Chapitre II : Structures Algébriques

I- Groupes

1- Lois de composition interne

Définition:

Soit E un ensemble, On appelle loi de composition interne une application de E×E dans E.

$$\varphi:\begin{cases} E \times E \longrightarrow E \\ (a,b) \longrightarrow a * b \end{cases}$$

Exemple :

- **Sur N** la multiplication ou l'addition des entiers forme une loi de composition interne.
- Si E est un ensemble, la composition des applications est une loi de composition interne sur l'ensemble des fonctions de E dans E : $\mathcal{F}(E,E)$
- Si E est un ensemble, l'intersection ou la réunion sont des lois de composition interne sur l'ensemble des parties de E : $\mathcal{P}(E)$

Définition:

Soit $*$ une loi de composition interne sur un ensemble E. On dit que $*$ est :

- commutative si et seulement si $\forall(a,b) \in E^2; a * b = b * a$
- associative si et seulement si $\forall(a,b,c) \in E^3; a * (b * c) = (a * b) * c$
- admet un élément neutre si et seulement si $\forall x \in E; e * x = x * e = x$

Proposition (Unicité de l'élément neutre)

Si (E, $*$) possède un élément neutre, il est unique.

Exemple

– (N, +), + est commutative et associative. 0 est l'unique élément neutre.
– (N, ×),× est commutative et associative. 1 est l'unique élément neutre.
– Soit E un ensemble. On considère l'ensemble des applications de E dans E muni de la composition : $(\mathcal{F}(E,E),\ \circ)$. La loi de composition interne ∘ est associative mais pas commutative. Id_E est l'élément neutre de cette loi.

Définition : symétrique

On suppose que (E, $*$) possède un élément neutre e. Soit un élément x ∈ E. On dit qu'un élément y ∈ E est un symétrique (ou un inverse) de l'élément x si et seulement si : x $*$ y = y $*$ x = e
Si tel est le cas, y est unique et est appelé symétrique de x.

Remarque : L'élément neutre est toujours son propre symétrique :$e^{-1} = e$.

Notation : Si un élément x de (E, $*$) admet un symétrique :

- On l'appelle inverse de x et on le note x^{-1} lorsque la loi est notée multiplicativement
- On l'appelle opposé de x et on le note - x lorsque la loi est notée additivement.

Exemple

– Le seul élément de (N, +) qui admet un opposé est 0.
– Tout élément n ∈ Z muni de l'addition admet un opposé.
– Les deux seuls éléments de Z. muni de la multiplication qui admettent un inverse sont 1 et −1.
– Tout élément p/q de Q. admet un inverse donné par q/p.
– Si f ∈ F(E,E) muni de la loi de composition, f est inversible si et seulement si elle est bijective.

Proposition : Règles de calcul avec les inverses

– Si x est symétrisable alors x^{-1} est aussi symétrisable et : $(x^{-1})^{-1} = x$

– Si x et y sont symétrisables, x ∗ y est aussi symétrisable et : $(x * y)^{-1} = y^{-1} * x^{-1}$
.

Définition :
Soit ∗ une loi de composition interne dans un ensemble E. On dit qu'un élément r ∈ E est régulier à droite (respectivement à gauche) de ∗ si :
∀b, c ∈ E, b ∗ r = c ∗ r ⇒ b = c, (respectivement ∀b, c ∈ E, r ∗ b = r ∗ c ⇒ b = c)
Si r est un élément régulier à droite et à gauche de ∗, on dit que r est un élément régulier de ∗ dans E.

2- Groupe

Définition:
On appelle groupe, tout ensemble non vide G muni d'une loi de composition interne ∗ tel que :
1. ∗ est associative ;
2. ∗ possède un élément neutre e ;
3. Tout élément de E est symetrisable.

Si de plus ∗ est commutative, on dit que (G, ∗) est un groupe commutatif, ou groupe Abélien

Exemple :
- Un exemple illustratif de groupe abélien est (Z, +).
- Soit E un ensemble. On note S(E) l'ensemble des bijections de E dans E. Alors (S(E), ∘}) est un groupe (en général non abélien).

