

CHAPITRE C2

STRUCTURES ALGÉBRIQUES

Objectifs

- Appréhender les notion de structures et de sous-structures.
- Identifier les règles de calculs spécifiques aux groupes/anneaux.
- Construction de morphismes.

1 Loi de composition interne

1.1 Caractéristiques

Définition C2.1

Soit E un ensemble. Une **loi de composition interne** sur E est une application

$$\begin{aligned}\star : \quad E &\longrightarrow E \\ (x, y) &\longmapsto x \star y\end{aligned}$$

Notations.

- On note $x \star y$ plutôt que $\star(x, y)$ par imitation des lci usuelles $+$, \times ou \circ définies sur des ensembles de nombres ou de fonctions.
- On note (E, \star) l'ensemble E muni de la loi \star . Cela forme ce qu'on appelle un **magma**.

Définition C2.2

Avec les mêmes notations, on dit que la loi \star est

- (i) **associative** lorsque $\forall x, y, z \in E, (x \star y) \star z = x \star (y \star z)$,
- (ii) **commutative** lorsque $\forall x, y \in E, x \star y = y \star x$.

Remarque. Le cas échéant, on dit que le magma (E, \star) est associatif (resp. commutatif).

Définition C2.3

Soit E un ensemble muni de deux lois de composition internes \star et \otimes . On dit que \star est **distributive** par rapport à \otimes lorsque

$$\forall x, y, z \in E, \begin{cases} x \star (y \otimes z) = (x \star y) \otimes (x \star z) \\ (y \otimes z) \star x = (y \star x) \otimes (z \star x) \end{cases}.$$

1.2 Élément neutre

Définition C2.4

Soit (E, \star) un magma unifère et soit $e \in E$. On dit que e est un **élément neutre** pour \star lorsque $\forall x \in E, x \star e = e \star x = x$.

Proposition C2.5

Si un magma (E, \star) admet un élément neutre, alors ce dernier est nécessairement unique.

Remarque. On parle alors de magma unifère.

1.3 Symétrique d'un élément

Définition C2.6

Soit E un magma et $x \in E$.

- (i) Un **symétrique à droite** de x pour la loi \star est un élément $x' \in E$ vérifiant : $x \star x' = e$.
- (ii) Un **symétrique à gauche** de x pour la loi \star est un élément $x' \in E$ vérifiant : $x' \star x = e$.
- (iii) Un **symétrique** de x pour la loi \star est un élément $x' \in E$ vérifiant : $x \star x' = x' \star x = e$.

On dit que x est **symétrisable** lorsqu'il admet un symétrique.

Proposition C2.7

Soit (E, \star) un magma associatif unifère. Si un élément $x \in E$ possède un symétrique à droite y et un symétrique à gauche z , alors $y = z$ et x possède un unique symétrique $x' = y = z$.

Proposition C2.8

Soit (E, \star) un magma associatif unifère et notons e son neutre.

- (i) e est le symétrique de e .
- (ii) Si un élément $x \in E$ a pour symétrique x' , alors x' a pour symétrique x .
- (iii) Soit $x, y \in E$ admettant pour symétriques respectifs x' et y' . Alors $x \star y$ admet pour symétrique $y' \star x'$.

1.4 Itérés d'un élément

Dans ce paragraphe, (E, \star) désigne un magma associatif et unifère dont on note e l'élément neutre.

Définition C2.9

Soit $x \in E$.

- (i) On définit par récurrence les **itérés** de x pour $n \in \mathbb{N}$:

$$\begin{cases} x^0 = e \\ \forall n \in \mathbb{N}, x^{n+1} = x^n \star x \end{cases}.$$

- (ii) Si x admet un symétrique x' , on définit les itérés de x pour n entier négatif par :

$$x^n = (x')^{-n}.$$

Proposition C2.10

Soit $x, y \in E$. Soit $n, m \in \mathbb{N}$.

