

I) Rapports

1) Groupes

a/ Définition: $(G, *)$ groupe \Leftrightarrow $\begin{cases} G \neq \emptyset, \text{ avec } * \text{ loi de composition interne.} \\ * \text{ associative} \\ * \text{ admet } e \text{ neutre} \\ \forall x, \exists \text{ un symétrique } x^{-1}. \end{cases}$ Et, si $*$ est commutative, G est "abelien".

b/ Exemples: $(M_n(K), +)$; $(GL_n(K), \cdot)$; $(\mathbb{Z}(E), +)$; $(GL(E), \cdot)$.

c/ Ordre: Si G est fini, card $G = |G|$ est défini et se nomme aussi "ordre du groupe".

2) Sous-groupes:

a/ Définition: (G, \cdot) un groupe. H une partie de G est un sous groupe de $G \Leftrightarrow \begin{cases} H \neq \emptyset \\ H \text{ stable pour } \cdot, \forall x, y \in H, xy \in H \\ (H, \cdot) \text{ un groupe} \end{cases}$

Caractérisation: H ss. gpe de $G \Leftrightarrow \begin{cases} H \neq \emptyset \\ \forall (x, y) \in H^2, xy \in H \\ \forall x \in H, x^{-1} \in H \end{cases} \Leftrightarrow \begin{cases} H \neq \emptyset \\ \forall (x, y) \in H^2, xy^{-1} \in H \end{cases}$

b/ Exemples: $\{0\}$ ss gpe de (\mathbb{C}^*, \cdot)

\mathbb{R}^* ss gpe de $(\mathbb{C}, +)$

\mathbb{R}^* ss gpe de (\mathbb{R}^*, \cdot)

Propriété: les sous groupes de $(\mathbb{Z}, +)$ sont les $m\mathbb{Z}$, $m \in \mathbb{Z}$.

3) Morphisme de groupes.

a/ Définition: (G, \cdot) et (G', \cdot) deux sous-groupes. $f: G \rightarrow G'$ est un morphisme de gpe $\Leftrightarrow \forall x, y \in G, f(xy) = f(x) \cdot f(y)$.

b/ Propriétés: $\text{Im } f = f(G)$ est un ss gpe de G'

$\text{Ker } f$ est un ss gpe de G .

c/ Exemples: $\text{Ln}: (\mathbb{R}^*, \cdot) \rightarrow (\mathbb{R}, +)$ est un morphisme de groupe, et comme Ln est bijectif, c'est un isomorphisme.

Inv est la morphisme réciproque de Ln .

$(\mathbb{C}^*, \cdot) \xrightarrow{\psi} (\mathbb{R}^*, \cdot)$, avec $\text{Ker } \psi = \mathbb{U}$.

$z \mapsto |z|$

$(GL(E), \cdot) \xrightarrow{\varphi} (\mathbb{C}^*, \cdot)$, car $\det uov: \det u \cdot \det v = \det(u \circ v)$
 $u \mapsto \det u$

Δ On notera que $\text{Ker } \varphi = \{u \in GL(E) \mid \det u = 1\} = SL(E)$ est le groupe spécial linéaire de E .

4) Sous-groupe monogène, ss gpe cyclique.

Soit (G, \cdot) un groupe, et $a \in G$.

Soit le morphisme $\varphi_a: \begin{cases} \mathbb{Z} \rightarrow (G, \cdot) \\ k \mapsto a^k \end{cases}$

$\text{Ker } \varphi_a$ est de la forme $m\mathbb{Z}$.

$\text{Im } \varphi_a = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ sous-groupe engendré par a .

On le nomme sous-groupe monogène de G .

Si $|\langle a \rangle|$ est fini, c'est un sous-groupe cyclique de G .

ex: $(\mathbb{Z}, +) = \langle 1 \rangle$ est monogène.

