

I-Groupes =

* **sous groupe** : si $(G, *)$ est un grp et $H \subset G$ et un s.g de G si :

$$\text{si} = \begin{cases} \textcircled{1} e \in H \quad (H \neq \emptyset) \\ \textcircled{2} \forall x, y \in H, \underbrace{x * y^{-1}}_{x * y \in H \text{ et } y^{-1} \in H \text{ (a en 1)}} \in H \end{cases}$$

$\Rightarrow (H, *)$ est un groupe.

Th = H est un s.g de $(\mathbb{Z}, +)$ si : $\exists a \in \mathbb{N}$ tq :

$$H = a \cdot \mathbb{Z}$$

Th = l'intersection qdq de s.g est un s.g.

* **Morphisme de grp** = soient $(G, *)$, (G', τ) 2 grps on dit que :

$f: (G, *) \longrightarrow (G', \tau)$ est un morphisme de grp si

$$\forall x, y \in G, \{ f(x * y) = f(x) \tau f(y) \}$$

- Prop = si e, e' les neutres de G et G' et f morphisme de $G \rightarrow G'$

$$\textcircled{1} f(e) = e'$$

$$\textcircled{2} (f(x))^{-1} = f(x^{-1})$$

$$\textcircled{3} f(\underbrace{x * x * \dots * x}_{n \text{ fois}}) = \underbrace{f(x) \tau f(x) \tau \dots \tau f(x)}_{n \text{ fois}}$$

$\textcircled{4}$ si H s.g de G alors : $f(H)$ s.g de G'

⊙ si k s.g. de G' alors: $f^{-1}(k)$ s.g. de G .

* noyau de morphisme:

$$\text{Ker}(f) = \{ x \in G \text{ tq: } f(x) = e' \} = f^{-1}(\{e'\})$$

* image de morphisme:

$$\text{Im}(f) = \{ f(x) \mid x \in G \} = f(G)$$

Prop:

⊙ f injective si: $\text{Ker } f = \{e\}$

⊙ f surjective si: $\text{Im } f = G'$

Déf: $f: G \rightarrow G'$ morphisme

⊙ si $G = G'$: f est endomorphisme.

⊙ si f bijective: f isomorphisme.

⊙ si $G = G'$ et f bij: f automorphisme.

* sous grp engendré par élt:

$A \subset G$, $\langle A \rangle$: s.g. engendré par A (le plus petit s.g. de A contenant A)

$$A = \bigcap \begin{matrix} H \\ H \text{ s.g. } G \\ A \subset H \end{matrix}$$

⊙ si H s.g. de G tq: $A \subset H$ alors $\langle A \rangle \subset H$

⊙ si A s.g. de G : $\langle A \rangle = A$

$$\langle \emptyset \rangle = \{e\} \quad / \quad \langle e \rangle = \{e\}$$

Not^e: itérée d'un élt : $(G, *)$ un grp et $x \in G$:

notation multiplicative =

$$x^n = \begin{cases} \underbrace{x * x * \dots * x}_{n \text{ fois}} & \text{si } n > 0 \\ e & \text{si } n = 0 \\ \underbrace{x^{-1} * x^{-1} * \dots * x^{-1}}_{-n \text{ fois}} & \text{si } n < 0 \end{cases}$$

notation additive :

$$n \cdot x = \begin{cases} \underbrace{x + x + \dots + x}_{n \text{ fois}} & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ \underbrace{-x - x \dots - x}_{-n \text{ fois}} & \text{si } n < 0 \end{cases}$$

⚠: soit $x \in G$:

$$\langle x \rangle = \{ x^n, n \in \mathbb{Z} \}$$

* ordre d'elt dans un grp =

$$o(x) = \min \{ k \in \mathbb{N}^* / x^k = e \}$$

la plus petite puissance de x qui donne e .
non nulle

Prop = $x \in G$ tq: $o(x) = d$

⊙ $x^m = e \Leftrightarrow d/m$

⊙ $\langle x \rangle = \{ e, x, \dots, x^{d-1} \}$

⊙ si $\text{card}(\underbrace{G}_{\text{fini}}) = n$, $\forall x \in G$, $\langle x \rangle$ d'ordre fini et $o(x) \mid n$

Th = Lagrange = si $(G, *)$ grp tq $\text{card}(G)$: fini
si H sq de G alors $\text{card}(H)$ fini et :

$$\frac{\text{card}(H)}{\text{card}(G)} = \frac{\theta(H)}{\theta(G)}$$

* Groupe monogène - cyclique =

on dit que G est monogène si :

$$\exists a \in G \text{ tq : } G = \langle a \rangle$$

si de plus G est fini : G est cyclique.