- (i) $x^n \star x^m = x^{n+m}$,
- (ii) $(x^n)^m = x^{nm}$,
- (iii) si x et y commutent, alors x^n et y^m commutent et $(x^n \star y^m) = (x \star y)^{n+m}$.

Si x et/ou y admettent un symétrique, alors ces identités sont valables pour n et/ou m dans \mathbb{Z} .

Notations. Deux notations courantes : la notation multiplicative et la notation additive.



2 Groupes

2.1 Définitions et exemples

Définition C2.11

On dit qu'un ensemble G muni d'une loi de composition interne \star est un **groupe** lorsque

A \star est associative,

N G contient un élément neutre pour la loi \star ,

S tout élément de G est symétrisable.

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

Notation. Dans la suite, on adoptera la notation multiplicative. Notamment le symétrique de $x \in E$ sera noté x^{-1} et appelé inverse de x . On note en toute généralité e_G le neutre de G .

Théorème et définition C2.12

Soit E un ensemble non vide.

- On appelle **permutation** de E toute application bijective $\sigma : E \rightarrow E$ et on note S_E l'ensemble des permutations de E .
- (S_E, \circ) est un groupe appelé **groupe symétrique** ou **groupe des permutations** de E .

Remarque. (S_E, \circ) n'est presque jamais un groupe abélien. Plus précisément, il l'est si et seulement si E contient au plus 2 éléments.

Notation. Dans le cas où $E = \llbracket 1, n \rrbracket$, on note $S_n = S_{\llbracket 1, n \rrbracket}$.

Proposition C2.13

Soit $n \in \mathbb{N}$. S_n est un groupe fini contenant $n!$ éléments.

Proposition et définition C2.14

Soit (G_1, \star_1) et (G_2, \star_2) deux groupes. On munit l'ensemble $G_1 \times G_2$ de la loi \otimes définie par :

$$\forall (x_1, x_2), (y_1, y_2) \in G_1 \times G_2, (x_1, x_2) \otimes (y_1, y_2) = (x_1 \star_1 y_1, x_2 \star_2 y_2).$$

- $(G_1 \times G_2, \otimes)$ est un groupe, appelé **groupe produit** de G_1 et G_2 .
- $(G_1 \times G_2, \otimes)$ est un groupe abélien si et seulement si G_1 et G_2 sont abéliens.

Remarque. On peut étendre cette construction au produit cartésien de n groupes, dont le neutre sera le n -uplet des neutres des n groupes.

2.2 Sous-groupes

Définition C2.15

Soit (G, \star) un groupe et $H \subset G$. On dit que H est un sous-groupe de G lorsque

- $e_G \in H$,
- H est stable par \star , i.e. $\forall x, y \in H, x \star y \in H$,
- H est stable par passage au symétrique, i.e. $\forall x \in H, x^{-1} \in H$.

Proposition et définition C2.16

Soit (G, \star) un groupe et H un sous-groupe de G .

- L'application $H \times H \rightarrow H$ définit une loi de composition interne sur H appelée **loi induite** par \star sur H , et souvent encore notée \star .
- (H, \star) est un groupe.

Proposition C2.17

Toute intersection d'une famille de sous-groupes de (G, \star) est un sous-groupe de G

2.3 Morphismes de groupes

Définition C2.18

Soit (G_1, \star_1) et (G_2, \star_2) deux groupes. On appelle

- **morphisme de groupes** de G_1 dans G_2 toute application $\varphi : G_1 \rightarrow G_2$ vérifiant

$$\forall x, y \in G_1, \varphi(x \star_1 y) = \varphi(x) \star_2 \varphi(y),$$

- **isomorphisme** de groupes tout morphisme de groupes bijectif,
- **endomorphisme** de G_1 tout morphisme de G_1 dans lui-même,
- **automorphisme** de G_1 tout endomorphisme bijectif de G_1 dans lui-même.

On dit que G_1 et G_2 sont **isomorphes** lorsqu'il existe un isomorphisme de G_1 dans G_2 .