$\forall n, \mathbb{U}_n = \{e^{i \frac{2\pi k}{n}} \mid k \in [0, n-1]\}$ monogène cyclique de (\mathbb{C}^*, \cdot) et engendré par $e^{i \frac{2\pi}{n}}$

$\mathbb{U}_n = \langle e^{i \frac{2\pi}{n}} \rangle$

5) Produit de deux groupes

Soit (G, \cdot) et (H, \cdot) deux groupes. On définit $(G \times H, \cdot)$ avec la loi: $(x, y) \cdot (x', y') = (xx', yy')$

ex: $\mathbb{U}_2 \times \mathbb{U}_2$ gpe produit à 4 éléments. Groupe de Klein.

II) Sous groupe engendré par une partie1) Définition:

a/ Propriété (évidente): Si (G, \cdot) est un gpe, toute N de ss gpes de G est un sous-gpe de G .

b/ DEF: Soit $A \subset G$. H est le ss gpe engendré par A dans $G \Leftrightarrow H = \bigcap_{F \text{ ss gpe de } G} F = \langle A \rangle$

F ss gpe de G
 $A \in F$

ex: $A = \emptyset$ donc $\langle \emptyset \rangle = \{e\}$.

2) Cas où $A = \{a\}$:

Propriété: $\langle \{a\} \rangle = \{a^k \mid k \in \mathbb{Z}\} = \langle a \rangle$.

3) Cas général avec $A \neq \emptyset$. Description de $\langle A \rangle$

Propriété: $\langle A \rangle$ est constitué de l'ens. des produits $a_1 \dots a_n$ ($n \geq 1$) où $\forall i, a_i \in A$ ou $a_i^{-1} \in A$.

4) Définition:

lorsque $\langle A \rangle = G$, on dit que A est une partie "génératrice" de G , ou que " A engendre G ".

III) Théorème de Lagrange : Si G est un gpe fini et si H sous-gpe de G , alors $\text{card}(H)$ divise $\text{card}(G)$.

1) RST associés à un sous-gpe.

a/ Relation d'équivalence à gauche : Soit H sous-gpe de G , on définit $R_g(H)$ sur G : $x R_g y \Leftrightarrow x^{-1}y \in H$.

b/ Définition : les classes d'équivalence modulo $R_g(H)$ s'appellent les classes à gauche de G modulo H .

. Classe à gauche de $x \in G$: $\{y \in G / x^{-1}y \in H\} = xH$.

. L'ens. quotient $(G/R_g(H))$ est l'ens. des classes d'équivalence.

c/ On définit de même R_d : $x R_d y \Leftrightarrow xy^{-1} \in H$.

2) Compatibilités : la relation R_g est compatible avec la loi de G ($x R_g y \Rightarrow (ax) R_g (ay)$)

3) Indice de H dans G :

. Propriété : $G/R_g(H)$ et $G/R_d(H)$ sont en bijection.

. Définition : En cas fini, ces ensembles ont le même cardinal noté $[G:H]$. On nomme cette grandeur "indice" dans G .

4) Théorème : Si G est un gpe fini et H un sous-gpe de G , alors $\text{card } G = \text{card } H \times [G:H]$.

. Conséquences : $\begin{cases} \text{Si } G \text{ est fini, } \forall a \in G, \text{ card } \langle a \rangle / \text{card } G \\ \text{Si } G \text{ est fini et de cardinal } p \text{ premier, alors } G \text{ est cyclique.} \end{cases}$

IV) $(\mathbb{Z}/n\mathbb{Z}, +)$

1) Relation de congruence.

Dans le cas des $(n\mathbb{Z})$, les relations R_d et R_g sont égales et s'appellent "relation de congruence".

On note : $x \equiv y [n]$.

2) L'ens. quotient $\mathbb{Z}/n\mathbb{Z}$ est l'ens. des classes de congruence modulo n .

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ et $\text{card}(\mathbb{Z}/n\mathbb{Z}) = n$.

3) Structure de groupe sur $\mathbb{Z}/n\mathbb{Z}$: $\bar{x} + \bar{y} = \overline{x+y}$

. Théorème : $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif (abélien).