II - Anneaux:

* **Anneau** = $(A, +, \times)$ si :

- ① $(A, +)$ grp abélien de neutre 0_A
- ② $\times$ associative de neutre 1_A
- ③ $\times$ est distributive sur $+$: $\forall a, b, c \in A$
 $a(b+c) = ab + ac$
 $(b+c)a = bc + ca$

△: si $\times$ est commutative on dit: l'anneau $(A, +, \times)$ est commutatif.

* **sous-anneau**: $(A, +, \times)$ anneau

$(B, +, \times)$ s. anneau de A si: $B \subset A$

- ① $1_A \in B$ (contient le neutre de la loi $\times$)
- ② $\forall x, y \in B, xy \in B$ (stable par la loi $\times$)
- ③ $\forall x, y \in B, x - y \in B$

* **les inversibles** = $a \in (A, +, \times)$

a est inversible si: $\exists b \in A$ tq: $ab = ba = 1$
 b alors est unique noté a^{-1} : inverse de a .

Th: **$U(A)$** : l'ensemble des élt inversibles de l'anneau $(A, +, \times)$, est un grp multiplicatif.
 $(U(A), \times)$ est un grp.

* Produit fini d'anneaux:

soient $(A_1, +, \times), \dots, (A_n, +, \times)$ des anneaux.

$\|A = A_1 \times \dots \times A_n\|$, on définit les lois $+$ et $\times$ sur

$$A \text{ tq : } \odot (x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

$$\odot (x_1, \dots, x_n) \times (y_1, \dots, y_n) = (x_1 \times y_1, \dots, x_n \times y_n)$$

$\Rightarrow (A, +, \times)$ est un anneau de neutre :

$$\underline{0_A = (0_{A_1}, \dots, 0_{A_n})} \text{ et } \underline{1_A = (1_{A_1}, \dots, 1_{A_n})}$$

* $(a_1, \dots, a_n) \in A$ est inversible ssi $a_1, \dots, a_n$ sont inversibles et son inverse: $(a_1^{-1}, \dots, a_n^{-1})$

$$\triangle: U(A) = U(A_1) \times \dots \times U(A_n)$$

- Exemple = $(\mathbb{Z}^2, +, \times)$ est un anneau commutatif où:

$$\begin{cases} (a, b) + (c, d) = (a+c, b+d) \\ (a, b) \times (c, d) = (a \cdot c, b \cdot d) \end{cases} \quad \left| \quad U(\mathbb{Z}) = \{ (1, 1), (-1, 1) \}$$

de neutre $(0, 0)$ et $(1, 1)$

$$U(\mathbb{Z}^2) = \{ (1, 1), (-1, 1), (1, -1), (-1, -1) \}$$

* Diviseurs de zéro: on sait que =

$$\forall a, b \in A, a = 0_A \text{ ou } b = 0_A \Rightarrow ab = 0_A$$

$\rightarrow$ la réciproque est pas toujours vraie.

$$(\mathbb{Z}^2, +, \times): (1, 0) \times (0, 1) = (0, 0)$$



Déf: si $a, b \in A$ tq: $ab = 0_A$ avec $a, b \neq 0_A$
on dit que: a et b sont des diviseurs de zéro.

$(A, +, \times)$ est intégrale: $\begin{cases} \textcircled{1} A \neq \{0_A\} \\ \textcircled{2} \forall a, b \in A, ab = 0_A \rightarrow a = 0_A \text{ ou } b = 0_A \end{cases}$
- exp: $[K[x] \text{ est intégrale}]$
 $[M_n(\mathbb{R}) \text{ n'est pas intégrale}]$
ne possède pas des diviseurs de zéro.