Théorème : Règles de calcul dans un groupe
Soit (G, ∗) un groupe.
1) L'élément neutre est unique ;
2) Tout élément possède un unique symétrique ;
3) Pour tout élément x d'un groupe, on a $(x^{-1})^{-1} = x$
4) On peut simplifier : ∀(x, y) ∈ G² ; $\begin{cases} a * x = a * y \Longrightarrow x = y \\ x * a = y * a \Longrightarrow x = y \end{cases}$
5) Soit (a, b) ∈ G². L'équation a∗x = b possède une unique solution : x = (a^{-1}) ∗b
6) ∀(x, y) ∈ G² ; $(x * y)^{-1} = y^{-1} * x^{-1}$

Définition
Soit G un groupe dont la loi est noté multiplicativement. On dit qu'un élément x de G est d'ordre fini s'il existe un entier naturel non nul k tel que $x^k = e$. Si tel est le cas on appelle ordre de x le plus petit entier k ∈ N^* tel que $x^k = e$.

Proposition
Avec les mêmes hypothèses que précédemment, on définit, pour tout x de G, l'ensemble $E(x) = \{k \in Z \; tel \; que \; x^k = e\}$. Alors E(x) est un sous-groupe de Z, qui est différent de {0} si et seulement si x est d'ordre fini, auquel cas l'ordre de x est le générateur positif de E(x).

Corollaire
Soit x un élément d'ordre n de G. Alors on a, pour tout m ∈ Z, l'équivalence
$x^m = e$ ⇔ n divise m.

Proposition : Groupe produit
On considère deux groupes (G, ■) et (H, •) et sur l'ensemble G×H, on définit la loi ∗ par :
∀((x, y), (x', y'))∈ (G×H)², (x, y) ∗ (x', y') = (x ■ x', y • y')
Alors (G×H, ∗) est un groupe appelé groupe produit.

Définition: Sous-groupe
Soit (G, ∗) un groupe. On dit qu'une partie H⊂G est un sous-groupe de G si et seulement si :

1. e $\in$ H;
2. la partie H est stable par la loi : $\forall (x, y) \in H^2$, $x * y \in H$.
3. $\forall x \in H$; $x^{-1} \in H$

Proposition : Caractérisation des sous groupe
Soient (G, $*$) un groupe et H une partie non vide de G. H est un sous groupe de G si et seulement si

1. e $\in$ H;
2. $\forall (x, y) \in H^2$; $x * y^{-1} \in H$

Exemple :
- Z est un sous-groupe de R pour l'addition.
- n.Z est un sous-groupe de Z.
- L'ensemble des bijections croissantes est un sous-groupe du groupe des bijections de R dans R.
- L'ensemble des isométries du plan est un sous-groupe du groupe des bijections du plan. (Rappelons qu'une isométrie est une bijection conservant les distances).

Théorème : Un sous-groupe a une structure de groupe
Si la partie H est un sous-groupe de (G, $*$), alors puisque cette partie est stable pour la loi de composition interne, on peut définir la restriction de la loi $*$ à H qui est une loi de composition interne sur H. Muni de cette loi restreinte, (H, $*$) est un groupe.

Exemple :
Montrons que (U, ×) est un groupe avec : U = {z $\in$ C / |z| = 1}. Il suffit de prouver que c'est un sous-groupe de (C., ×).
- ✓ Comme |1| = 1, il est clair que 1 $\in$U.
- ✓ Soient x, y $\in$U, On a $|xy^{-1}| = |x||y^{-1}| = 1$ donc $x\, y^{-1} \in$U.
- ✓ Donc U est un sous-groupe de (C., ×) et (U, ×) admet par conséquent une structure de groupe.

Théorème : L'intersection de sous-groupes est un sous-groupe
Si H_1 et H_2 sont deux sous-groupes d'un groupe G, alors $H_1 \cap H_2$ est un sous-groupe de G, ou plus généralement l'intersection d'une famille de sous-groupes, d'un groupe G est un sous-groupe de G.

Remarque :
La réunion de deux sous-groupes n'est en revanche pas un sous-groupe en général.

Définition : Sous-groupe engendré par une partie
Soit S une partie d'un groupe G. On appelle sous-groupe engendré par S, et on note $\langle S \rangle$ le plus petit sous-groupe contenant S. C'est l'intersection de tous les sous-groupes de G qui contiennent S.