4) Morphisme de \mathbb{Z} dans $\mathbb{Z}/n\mathbb{Z}$.

$$p \begin{cases} \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \\ x \mapsto \bar{x} \end{cases}$$
 est un morphisme de groupes additifs. C'est le morphisme canonique de \mathbb{Z} sur $\mathbb{Z}/n\mathbb{Z}$.
Il est surjectif, et $\text{Ker}(p) = n\mathbb{Z}$.

V) Application aux gpes monoïdes et cycliques

1) $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique.

En effet, car $\langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z}$ et que $|\mathbb{Z}/n\mathbb{Z}| = n$.

2) Théorème :

Soit $\langle a \rangle$ un gpe monoïde et $p_a \begin{cases} \mathbb{Z} \rightarrow \langle a \rangle \\ k \mapsto a^k \end{cases}$, de noyau $n\mathbb{Z}$ avec $n > 0$.
 $\begin{cases} \text{Si } n=0, \langle a \rangle \text{ est infini et isomorphe à } (\mathbb{Z}, +) \\ \text{Si } n>0, \langle a \rangle \text{ est fini et isomorphe à } (\mathbb{Z}/n\mathbb{Z}, +) \end{cases}$

3) Ordre d'un élément de $\mathbb{Z}/n\mathbb{Z}$.

a/ Soit $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ avec $x \in \mathbb{Z}$. L'ordre de \bar{x} est $\frac{n}{\text{pgcd}(n, x)}$.

b/ Générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$:

\bar{x} générateur de $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \langle \bar{x} \rangle = \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \text{card} \langle \bar{x} \rangle = n \Leftrightarrow \frac{n}{\text{pgcd}(n, x)} = n \Leftrightarrow \text{pgcd}(n, x) = 1$.

. On note ϕ l'indicateur d'Euler, tq $\phi(n)$ = nombre d'entiers premiers avec n .

4) Sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$.

$\forall p \in \text{diviseurs de } n, \exists ! \text{ sous-gpe } H \text{ de } \mathbb{Z}/n\mathbb{Z} \mid \text{card } H = p$.

1) Groupes quotients

- a) Rappel : Soit (G, \cdot) un gpe et H un sous-groupe de G . On associe à H les relations R_H et R_H sur G tq : $\begin{cases} x R_H y \Leftrightarrow x^{-1}y \in H \\ x R_H y \Leftrightarrow x y^{-1} \in H \end{cases}$
On en déduit si G est fini que : $\text{card } G = \text{card } H \times (\text{nombre de classes à gauche})$
 $\text{card } G = \text{card } H \times [G:H]$

2) Sous-groupes distingués : Remarquons que $R_H = R_H \Leftrightarrow \forall x \in G, xH = Hx$.

- a) Définition : H un sous-groupe de G est dit distingué ssi $\forall x \in G, xH = Hx$. On note $H \triangleleft G$.
b) Théorème : Soit $f: G \rightarrow G'$ un morphisme de groupes, alors $\text{Ker } f \triangleleft G$.
c) Exemples : $G \triangleleft G$; $\{e\} \triangleleft G$; Si G commutatif, alors tout sous-groupe est distingué;

$$\Leftrightarrow \begin{cases} \forall x \in G, xH = Hx \\ \forall x \in G, xHx^{-1} = H \\ \forall x \in G, xHx^{-1} \subset H \end{cases}$$

3) Groupes quotients

- a) Théorème : $(G/H, \cdot)$ est un groupe, nommé groupe quotient de G par H et noté G/H , ssi H est distingué dans G .
b) Projection canonique : Soit $H \triangleleft G$ et $p: G \rightarrow G/H$ la projection $p: x \mapsto xH$. La projection p est un morphisme de groupes surjectif et de noyau H .
c) Théorème de passage au quotient : $f: G \rightarrow G'$ morphisme de gpe, et $H \triangleleft G$ tq $H \subset \text{Ker } f$. Alors, $\exists ! \bar{f}: G/H \rightarrow G'$ tq $f = \bar{f} \circ p$.
• Propriété : $\text{Im } \bar{f} = \text{Im } f$; \bar{f} injective $\Leftrightarrow \text{Ker } f = H \Leftrightarrow \bar{f}$ bijective; $G/\text{Ker } f \cong \text{Im } f$.