*** Corps:** on appelle corps tt anneau $(K, +, \times)$ tq:
 $\begin{cases} \textcircled{1} (K, +, \times) \text{ est commutatif} \\ \textcircled{2} K \neq \{0_A\} \\ \textcircled{3} \forall \text{ élt de } K, \text{ non nul, est inversible.} \end{cases}$
corps usuels:
 $\begin{pmatrix} \mathbb{Q} / +, \times \end{pmatrix}$
 $\begin{pmatrix} \mathbb{R} / +, \times \end{pmatrix}$
 $\begin{pmatrix} \mathbb{C} / +, \times \end{pmatrix}$

*** sous-corps:** $(K, +, \times)$ est un corps.

on appelle $(L, +, \times)$ s. corps de K si:

$\begin{cases} \textcircled{1} L \text{ est un s. anneau de } (K, +, \times) \\ \textcircled{2} \forall x \in L, x \neq 0_K \rightarrow x^{-1} \in L \end{cases}$ a et b inversibles.

⚠: tout corps est intégrale.

$$\begin{aligned} ab &= 0 \\ a^{-1}a \cdot bb^{-1} &= 0 \\ 1 &= 0 \quad \text{absurde} \end{aligned}$$

• si a est inversible: il n'est pas diviseurs de zéro

*** morphisme d'anneaux:** $(A, +, \times)$ et $(A', +, \times)$ des anneaux
 $f: A \rightarrow A'$ est un morphisme si:

$\begin{cases} \textcircled{1} f(1_A) = 1_{A'} \\ \textcircled{2} \forall x, y \in A, f(x+y) = f(x) + f(y) \\ \textcircled{3} \forall x, y \in A, f(xy) = f(x)f(y) \end{cases}$

* les idéaux = $(A, +, \times)$ anneau commutatif.

on appelle idéal de A , tt partie I de A tq: $(I, +)$

- $\left\{ \begin{array}{l} \textcircled{1} 0_A \in I \\ \textcircled{2} \forall x, y \in I, x+y \in I \\ \textcircled{3} \forall a \in A, \forall x \in I, ax \in I \text{ (absorption)} \end{array} \right\}$
- $(I, +)$ s.g. $\xrightarrow{\text{exp}} n\mathbb{Z}$ est un idéal de A $\left[\begin{array}{l} \text{Ker } f \text{ est un idéal} \\ \text{morphisme} \end{array} \right]$

Δ : un idéal est un s.g. $(I, +)$ (on prend $a = -1$ en (3))

• si $1_A \in I \Rightarrow I = A$

• si $I \cap U(A) \neq \emptyset \Rightarrow I = A$: I contient un élt inversible

Δ : on dit que: a divise b $\Rightarrow$ idéaux de corps = $\{0_K\}$ ou $= K$
dans A :

si $\exists c \in A$ tq: $b = ac$

on note: $aA = \{ax, x \in A\}$

un idéal: engendré par a .

Th = les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$

Th = les idéaux de $K[x]$ sont de la forme: $P \mid K[x]$
avec: $P \in K[x]$

* d'ensemble $\mathbb{Z}/n\mathbb{Z}$:

* soit $n \in \mathbb{N}^*$, $a \equiv b [n] \Leftrightarrow n \mid (b-a)$

$\equiv$: est une relation d'équivalence sur $\mathbb{Z}$.

* soit $a \in \mathbb{Z}$, $\bar{a}$: la classe d'équivalence de a

$$\bar{a} = \{ b \in \mathbb{Z}, \begin{matrix} a \equiv b [n] \\ b \equiv a [n] \end{matrix} \} = \{ a + nk, k \in \mathbb{Z} \}$$

- Exp : $a \equiv b [3] \Leftrightarrow 3 \mid b-a$ $= a + n\mathbb{Z}$

$$\bar{4} = \{ b \in \mathbb{Z}, 4 \equiv b [3] \} = \{ 1, 4, 7, 10, \dots \} \Rightarrow \bar{4} = \bar{1} = \bar{7}$$

