$$\text{donc } an = ay \Rightarrow a(n-y) = 0$$

$$\Rightarrow n-y = 0 \text{ car } A \text{ intègre et } a \neq 0.$$

$$\text{donc } n = y$$

d'où f est injective de A dans lui-même

or $|A| < \infty$ donc f est bijective

En particulier, il existe $n \in A$ $\neq$ $f(n) = 1_A$.

$$c \text{ à d : } an = 1_A$$

donc a est inversible

ouf. A est un corps.

2) $\Rightarrow$ A un corps.

Soit I un idéal de A .

s. $I \neq \{0\}$ alors $\exists a \in I \setminus \{0\}$.

$a \neq 0 \Rightarrow a$ est inversible.

$$1 = a \cdot a^{-1} \in I \text{ car } \begin{cases} a \in I \\ I \text{ idéal de } A \end{cases}$$

donc $\forall n \in A, n = n \cdot 1 \in I$.

d'où $A \subset I$ et $I = A$.

on a: A et $\{0\}$ sont les seuls idéaux du corps A .

$\Leftrightarrow$ on suppose que A et $\{0\}$ sont les seuls idéaux de A .

Soit $a \in A \setminus \{0\}$.

$(a) = \{an, n \in A\}$ est un idéal de A , contenant

$a \neq 0$ donc $(a) = A$.

En particulier $1 \in (a)$

$$\Rightarrow \exists n \in A \text{ tq } an = 1.$$

$\Rightarrow a$ est inversible

on a: A est un corps.

Ex 2: $(G, \cdot)$ un gpe d'elt neutre e .

$\Rightarrow$ Soit $(n, y) \in G^2$, m q $ny = ym$.

on a $z^2 = e \quad \forall z \in G$ donc $z^{-1} = z \quad \forall z \in G$.

$$\text{donc } (ny)^{-1} = ny \Rightarrow y^{-1} \cdot n^{-1} = ny.$$

$$\Rightarrow yn = ny$$

e .

donc G est abélien.

2) $\Rightarrow$ G cyclique d'ordre n .

G cyclique donc $\exists a \in G$ tq $G = \langle a \rangle = \{a^k, k \in \mathbb{Z}\}$.

$|G| = n < \infty$ donc a est d'ordre fini
de plus $o(a) = |\langle a \rangle| = |G| = n$.

$\Leftarrow$ $|G| = n$.

$\exists a \in G, o(a) = n$.

$\langle a \rangle$ est un sous-gpe de G .

$$|\langle a \rangle| = o(a) = n = |G|$$

donc $G = \langle a \rangle$ est cyclique.

b) G gpe d'ordre premier p . ($p \geq 2$)

Soit $a \in G \setminus \{e\}$.

$o(a)$ divise $|G| = p$: premier.

$$\Rightarrow o(a) = 1 \text{ ou } o(a) = p.$$

or $a \neq e$ donc $o(a) \neq 1$ et par suite

$$o(a) = p = |G|$$

donc d'op $\hat{s}$ a) G est cyclique.

c) Soit G un gpe d'ordre $n \leq 5$.

mq G est abélien.

* si $|G| = 1$ alors $G = \{e\}$ est abélien.

* si $|G| = n \in \{2, 3, 5\}$ alors n est premier donc G est cyclique.

* si $|G| = 4$.

1^{er} cas: G contient un élément d'ordre 4 donc il est cyclique d'après 2. a.

2^{er} cas: G ne contient aucun elt d'ordre 4.

$\forall u \in G, o(u)$ divise $|G| = 4$.

$$\Rightarrow o(u) \in \{1, 2, 4\}.$$

$$\Rightarrow o(u) \in \{1, 2\} \text{ car } o(u) \neq 4.$$

$$\Rightarrow u^2 = e.$$

donc G est abélien, d'après 1°).

Cl. si $|G| \leq 5$ alors G est abélien.

d) on prend $G = S_3$: le gpe symétrique d'ordre 3.

$$|G| = 3! = 6.$$

soient $\tau = \tau_{12} = (1\ 2)$ et $\sigma = (1\ 2\ 3)$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ et } \sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & . & . \end{pmatrix}$$

$$\tau\sigma(1) \neq \sigma\tau(1) \text{ donc } \tau\sigma \neq \sigma\tau$$

on a S_3 est un gpe d'ordre 6, non abélien.