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ p \downarrow & & \uparrow \bar{f} \\ G/H & & \end{array}$$

4) Application aux corps de $(\mathbb{Z}/\mathbb{Z})^*$

- a) Propriété : Soit p premier, et $\mathbb{Z}/\mathbb{Z} = \mathbb{F}_p$ est un corps. Dans \mathbb{F}_p^* , il y a $\frac{p-1}{2}$ carrés et $\frac{p-1}{2}$ non carrés (p impair).
b) Caractérisation des carrés : x carré de $\mathbb{F}_p^* \Leftrightarrow x^{\frac{p-1}{2}} = 1$.

II) Conjugaison

1) Automorphisme d'un gpe

- a) Définition : un automorphisme du gpe G est un morphisme de G sur G , bijectif, de $G \rightarrow G$. L'ens. $\text{Aut}(G)$ constitue un gpe pour la loi \circ , image de (f, e) , e l'ens. des bijections de G dans lui-même.

- b) Automorphisme intérieur : Soit $a \in G$. L'application $\varphi_a: \begin{cases} G \rightarrow G \\ x \mapsto \varphi_a(x) = axa^{-1} \end{cases}$ est un automorphisme de G , dit "intérieur".
On remarque que $(\varphi_a)^2 = \text{id}_G$.

- c) Intérieur de G : $\text{Int}(G)$ est l'ensemble des automorphismes intérieurs de G . $\text{Int}(G) \subset \text{Aut}(G)$.

- Propriété : L'application $\varphi: \begin{cases} G \rightarrow \text{Aut}(G) \\ a \mapsto \varphi(a) = \varphi_a \end{cases}$ est un morphisme de groupes.

- Corollaire : $\text{Int}(G) = \text{Im } \varphi$ est un sous-groupe de $(\text{Aut}(G), \circ)$.

Soit $Z = \{x \in G / \forall y \in G, xy = yx\}$ le centre de G . $\text{Ker } \varphi = Z$. $G/Z \cong \text{Int}(G)$.

Si G est abélien, alors $\text{Int}(G) = \{id\}$.

2) Éléments conjugués

- a) Définition : x et y sont conjugués dans $G \Leftrightarrow \exists a \in G / y = \varphi_a(x) = axa^{-1}$. C'est une RST sur G .

- et qn vérifie : $\forall x \in x, e \cdot x = x$ et $\forall x \in x, \forall y \in G, y \cdot x = y \cdot x$, $g \cdot (h \cdot x) = (g \cdot h) \cdot x$.

- b) Définition : Deux sous-ensembles H et H' de G sont conjugués $\Leftrightarrow \exists a \in G / H' = \varphi_a(H) = aHa^{-1}$. C'est une RST sur les groupes.

- c) Remarque : Si G est abélien, $w(x) = \{x\}$ et si $H \subset G$, alors $w(H) = \{H\}$.

.. Pour $x \in G$, $w(x) = \{x\} \Leftrightarrow x \in Z$

... Pour $H \subset G$, $w(H) = \{H\} \Leftrightarrow H$ est distingué dans G .

... Pour $H \subset G$, $H \triangleleft G \Leftrightarrow H$ est une réunion de classes de conjugaison.

III) Groupe agissant sur un ensemble

- a) Définition : Soit (G, \cdot) un gpe. Soit X un ens. non vide. Une "opération" (ou "action") de G sur X est une application $G \times X \rightarrow X$ $(g, x) \mapsto g \cdot x$ opération
et qn vérifie : $\forall x \in X, e \cdot x = x$ et $\forall x \in X, \forall g \in G, \forall h \in G, g \cdot (h \cdot x) = (g \cdot h) \cdot x$.

- Propriété : Soit G agissant sur X . Pour tout $g \in G$, l'application partielle $x \mapsto g \cdot x$ est une bijection de X sur lui-même.