1 $\mathbb{Z}/n\mathbb{Z}$: les classes d'éq de $\mathbb{Z}$ pour la relation $\equiv [n]$
c'est un ensemble fini à n élts qui sont :

$$\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}$$

Th : $\forall a, b, a_0, b_0 \in \mathbb{Z}$, $a \equiv a_0 [n]$ et $b \equiv b_0 [n]$

alors : $a+b \equiv a_0+b_0 [n]$ et $ab \equiv a_0b_0 [n]$

⚠ : on définit 2 lois $^+ \quad ^\times$ sur $\mathbb{Z}/n\mathbb{Z}$ tq :

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{et} \quad \bar{a} \times \bar{b} = \overline{ab}$$

* de groupe $\mathbb{Z}/n\mathbb{Z} = (\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien
à n élts de neutre $\bar{0}$.

* $\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}$, $-\bar{a} = \overline{-a}$ et $\forall k \in \mathbb{Z}$, $k\bar{a} = \overline{ka}$

* $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique et $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$

* des générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont : $\bar{m} \quad \forall m \in \mathbb{Z}$

$$m \in \mathbb{Z}, m \wedge n = 1 \Rightarrow \mathbb{Z}/n\mathbb{Z} = \langle \bar{m} \rangle \quad \text{avec } m \wedge n = 1$$

si m est premier $\Rightarrow \forall m \in \mathbb{Z}^*, \mathbb{Z}/n\mathbb{Z} = \langle \bar{m} \rangle$

$$\text{si } n \text{ multiple de } n \Rightarrow \bar{a} = \bar{0} \quad \left| \quad \mathbb{Z}/6\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{5} \rangle$$

Th: $(G, *)$ groupe monogène
infini

(1) $\rightarrow$ si $\text{card}(G) = +\infty$ alors $(G, *)$ est isomorphe
à $(\mathbb{Z}, +)$: $\exists$ f morphisme de grp bijectif
tq: $f: (\mathbb{Z}, +) \rightarrow (G, *)$

(2) $\rightarrow$ si $\text{card}(G) = n \in \mathbb{N}^*$ alors $(G, *)$ est isomorphe
fini: (cyclique) à $(\mathbb{Z}/n\mathbb{Z}, +)$: $\exists$ f morphisme
de grp bijectif tq: $f: (\mathbb{Z}/n\mathbb{Z}, +) \rightarrow (G, *)$

(1): soit $G = \langle a \rangle$

$$f: \mathbb{Z} \rightarrow G \quad \text{mq } f \text{ morphisme + bij} \quad f: \mathbb{Z} \rightarrow G$$

$$k \mapsto a^k$$

$$* f(k+k') = a^{k+k'} = a^k \times a^{k'} = f(k) \times f(k') = \text{morphisme}$$

$$* \forall b \in G, b = a^k = f(k) : \text{surj}$$

$$\exists k \in \mathbb{Z}$$

$$* \text{Ker } f = \{ k \in \mathbb{Z} \text{ tq } f(k) = e_G \} : \text{sg de } \mathbb{Z} = n\mathbb{Z}$$

(2): $f': \mathbb{Z}/n\mathbb{Z} \rightarrow G$

$$f'(\bar{k}) = a^k \quad \text{morphisme}$$

$$* f'(k+k') = a^{k+k'} = a^k \cdot a^{k'} = f(k) \cdot f(k')$$

$$* \text{Ker } f' = \{ \bar{k} \in \mathbb{Z}/n\mathbb{Z} \text{ tq } a^k = e_G = 1 \} = \{ \bar{0} \}$$

$$* \text{Im } f' = \{ a^k / k \in \mathbb{Z} \} = G \Rightarrow \text{bij}$$

si $n=0$:

f inj
 $\hookrightarrow$ bij

si $n \neq 0$:

$$f(k) = f(k')$$

$$k - k' \in \text{Ker } f$$

$$a^k = a^{k'}$$

$$k \equiv k' [n]$$

$$\bar{k} = \bar{k'}$$

* L'anneau: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

$\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif de neutres $\bar{0}$ et $\bar{1}$.

Dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, $\bar{m}$ est inversible ssi: $m \wedge n = 1$

$\bar{m}$ inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \exists \bar{k} \in \mathbb{Z}/n\mathbb{Z}$ tq: $\bar{m}\bar{k} = \bar{1}$

$$\Leftrightarrow \exists k \in \mathbb{Z} \text{ tq: } mk \equiv 1[n]$$

$$\Leftrightarrow \exists k \in \mathbb{Z} \text{ tq: } n \mid mk - 1$$

$$\Leftrightarrow \exists k \in \mathbb{Z}, k' \in \mathbb{Z} \text{ tq: } mk + nk' = 1$$

identité de Bezout $\Leftrightarrow \underline{\underline{m \wedge n = 1}}$

si $m \wedge n = 1$ alors $(\bar{m})^{-1} = \bar{u}$
 $(mu + nv = 1)$
 Bezout

Th: $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps } ssi: p est premier
 un anneau intègre

$\mathbb{Z}/p\mathbb{Z}$ corps, $a \in \{2, \dots, p-1\}$
 $\bar{a}$ inversible $\Rightarrow \bar{a} \neq \bar{0}$

$a \wedge p = 1$, $a \not\equiv 0 \pmod{p} \Rightarrow p$ premier

p premier, $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{p-1}\}$

$\forall k \in \{2, \dots, p-1\} \Rightarrow p \wedge k = 1$

$\Rightarrow \bar{k}$ est inversible

$\Rightarrow \mathbb{Z}/p\mathbb{Z}$ est un corps

p premier: soit $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$ tq: $\bar{a} \cdot \bar{b} = \bar{0} \Rightarrow \bar{a}\bar{b} = \bar{0}$

$\Rightarrow p \mid ab$ or premier $\begin{cases} p \mid a \\ \text{ou} \\ p \mid b \end{cases}$
 $\Rightarrow \bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$

supp p n'est pas premier =
 $\exists 1 < a, b < p$ tq: $p = ab$
 $\bar{p} = \bar{a} \cdot \bar{b} = \bar{a}\bar{b}$ or $\bar{p} = \bar{0}$

$\Rightarrow \bar{a}\bar{b} = \bar{0}$ or $\bar{a} \neq \bar{0}$
 $\bar{b} \neq \bar{0}$

$\Rightarrow \mathbb{Z}/p\mathbb{Z}$ n'est pas intègre.

Th du reste chinois = si $m \wedge n = 1$

alors:

$$f: \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$f(\bar{k}) = (\hat{k}, \bar{k})$ est un isomorphisme d'anneaux.

notation: $k \in \mathbb{Z}$

$$\bar{k} \in \mathbb{Z}/mn\mathbb{Z}$$

$$\hat{k} \in \mathbb{Z}/m\mathbb{Z}$$

$$\bar{k} \in \mathbb{Z}/n\mathbb{Z}$$

→ conséquence: un système de type =

$$\begin{cases} x \equiv a [m] \\ x \equiv b [n] \end{cases} \quad \text{avec: } m \wedge n = 1$$

$$f: \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$\bar{x} \longmapsto (\hat{x}, \bar{x})$$

$$(\bar{a}, \bar{b}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \exists! x \in \mathbb{Z}/mn\mathbb{Z} \text{ tq: } f(\bar{x}) = (\bar{a}, \bar{b})$$

$$\exists! x \in \mathbb{Z}/mn\mathbb{Z} \text{ tq: } \begin{cases} x \equiv a [m] \\ x \equiv b [n] \end{cases}$$

$$\rightarrow y = x + mnk, k \in \mathbb{Z}$$

① sol^{ie} particulière: $nv + mu = 1$

* Algèbre = $(A, +, \times, \cdot)$ "+" et "x" lci

1/ $(A, +, \times)$ anneau

2/ $(A, +, \cdot)$ e.v

$$3/ \alpha \cdot (x \times y) = (\alpha \cdot x) \times y = x \times (\alpha \cdot y)$$

sous algèbre =

B C A

$$\textcircled{1} 1_A \in B$$

$$\textcircled{2} x \times y \in B$$

$$\textcircled{3} \alpha \in K, \alpha x + y \in B$$

→ morphisme d'algèbre: $f: A \rightarrow A'$

$$1/ f(1_A) = 1_{A'}$$

$$2/ f(x \times y) = f(x) \times f(y)$$

$$3/ f(\alpha x + y) = \alpha f(x) + f(y)$$