

Groupes et action des groupes.

1 Groupes.

Définition. Groupes.

Soit G un ensemble non vide muni d'une loi de composition interne notée \cdot (en abrégé l.c.i), on dit que (G, \cdot) est un groupe ssi :

- 1) La loi \cdot est associative.
- 2) La loi \cdot admet un neutre noté e_G .
- 3) Tout élément de G est symétrisable.

Si de plus la loi \cdot est commutative on dit que (G, \cdot) est un groupe commutatif ou abélien.

Exemples :

- 1) $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, (\mathbb{C}^*, \times) sont des groupes abéliens.
- 2) $(GL_2(\mathbb{R}), \times)$ est un groupe non abélien.

Définition. Sous-groupes.

Soit (G, \cdot) un groupe et H une partie de G , on dit que H est un sous-groupe de G ssi :

- 1) $H \neq \emptyset$ ($e_G \in H$).
- 2) $\forall x, y \in H, x \cdot y^{-1} \in H$.

Remarque.

Si H est un sous-groupe de (G, \cdot) , alors (H, \cdot) est un groupe.

Définition. Produit de deux groupes.

Soient (G_1, \top) , (G_2, \perp) deux groupes, on définit sur $G_1 \times G_2$ la loi \cdot définie par :
 $\forall (x, y), (x', y') \in G_1 \times G_2 : (x, y) \cdot (x', y') = (x \top x', y \perp y')$.

Proposition.

$(G_1 \times G_2, \cdot)$ est un groupe dit groupe produit des groupes (G_1, \top) et (G_2, \perp) .

Remarque.

Si de plus (G_1, \top) et (G_2, \perp) sont abéliens, alors $(G_1 \times G_2, \cdot)$ est un groupe abélien.

Théorème et définition. Sous-groupe engendré par une partie.

Soit (G, \cdot) un groupe et A une partie de G non vide ; L'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G noté $\langle A \rangle$ ou $gr(A)$ et appelé sous-groupe engendré par A . C'est le plus petit sous-groupe de G (au sens de l'inclusion) contenant A .

Proposition.

Soit A une partie non vide d'un groupe (G, \cdot) , alors on a :

$$\langle A \rangle = \{x \in G / \exists n \in \mathbb{N}^*, x_1, \dots, x_n \in A \cup A^{-1}, x = \prod_{k=1}^n x_k\} \text{ où } A^{-1} = \{x^{-1} / x \in A\}.$$

2 Action d'un groupe.

Définition. Action d'un groupe.

Soit (G, \cdot) un groupe et E un ensemble. On appelle action ou opération de G sur E toute application $(g, x) \in G \times E \mapsto g \cdot x \in E$ vérifiant :

- 1) $\forall x \in E : e_G \cdot x = x$.
- 2) $\forall x \in E, \forall g, g' \in G : g \cdot (g' \cdot x) = (g \cdot g') \cdot x$.

Théorème.

Si (G, \cdot) est un groupe opérant sur un l'ensemble E , alors l'application de (G, \cdot) dans $(S(E), \circ)$ qui à tout $g \in G$ associe $\phi(g)$ définie par $: x \in E \mapsto \phi(g)(x) = g.x$ est bien définie et est un morphisme de groupes.

Remarque.

La réciproque du théorème précédent est vraie, ainsi une opération d'un groupe G sur un ensemble E revient à la donnée d'un morphisme de groupes de (G, \cdot) vers $(S(E), \circ)$.

Définition. Action transitive.

Une action d'un groupe G sur un ensemble E est dite transitive ssi : $\forall x, y \in E, \exists g \in G : y = g.x$.

Proposition.

Soit G un groupe opérant sur un ensemble E , on définit la relatio binaire suivante :

$$\forall x, y \in E \quad x \mathfrak{R} y \iff \exists g \in G, y = g.x.$$

\mathfrak{R} est une relation d'équivalence sur E , les classes d'équivalence modulo \mathfrak{R} sont appelés orbites.

Remarque.

La relation \mathfrak{R} est transitive \Leftrightarrow Il y a une seule orbite.

Définition. Stabilisateur.

Soit G un groupe opérant sur un ensemble E et $x \in E$, on appelle stabilisateur de x la partie de G notée S_x et définie par : $S_x = \{g \in G / g.x = x\}$

Proposition.

Pour tout $x \in E, S_x$ est un sous-groupe de G .

3 Groupes $\mathbb{Z}/n\mathbb{Z}$.

Proposition.

Les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n.\mathbb{Z}$ avec $n \in \mathbb{N}$.

Théorème et définition.

Soit $n \in \mathbb{N}$ on définit dans \mathbb{Z} la relation binaire suivante : $\forall x, y \in \mathbb{Z} : x \mathfrak{R} y \Leftrightarrow n|x - y$ et on écrit dans ce cas $x \equiv y \pmod{n}$.

Cette relation est une relation d'équivalence, il y a exactement n classes d'équivalence à savoir : $\bar{0}, \bar{1}, \dots, \bar{n-1}$, l'ensemble de ces classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$.

Dans $\mathbb{Z}/n\mathbb{Z}$ on définit une loi de composition interne définie par : $\forall x, y \in \mathbb{Z}, \bar{x} + \bar{y} = \overline{x + y}$, cette loi est bien définie, compatible avec la relation congruence modulo n et on a le résultat suivant :

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

Définition. Groupes monogènes, cycliques.

Soit (G, \cdot) un groupe et $a \in G$, le sous-groupe engendré par $\{a\}$ (on dit aussi par a) noté $\langle a \rangle$ est égal à : $\langle a \rangle = \{a^k / k \in \mathbb{Z}\}$.

Quand un groupe est engendré par l'un de ses éléments, il est dit monogène, si de plus il est fini, on dit qu'il est cyclique.

Théorème.

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique, engendré par tous les \bar{k} tel que : $1 \leq k \leq n - 1$ et $k \wedge n = 1$.

Remarque.

Soit $U_n = \{z \in \mathbb{C} / z^n = 1\} = \{\exp(\frac{2ik\pi}{n}) / 0 \leq k \leq n - 1\}$, alors U_n est un sous-groupe cyclique de (\mathbb{C}^*, \cdot) engendré par les $\exp(\frac{2ik\pi}{n})$ tel que : $1 \leq k \leq n - 1$ et $k \wedge n = 1$.

Théorème.

Soit (G, \cdot) un groupe et $a \in G$ et $\phi : (\mathbb{Z}, +) \longrightarrow (G, \cdot), k \in \mathbb{Z} \longmapsto \phi(k) = a^k$, alors on a :

- 1) ϕ est un morphisme de groupes.
- 2) $\ker(\phi) = \{0\} \Rightarrow \langle a \rangle$ est isomorphe à \mathbb{Z} .
- 3) $\ker(\phi) = n.\mathbb{Z} \Rightarrow \langle a \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.