2) Exemples : $X = G$, alors G agit sur lui-même. Notamment, G agit sur lui-même par translation à gauche : $g \cdot x = gx$.

ou G agit sur lui-même par conjugaison : $g \cdot x = gxg^{-1}$.

.. G agit par conjugaison sur l'ensemble de ses sous-groupes : $g \cdot H = gHg^{-1}$.

... En algèbre linéaire $G = GL(E)$ agit :
.. sur $E \Leftrightarrow u \cdot v = u(v)$.

.. sur les droites vectorielles $\Leftrightarrow u \cdot D = u(D)$.

.. sur $\mathcal{L}(E) \Leftrightarrow u \cdot v = u \circ v^{-1}$ (similitude)

3) Orbites

- a) Définition : Soit G agissant sur X , et $x \in X$. On appelle "orbite" de x sous l'action de G l'ensemble $\Omega(x) = \{g \cdot x / g \in G\}$.

- b) RST : La relation \sim sur X telle que $x R y \Leftrightarrow \exists g \in G / y = g \cdot x$ est une RST.

Les classes d'équivalence sont les orbites. Elles constituent une partition de X .

- c) Exemples : $X = G$ pour la conjugaison, alors $\Omega(x) = w(x)$.

.. $X = G$ par translation à gauche, alors $\Omega(x) = G$

.. H sous-groupe de G agissant sur G par transl. à gauche : $\Omega(x) = Hx$, classe à droite.

... $GL_n(\mathbb{C})$ agit sur l'ens. des droites vectorielles de E . $\Omega(D) = \{u(D), u \in GL_n(\mathbb{C})\} =$ ens. de toutes les droites.

... $GL_n(K)$ sur $\Omega_n(K)$ par similitude. $\Omega(A) =$ classe de similitude.

4) Groupe d'isotopie, stabilisateur

a) Définition: Soit G agissant sur X , et $x \in X$. On note " G_x " et on appelle "stabilisateur de x " l'ensemble $G_x = \{g \in G / g \cdot x = x\}$.

b) Propriété: G_x est un sous-groupe de G .

c) Exemple: S_n agit sur G par conjugaison, $G_x = \{a \in G / a \cdot x = x\} =$ ens. des éléments qui commutent avec $x = C_x$ le centralisateur de x .
.. Si G agit sur l'ens. de ses sous-ensembles par conjugaison, $G_H = \{x \in G / x H x^{-1} = H\}$ appelé "normalisateur de H ". On note que $H \triangleleft G_H$.

d) Théorème: Il existe une bijection entre l'orbite $\Omega(x)$ pour $x \in X$ et l'ensemble quotient G/G_x .

e) Corollaire: Si $\Omega(x)$ est fini, alors $|\Omega(x)| = [G : G_x]$. Et si G est fini: $|G| = |\Omega(x)| \cdot |G_x|$.

5) Equation aux classes

a) Définition: Soit G agissant sur X , avec X fini. On nomme Θ l'ensemble des orbites, X étant la réunion disjointe on a: $|X| = \sum_{\Omega \in \Theta} |\Omega|$.

Si on choisit un élément dans chaque orbite et qu'on nomme \mathcal{B} l'ensemble obtenu, alors: $|X| = \sum_{x \in \mathcal{B}} [G : G_x]$
Ces deux égalités sont "l'équation aux classes".

Et si G est aussi fini, alors $|X| = \sum_{x \in \mathcal{B}} \frac{|G|}{|G_x|}$.

b) Cas de la conjugaison: Soit $X = G$ fini. Nous avons donc l'équation $|G| = \sum_{x \in \mathcal{B}} \frac{|G|}{|G_x|}$. Or, pour la conjugaison $\Omega(x) = \mathcal{C}(x)$.

Donc, pour $x \in Z$, $\mathcal{C}(x) = \{x\}$. Notons $\mathcal{B}' = \mathcal{B} \setminus Z$. L'équation devient: $|G| = |Z| + \sum_{x \in \mathcal{B}'} \frac{|G|}{|G_x|}$.

c) Théorème de Burnside: Si G de cardinal p^n , avec $n \geq 1$ et p premier, alors $Z \neq \{e\}$.