3- Morphisme de groupe

Définition : Morphisme
Soients deux groupes $(G_1,\ *)\ et\ (G_2,\ \cdot)$. Une application $f: G_1 \rightarrow G_2$ est un morphisme de groupes si et seulement si : $\forall (x, y) \in {G_1}^2; f(x * y) = f(x) \cdot f(y)$
On dit de plus que f est un :
- endomorphisme lorsque $G_1 = G_2$

- isomorphisme lorsque f est bijective
- automorphisme lorsque f est un endomorphisme et un isomorphisme

PROPOSITION : Propriétés des morphismes de groupes
Si e_1 est l'élément neutre de G_1 et e_2 l'élément neutre de G_2, alors

1. $f(e_1) = e_2$;
2. $\forall x \in G_1$; $(f(x))^{-1} = f(x^{-1})$

Théorème : Image directe et réciproque de sous-groupes par un morphisme
Soient deux groupes $(G_1, *)$ et $(G_2, \cdot)$. Et soit $f: G_1 \to G_2$ un morphisme de groupes

1) Si H_1est un sous-groupe de G_1, alors $f(H_1)$ est un sous-groupe de G_2 ;
2) Si H_2est un sous-groupe de G_2, alors $f^{-1}(H_2)$ est un sous-groupe de G_1

Définition : Noyau, image d'un morphisme de groupes
On considère un morphisme de groupes $f: G_1 \to G_2$. On note e_1 l'élément neutre du groupe G_1 et e_2 l'élément neutre du groupe G_2 On définit

- le noyau du morphisme f : $Ker\ f = \{x \in G_1\ tel\ que\ f(x) = e_2\} = f^{-1}(e_2)$
- l'image du morphisme f : $Im\ f = f(G_1) = \{x \in G_2\ tel\ que\ \exists\ x \in G_1\ f(x) = y\}$

Ker f est un sous-groupe de G_1 et Imf est un sous-groupe de G_2.

Théorème : Caractérisation des morphismes injectifs
Un morphisme $f: G_1 \to G_2$ est injectif si et seulement si $Ker\ f = \{e_1\}$

4- Groupe symétrique

Définition: Groupe symétrique d'un ensemble
Soit E un ensemble. Une permutation de E est une bijection de E dans E. On note S_E l'ensemble des permutations de E. Si $E = \{1, 2, \ldots\ldots, n\}$ on le note simplement S_n.
L'ensemble S_E muni de la loi de composition des applications est un groupe de neutre $e = I_d$ appelé groupe symétrique sur l'ensemble E.
Une permutation se note $\sigma = \begin{pmatrix} 1 & 2 & . & . & n \\ \sigma(1) & \sigma(2) & . & . & \sigma(n) \end{pmatrix}$, on écrit souvent $\sigma\sigma'$ $pour$ $\sigma o \sigma'$

Exemple :
Soit $E = \{1, 2, 3, 4, 5\}$ et $\sigma, \tau \in S_n$ telles que $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$

le calcul de $\sigma\tau$ donne $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$

Définition: Support
Soit $\sigma \in S_n$, l'ensemble $Supp(\sigma) = \{i,\ \sigma(i) \neq i\}$ est appelé le support de σ

Définition: Cycle
Une permutation σ de S_E est un cycle de longueur $l \geq 2$, s'il existe l éléments distincts $a_1, a_2 \ldots. a_l$ de E tel que $\sigma(a_1) = a_2 \ldots. \sigma(a_l) = a_1\ et\ a_1(x) \neq x\ \forall\ x \in E \setminus \{a_1, a_2 \ldots. a_l\}$
On utilise alors la notation cyclique $\sigma = (a_1, a_2 \ldots. a_l)$
Un cycle de longueur 2 est appelé une transposition.

Théorème :
Soit $\sigma \in S_n$ tel que $\sigma \neq I_d$ il existe $k \geq 1$ et $c_1, c_2 \ldots. c_k$ des cycles à support deux à deux disjoints, tels que $\sigma = c_1. c_2 \ldots. c_k$. Cette décomposition est unique à l'ordre près des facteurs et est appelée décomposition canonique de σ.

Exemple :

1) Soit $E = \{1, 2, 3, 4, 5\}$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$, On remarque que σ = (1 3 5 4) = (3 5 4 1) = (5 4 1 3) = (4 1 3 5):

2) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 3 & 6 & 4 \end{pmatrix}$, vérifier que $\sigma = (1, 5, 6, 2)(3, 4)$

3) Explicitez la décomposition de la permutation $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 8 & 6 & 7 & 5 & 4 & 1 \end{pmatrix}$

4) Donner l'ordre de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 2 & 5 \end{pmatrix}$

Définition: Conjugaison

Soient σ et σ' deux permutations de S_n. On dit que σ est conjuguée à σ' s'il existe une permutation τ de Sn telle que $\sigma = \tau \; o \; \sigma' \; o \; \tau^{-1}$

: