Structures algébriques, groupes finis, groupes diédraux

M.Dridi

Structures algébriques: Loi de composition interne

Loi de composition interne

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

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

Exemples

- Si $E = \mathbb{N}$, 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 : $\mathscr{F}(E,E)$
- Si E est un ensemble, l'intersection ou la réunion sont des lois de composition interne sur l'ensemble des parties de E : $\mathscr{P}(E)$

Structures algébriques: Loi de composition interne

Une partie F de E est dite **stable** par la l.c.i. $*$, si :

$$\forall (a, b) \in F^2 \quad a * b \in F$$

On appelle **l.c.i. induite** par $*$ dans F la restriction de $*$ à $F \times F$.

Exemples :

- La partie $\mathbb{R}_-$ de $\mathbb{R}$ est stable par $+$.
- La partie $\mathbb{R}_+$ est stable par $\times$.
- La partie $\mathbb{R}_-$ n'est pas stable par $\times$.

3

Structures algébriques: Loi de composition interne

Propriétés d'une l.c.i.

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

- *commutative* si et seulement si $\forall (a,b) \in E^2,\ a \star b = b \star a$,
- *associative* si et seulement si $\forall (a,b,c) \in E^3,\ a \star (b \star c) = (a \star b) \star c$.

On dit que plus que $\star$ admet $e \in E$ comme *élément neutre* si et seulement si $\forall x \in E,\ e \star x = x \star e = x$

Unicité de l'élément neutre

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

Exemples

- Pour le couple $(\mathbb{N}, +)$, $+$ est commutative et associative, l'élément neutre est 0.
- Pour le couple $(\mathbb{N}, \times)$, $\times$ est commutative et associative, 1 est l'unique élément neutre .
- Pour le couple $(\mathscr{P}(G), \cup)$, la loi est commutative, associative, la partie $\varnothing$ est neutre pour cette loi.
- Soit E un ensemble. On considère l'ensemble des applications de E dans E muni de la composition : $(\mathscr{F}(E,E), \circ)$. La loi de composition interne $\circ$ est associative mais pas commutative. Id_E est l'élément neutre de cette loi.

4

Structures algébriques: Loi de composition interne

Symétrique

On suppose que $(E, \star)$ possède un élément neutre e. Soit un élément $x \in E$. On dit qu'un élément $y \in E$ est un *symétrique* (ou un *inverse*) de l'élément x si et seulement si :

$$x \star y = y \star x = e$$

Si tel est le cas, y est unique et est appelé le *symétrique de x*.

Notation Si un élément x de $(E, \star)$ 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 de x et on le note $-x$ lorsque la loi est notée additivement.

Règles de calcul avec les inverses

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

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

5

Structures algébrique : Structure de groupe

Déf : Soit G un ensemble. On dit que $(G, \star)$ est un groupe si $\star$ est une loi de composition interne sur G vérifiant :

- la loi $\star$ est associative ;
- G possède un élément neutre ;
- tout élément x de G admet un symétrique.

Si de plus la loi $\star$ est commutative, on dit que le groupe est abélien (ou commutatif).

Exemples

– Les couples $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes.
– Les couples $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ sont des groupes.

6

Structures algébrique : Structure de groupe

Groupes des bijections d'un ensemble

Soit E un ensemble. On note $\mathfrak{S}(E)$ l'ensemble des bijections de E dans E. Alors $(\mathfrak{S}(E), \circ)$ est un groupe (en général non abélien).

Groupe produit

On considère deux groupes $(G, \star)$ et $(H, \bullet)$ et sur l'ensemble $G \times H$, on définit la loi $\bigstar$ par :

$$\forall ((x,y),(x',y')) \in (G \times H)^2, \quad (x,y) \bigstar (x',y') = (x \star x', y \bullet y')$$

Alors $(G \times H, \bigstar)$ est un groupe appelé *groupe produit*.

Structures algébrique : Sous-groupe

Soit $(G, \star)$ un groupe. On dit qu'une partie $H \subset G$ est un *sous-groupe* de G si et seulement si :

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

Exemples

- $\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$ pour l'addition.
- $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ pour l'addition.
- L'ensemble des bijections croissantes est un sous-groupe du groupe des bijections de $\mathbb{R}$ dans $\mathbb{R}$.
- 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).

Structures algébrique : Sous-groupe

Caractérisation des sous-groupes

Soient $(G, \star)$ 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. $\forall (x, y) \in H^2$, $\boxed{x \star y^{-1} \in H}$.

Un sous-groupe a une structure de groupe

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

Structures algébrique : Sous-groupe

Exemple

Montrons que $(\mathbb{U}, \times)$ est un groupe avec : $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$. Il suffit de prouver que c'est un sous-groupe de $(\mathbb{C}^*, \times)$.

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

Structures algébrique : Morphisme de groupes

Morphisme de groupes

Soient deux groupes $(G_1, \star)$ et $(G_2, \bullet)$.
Une application $f : G_1 \longrightarrow G_2$ est un *morphisme* de groupes ou *homomorphisme* si et seulement si :

$$\forall (x, y) \in G_1^2, \quad f(x \star y) = f(x) \bullet f(y)$$

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.

Exemples :

$$\begin{array}{|cccc} (\mathbb{Z}, +) & \rightarrow & (\mathbb{R}_+^*, \times) \\ n & \mapsto & 2^n \end{array} \qquad \begin{array}{|cccc} (\mathbb{R}_+^*, \times) & \rightarrow & (\mathbb{R}, +) \\ x & \mapsto & \ln x \end{array} \qquad \begin{array}{|cccc} (\mathbb{C}, \times) & \rightarrow & (\mathbb{C}, \times) \\ z & \mapsto & \bar{z} \end{array}$$

Structures algébrique : Morphisme de groupes

Propriétés des morphismes de groupes

Si $(G_1, \star)$ est un groupe d'élément neutre e_1, si $(G_2, \bullet)$ est un groupe d'élément neutre e_2

et si $f : G_1 \longrightarrow G_2$ est un morphisme de groupes, alors

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

Structures algébrique : Morphisme de groupes

Image directe et réciproque de sous-groupes par un morphisme

Soient $(G_1, \star)$ et $(G_2, \bullet)$ deux groupes et soit $f : G_1 \mapsto G_2$ un morphisme de groupes.

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

Noyau, image d'un morphisme de groupes

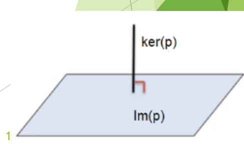
On considère un morphisme de groupes $f : G_1 \mapsto G_2$. On note e_1 l'élément neutre du groupe G_1 et e_2 l'élément neutre du groupe G_2. On définit

– le *noyau* du morphisme f :

$$\mathrm{Ker}\, f = \{x \in G_1 \mid f(x) = e_2\} = f^{-1}(\{e_2\})$$

– l'*image* du morphisme f :

$$\mathrm{Im}\, f = f(G_1) = \{y \in G_2 \mid \exists x \in G_1 \; f(x) = y\}$$



1

Structures algébrique : Morphisme de groupes

Le noyau et l'image d'un morphisme de groupes sont des sous-groupes

On considère un morphisme de groupes $f : G_1 \mapsto G_2$. Alors

– $\mathrm{Ker}\, f$ est un sous-groupe de G_1

– $\mathrm{Im}\, f$ est un sous-groupe de G_2.

Caractérisation des morphismes injectifs

Un morphisme f de $(G_1, \star)$ dans $(G_2, \bullet)$ est injectif si et seulement si $\boxed{\mathrm{Ker}\, f = \{e_1\}}$.

Exemple : L'application $\left| \begin{array}{ccc} (\mathbb{R}, +) & \to & (\mathbb{C}^*, \times) \\ x & \mapsto & e^{ix} \end{array} \right.$ est un morphisme de groupes,

dont le noyau est $\mathrm{Ker}\, f = \{x \in \mathbb{R} \,,\; e^{ix} = 1\} = 2\pi\mathbb{Z}$, sous-groupe de $(\mathbb{R}, +)$.

14

Structures algébrique : Morphisme de groupes

Caractérisation des morphismes surjectifs

Un morphisme f de $(G_1, \star)$ dans $(G_2, \bullet)$ est surjectif si et seulement si $\boxed{\mathrm{Im}\, f = G_2}$.

Exemple : L'image du morphisme $\left| \begin{array}{ccc} (\mathbb{R},+) & \to & (\mathbb{C}^*, \times) \\ x & \mapsto & e^{ix} \end{array} \right.$

est $\mathrm{Im}\, f = \mathcal{U} = \{z \in \mathbb{C}\ ,\ |z| = 1\}$, qui est un sous-groupe de $(\mathbb{C}^*, \times)$.

15

Groupe fini, ordre d'un sous-groupe

DÉFINITIONS. Un groupe G est dit *fini* s'il n'a qu'un nombre fini d'éléments. Dans ce cas, le nombre d'éléments de G est appelé l'*ordre* de G. On le note $o(G)$, ou encore $|G|$. C'est un entier naturel non-nul.

Exemple

L'ensemble $\mathbb{Z}_n \equiv \{e, a, a^2, \ldots, a^{n-1}\}$ muni de la multiplication telle que $a^n = e$ est un groupe fini appelé le groupe cyclique $\mathbb{Z}_n$. Il est abélien.

L'espace $\mathbb{R}$ muni de l'addition, $(\mathbb{R}, +)$ est un groupe infini-dimensionel. De même pour $(\mathbb{Z}, +)$.

Le nombre de bijections de $\{1, \cdots, n\}$ dans $\{1, \cdots, n\}$ étant égal à $n!$, on en déduit que le groupe symétrique $\mathfrak{S}_n$ est un groupe fini d'ordre $n!$.

THÉORÈME DE LAGRANGE. *Soit H un sous-groupe d'un groupe fini G. Alors H est fini, et l'ordre de H divise l'ordre de G.*

16

Groupe fini, ordre d'un sous-groupe

Sous-groupe engendré par une partie d'un groupe

Déf: Si X est une partie de (G, ·), le sous-groupe de G engendré par X est l'intersection de tous les sous-groupes de G qui contiennent X

On note <X> le sous-groupe de G engendré par X et ce sous-groupe <X> est le plus petit (pour l'ordre de l'inclusion) des sous-groupes de G qui contiennent X.