IV) Groupe S_n

a) Rappel: S_n est le gr. des permutations de l'ensemble $E_n = \{1, 2, \dots, n\}$. La loi est la composition. Card $S_n = n!$

On définit la signature de σ : $\varepsilon(\sigma) = (-1)^N$ avec $N =$ nbre d'inversions $= \sum_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

ε est une morphisme de gr. de S_n dans $\{1, -1\}$. Le noyau de ε est le gr. alterné A_n , de cardinal $\frac{1}{2} n!$

$A_n \triangleleft S_n$ et $S_n/A_n \cong \{1, -1\}$. Les transpositions engendrent S_n .

b) Orbites

a) Définition: Soit $\tau \in S_n$, et q l'ordre de τ . Le sous-groupe cyclique $\langle \tau \rangle = \{e, \tau, \tau^2, \dots, \tau^{q-1}\}$ agit sur E_n : $\forall \tau \in \langle \tau \rangle, \forall x \in E_n, \tau x = \tau(x)$.

Pour cette action, les orbites de E_n s'appellent "les orbites de la permutation τ ".

Si $x \in E_n$, l'orbite de x est: $\Omega(x) = \{x, \tau(x), \dots, \tau^{q-1}(x)\}$ mais il peut y avoir des répétitions, donc: Card $\Omega(x) \leq q$

Plus précisément, Card $\Omega(x) \mid q$.

b) Action sur une orbite: Considérons $\Omega(x)$ sous l'action de $\langle \tau \rangle$. $\Omega(x)$ stable sous $\langle \tau \rangle$.

• Propriété: Soit λ le plus petit entier tel que $\tau^\lambda(x) = x$. Alors $\Omega(x) = \{x, \tau(x), \dots, \tau^{\lambda-1}(x)\}$.

c) Cycles

a) Définition: $\tau \in S_n$ est un cycle $\Leftrightarrow \tau$ possède une unique orbite de cardinal $> 1 \Leftrightarrow \tau$ a une 1^{ère} orbite non singleton.

• Définition: Si τ est un cycle, le cardinal de son orbite non singleton s'appelle la longueur de τ .

Une transposition est un cycle de longueur 2. L'orbite non singleton s'appelle le support du cycle.

b) Ordre d'un cycle: L'ordre d'un cycle τ est égal à sa longueur.

c) Conjugué d'un cycle: Si $\tau = (a_1, \dots, a_{k-1}, a_k)$ est un cycle, et $\sigma \in S_n$, alors: $\tau \sigma \tau^{-1} = (\sigma(a_1), \dots, \sigma(a_{k-1}), \sigma(a_k))$. On en déduit que les "k-cycles" forment une classe de conjugaison de S_n . Conséquence: S_n est engendré par les transpositions $(1, i)$ avec $i = 2, \dots, n$.

d) Signature d'un cycle: La signature d'un k-cycle est $(-1)^{k-1}$.

e) Décomposition en produit de cycles de supports disjoints

a) Propriété: Le produit de deux cycles de supports disjoints est commutatif.

b) Théorème: Toute permutation, $\neq e$, se décompose en produit de cycles de supports disjoints. La décomposition est unique, à l'ordre près.

f) Application

a) Calcul de l'ordre de τ : L'ordre de $\tau \in S_n$ est le ppcm des ordres " λ_i " des cycles de sa décomposition.

b) Calcul de conjugué: (..)

c) Calcul de signature: $\tau \in S_n, \tau = \tau_1 \dots \tau_r$. Alors $\varepsilon(\tau) = \varepsilon(\tau_1) \dots \varepsilon(\tau_r) = \prod_{i=1}^r (-1)^{\lambda_i - 1} = (-1)^{\sum_{i=1}^r (\lambda_i - 1)} = (-1)^{n-k}$, avec $k =$ nbre total d'orbites.

g) Générateurs de A_n

• Propriété: Les 3-cycles engendrent A_n ($n \geq 3$).