Proposition C2.19

Soit (G_1, \star_1) et (G_2, \star_2) deux groupes (dont on note e_1 et e_2 les neutres respectifs) et $\varphi : G_1 \rightarrow G_2$ un morphisme de groupes.

- (i) $\varphi(e_1) = e_2$.
- (ii) $\forall g \in G_1, \varphi(g^{-1}) = \varphi(g)^{-1}$.
- (iii) $\forall g \in G_1, \forall n \in \mathbb{Z}, \varphi(g^n) = \varphi(g)^n$.

Proposition C2.20

- (i) La composée de deux morphismes de groupes est un morphisme de groupes.
- (ii) La réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.

Théorème C2.21

Soit (G, \star) un groupe. L'ensemble des automorphismes de G , muni de la loi \circ , est un groupe, noté $(\text{Aut}(G), \circ)$.

2.4 Noyau, image d'un morphisme

Définition C2.22

Soit (G_1, \star_1) et (G_2, \star_2) deux groupes (dont on note e_1 et e_2 les neutres respectifs) et $\varphi : G_1 \rightarrow G_2$. On appelle

- (i) **image** de φ l'ensemble $\text{Im } \varphi = \varphi(G_1) = \{\varphi(g) \mid g \in G_1\}$.
- (ii) **noyau** de φ l'ensemble $\text{Ker } \varphi = \varphi^{-1}(\{e_2\}) = \{g \in G_1 \mid \varphi(g) = e_2\}$.

Proposition C2.23

Avec les notations précédentes,

- (i) $\text{Im } \varphi$ est un sous-groupe de G_2 .
- (ii) $\text{Ker } \varphi$ est un sous-groupe de G_1 .

Théorème C2.24

Avec les notations précédentes,

- (i) φ est surjective si et seulement si $\text{Im } \varphi = G_2$.
- (ii) φ est injective si et seulement si $\text{Ker } \varphi = \{e_1\}$.

3 Anneaux et corps

3.1 Structure d'anneau

Définition C2.25

On dit qu'un ensemble A muni de deux lois de composition interne $+$ et \times est un **anneau** lorsque **G** $(A, +)$ est un groupe abélien,

- A** la loi \times est associative,
 - N** la loi \times admet un élément neutre,
 - D** la loi \times est distributive par rapport à la loi $+$.
- $\left. \begin{array}{l} \text{la loi } \times \text{ est associative,} \\ \text{la loi } \times \text{ admet un élément neutre,} \end{array} \right\} (A, +, \times) \text{ est un magma associatif unifère}$

Lorsque de plus la loi \times est commutative, on dit que l'anneau $(A, +, \times)$ est **commutatif**.

Notations. Les éléments neutres seront notés respectivement 0_A et 1_A ou 0 et 1 s'il n'y a pas d'ambiguïté possible. On notera $-a$ le symétrique pour la loi $+$ d'un élément $a \in A$.

Proposition C2.26

Soit $(A, +, \times)$ un anneau, $a, b \in A$ et $n \in \mathbb{Z}$.

- (i) $a \times 0_A = 0_A \times a = 0_A$,
- (ii) $(-a) \times b = -(a \times b) = a \times (-b)$,
- (iii) $(n \cdot a) \times b = n \cdot (a \times b) = a \times (n \cdot b)$.

Théorème C2.27

Soit $(A, +, \times)$ un anneau, $n \in \mathbb{N}$ et $a, b \in A$ tels que $a \times b = b \times a$.

- (i) Formule du binôme de Newton :

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k \times b^{n-k}.$$

- (ii) Formule de Bernoulli :

$$a^n - b^n = (a - b) \times \left(\sum_{k=0}^{n-1} a^{n-1-k} \times b^k \right) = \left(\sum_{k=0}^{n-1} a^{n-1-k} \times b^k \right) \times (a - b).$$



3.2 Sous-anneaux

Définition C2.28

Soit $(A, +, \times)$ un anneau et $B \subset A$. On dit que B est un **sous-anneau** de A lorsque

- $(B, +)$ est un sous-groupe de A ,
- $1_A \in B$,
- B est stable par produit, *i.e.* $\forall x, y \in B, x \times y \in B$.

Remarque. Vérifier que $0_A \in B$ est superflu, c'est une conséquence de $1_A \in B$ et de la stabilité par différence.

Proposition C2.29

Soit $(A, +, \times)$ un anneau et B un sous-anneau de A . Muni des lois induites par $+$ et \times , B est alors un anneau.

3.3 Morphismes d'anneaux

Définition C2.30

Soit $(A, +, \times)$ et (A', \oplus, \otimes) deux anneaux. On appelle **morphisme d'anneaux** de A dans A' toute application $f : A \rightarrow A'$ vérifiant

- $\forall a, b \in A, f(a + b) = f(a) \oplus f(b)$,
- $\forall a, b \in A, f(a \times b) = f(a) \otimes f(b)$,
- $f(1_A) = 1_{A'}$.

Lorsque f est de plus bijective, on dit que f est un **isomorphisme** d'anneaux.

3.4 Anneau intègre

Définition C2.31

Soit $(A, +, \times)$ un anneau. On dit qu'un élément $a \in A$ est **inversible** lorsqu'il est symétrisable pour la loi \times , *i.e.* lorsque

$$\exists a' \in A, a \times a' = a' \times a = 1_A.$$

Proposition et définition C2.32

Soit $(A, +, \times)$ un anneau. On note $U(A)$ ou A^\times l'ensemble des inversibles de A . Alors $(U(A), \times)$ est un groupe, appelé **groupe des inversibles** de A .

Définition C2.33

Soit $(A, +, \times)$ un anneau commutatif.

(i) Un **diviseur de zéro** est un élément $a \in A$ non nul tel que

$$\exists b \in A \setminus \{0_A\}, a \times b = 0_A.$$

(ii) A est dit **intègre** lorsqu'il est non nul et sans diviseur de zéro, *i.e.*

$$\forall a, b \in A, (a \times b = 0_A \Rightarrow a = 0_A \text{ ou } b = 0_A).$$

Proposition C2.34

Soit $(A, +, \times)$ un anneau intègre. Soit $a, x, y \in A$ tels que $a \neq 0_A$. Alors

$$a \times x = a \times y \Rightarrow x = y.$$

Définition C2.35

Soit $(A, +, \times)$ un anneau. On dit qu'un élément $a \in A$ est **nilpotent** lorsqu'il existe $n \in \mathbb{N}$ tel que $a^n = 0_A$. Dans ce cas, le plus petit $n \in \mathbb{N}$ vérifiant $a^n = 0_A$ est appelé **indice** ou **ordre de nilpotence** de a .

Théorème C2.36

Soit $(A, +, \times)$ un anneau et $a \in A$. Si a est nilpotent, alors $1_A - a$ est inversible et

$$(1_A - a)^{-1} = \sum_{k=0}^{n-1} a^k.$$

3.5 Structure de corps**Définition C2.37**

On dit qu'un ensemble K muni de deux lois de composition internes $+$ et \times est un **corps** lorsque

A $(K, +, \times)$ est un anneau commutatif non réduit à $\{0_K\}$,

I tout élément non nul de K est inversible.


Définition C2.38

Soit $(K, +, \times)$ un corps et $L \subset K$. On dit que L est un **sous-corps** de K lorsque

- $(L, +, \times)$ est un sous-anneau de K ,
- L est stable par passage à l'inverse, *i.e.* $\forall x \in L \setminus \{0_K\}, x^{-1} \in L$.

Proposition C2.39

Soit $(K, +, \times)$ un corps et L un sous-corps de K . Muni des lois induites par $+$ et \times , L est alors un corps.

Méthodes

- Montrer qu'un ensemble est un sous-groupe, sous-anneau ou sous-corps d'une structure connue.
- Montrer qu'une application est un morphisme.
- Calculer le noyau d'un morphisme de groupes.