De toute la suite; $|G| = n \in \mathbb{N}^*$ et $u^2 = e$

$\forall n \in G$ (G est donc abélien)

on se propose de montrer que n est une puissance de 2

3) H s.o. de G ; $aH = \{ah, h \in H\}$, $H_a = H \cup aH$.

a) Soit $a \in G$.

$$f_a: H \longrightarrow aH$$

$$f_a: h \longmapsto ah.$$

* $\forall n \in aH$; $\exists h \in H$ tq $n = ah = f_a(h)$
donc f_a est surjective par construction.

* Soit $h, h' \in H$ tq $f_a(h) = f_a(h')$

$$\text{donc } a \cdot h = a \cdot h'$$

$$\Rightarrow a^{-1}a h = a^{-1}a h' \Rightarrow h = h'$$

d'où f_a est injective.

on si f_a est une bijection de H sur aH .

b) si $a \in H$ alors $a h \in H \quad \forall h \in H$

$$\text{donc } aH \subseteq H$$

de plus $|aH| = |H|$ car f_a est bijective

$$\text{donc } aH = H$$

$$\text{c) } a \notin H$$

$$\emptyset \neq H \subset H \cup aH = Ha \Rightarrow Ha \neq \emptyset.$$

$$\text{Soit } u, y \in Ha, \text{ on a } u \cdot y^{-1} \in Ha.$$

$$\underline{1^{\text{er}} \text{ cas:}} \quad u, y \in H \Rightarrow u \cdot y^{-1} \in H \subset Ha \text{ car } H < G.$$

$$\underline{2^{\text{e}} \text{ cas:}} \quad u, y \in a \cdot H.$$

$$u = ah \text{ et } y = ah' \text{ avec } h, h' \in H.$$

$$u \cdot y^{-1} = u y \quad \text{car } y^2 = e.$$

$$= a h a h'$$

$$= a^2 h h' \text{ car } G \text{ abélien.}$$

$$= h h' \in H \subset Ha \text{ car } a^2 = e.$$

$$\underline{3^{\text{e}} \text{ cas:}} \quad u \in H \text{ et } y \in aH$$

$$u y^{-1} = u y = u a h, \quad h \in H.$$

$$= a u h \in aH \text{ car } u h \in H.$$

$$\text{donc } u y^{-1} \in aH \cup H = Ha.$$

on a: Ha est un sous-groupe de G .

$$* \text{ on a } |Ha| = 2|H|.$$

on a fa: $H \longrightarrow aH$ est une bijection

$$\text{donc } |H| = |aH|.$$

$$\begin{aligned} \Rightarrow |Ha| &= |H \cup aH| = |H| + |aH| - |H \cap aH| \\ &= 2|H| - |H \cap aH|. \end{aligned}$$

$$\text{Soit } n \in H \cap aH. \Rightarrow \begin{cases} n \in H \\ n = ah, h \in H. \end{cases}$$

$$\Rightarrow a = nh^{-1} \in H \text{ (impossible)}$$

$$\text{donc } H \cap aH = \emptyset$$

$$\text{ou si } |Ha| = 2|H|.$$

$$4) G = \{e, u_2, \dots, u_n\}; G_1 = \{e\} \text{ et } G_{i+1} = G_i \cup u_{i+1} G_i, 1 \leq i \leq n-1.$$

$$g) \text{ pour } i=1; G_1 = \{e\} \text{ est un sous-groupe de } G \text{ et } |G_1| = 1 = 2^0$$

$$\text{Soit } i \in \{1, \dots, n-2\}.$$

$$\text{on suppose que } G_i \text{ est un s.g de } G \text{ d'ordre } 2^{n_i}$$

$$\text{si } u_{i+1} \in G_i \text{ alors } G_{i+1} = G_i \text{ est un s.g de } G$$

$$\text{d'ordre } 2^{n_i}$$

$$\text{si } u_{i+1} \notin G_i \text{ alors } G_{i+1} \text{ est un s.g de } G \text{ d'ordre}$$

$$2|G_i| = 2 \cdot 2^{n_i} = 2^{n_i+1}$$

$$\text{on si } G_i \text{ est un s.g de } G \text{ d'ordre } 2^{n_i}, n_i \in \mathbb{N}.$$

$$\text{il est clair que } G_1 \subset G_2 \subset \dots \subset G_n \subset G.$$

$$\text{d'autre part } e \in G_n.$$

$$\text{et } \forall i \in [1, n-1]; u_{i+1} \in u_{i+1} G_i \subset G_{i+1} \subset G_n$$

$$\text{donc } G \subset G_n \text{ et par suite } G_n = G.$$

$$g) n = |G| = |G_n| = 2^{n_n} = 2^k; k = m_n \in \mathbb{N}.$$