17

Groupe fini, ordre d'un sous-groupe

Soit G un groupe et S une partie de G. Si $G = < S >$, on dira que S est une *partie génératrice* de G (ou que S engendre G).

On dira que G est de *type fini* si une partie finie de G engendre G.

Exemple Le groupe $\mathbb{Z}$ muni de l'addition est engendré par un élément : 1. En effet si $n \in \mathbb{Z}$, alors $n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ fois}}$ si n est positif et $n = \underbrace{-1 - 1 - \cdots - 1}_{-n \text{ fois}}$ si n est négatif. Donc $\mathbb{Z}$ est de type fini.

Remarque Si G est un groupe alors $G = < G >$. En particulier tout groupe fini est de type fini. La réciproque est fausse : $\mathbb{Z}$ est un groupe infini ... de type fini.

18

Groupe fini, ordre d'un sous-groupe

Notation

Si S est une partie d'un groupe G. On notera :

$$S^{-1} := \{x^{-1} \mid x \in S\} \subset G.$$

Proposition

Soit G un groupe et S une partie de G.
1. Si $S = \emptyset$ alors $< S >= \{e_G\}$.
2. Si $S \neq \emptyset$ alors on a :
$< S >= \{x = x_1 x_2 \cdots x_n \mid \forall i \in \{1, \cdots, n\},\ x_i \in S \cup S^{-1},\ n \in \mathbb{N}\}$.

Groupe fini, ordre d'un sous-groupe

Groupe monogène, cyclique

Définition . Soit $(G, .)$ un groupe. $(G, .)$ est dit monogène s'il existe un élément x tel que pour tout élément y de $(G, .)$, il existe un entier relatif k tel que $y = x^k$. On note alors $G = \langle x \rangle$ et l'on dit que $(G, .)$ est engendré par x ou encore que x est un générateur de $(G, .)$. Si de plus, $(G, .)$ est d'ordre fini, on dit que $(G, .)$ est cyclique.

Un groupe est dit *monogène*, s'il est engendré par un seul de ses éléments

Exemples.

$(\mathbb{Z}, +)$ est monogène infini engendré par 1 ou -1.

Pour tout entier naturel non nul n, $\left(\mathbb{U}_n = \left\{e^{\frac{2ik\pi}{n}},\ k \in [\![0; n-1]\!]\right\}, \times\right)$ est un groupe cyclique d'ordre n.

Soit G un groupe fini d'ordre n. Dire que G est cyclique signifie qu'il existe dans G un élément a qui est d'ordre n, de sorte que $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

Groupe fini, ordre d'un sous-groupe

Théorème. *Tout groupe fini d'ordre premier est cyclique.*

Preuve : Soit G tel que $|G| = p > 0$, p premier. Soit $x \neq 1$ dans G, alors $|\mathrm{gr}(x)|$ divise p et, comme, $|\mathrm{gr}(x)| \neq 1$, $|\mathrm{gr}(x)| = p = |G|$, d'où $\mathrm{gr}(x) = G$.
tout élément de G, différent du neutre, engendre G.

Proposition et définition. *Soit G un groupe fini. Pour tout $x \in G$ distinct du neutre e, il existe un entier $n \geq 2$ unique tel que:*

$$x^n = e \quad \text{et} \quad x^k \neq e \text{ pour tout } 1 \leq k < n.$$

Le sous-groupe de G engendré par x est alors:

$$\langle x \rangle = \{e, x, x^2, x^3, \ldots, x^{n-1}\}.$$

L'entier n est l'ordre du sous-groupe $\langle x \rangle$ et est appelé l'ordre de l'élément x de G. On le note $|x|$. C'est un diviseur de l'ordre de G. Dans le cas où $x = e$, on a $\langle e \rangle = \{e\}$, et $|e| = 1$.

Définition. Pour tout entier $n \geq 2$, on appelle groupe diédral d'ordre $2n$, noté D_n, le sous-groupe des isométries affines conservant un polygone régulier à n côtés (avec la convention que pour $n = 2$, D_2 est le groupe des isométries conservant un segment).

On montre en géométrie que D_n est formé des $2n$ éléments distincts:

$$D_n = \{e, r, r^2, r^3, \ldots, r^{n-1}, s, sr, sr^2, sr^3, \ldots, sr^{n-1}\},$$

vérifiant les relations:

$$r^n = e, \quad s^2 = e, \quad sr^k = r^{n-k}s \quad \text{pour tout } 1 \leq k \leq n.$$

Le groupe diédral peut aussi admettre la présentation

$$D_n = \{r, s | r^n = e, \ s^2 = e, \ srs^{-1} = r^{-1}\}.$$

Proposition D_n est d'ordre $2n$ et $D_n = \langle r, s \rangle$ où r est la rotation d'angle $\frac{2\pi}{n}$ et s la symétrie par rapport à l'axe des abscisses.