Structures

I. Loi de composition interne

Définition. *Soit E un ensemble, on appelle loi de composition interne sur E une application $\star$ de $E \times E$ dans E. L'image du couple (x, y) est notée $x \star y$ au lieu de $\star(x, y)$.*

Exemple.
- *L'union et l'intersection sont des lois de composition internes sur l'ensemble $\mathcal{P}(E)$.*
- *Les opérations usuelles $+$, $-$ et $\times$ sont des lois de composition interne sur $\mathbb{R}$.*
- *La composition d'applications est une loi de composition interne sur l'ensemble $\mathcal{F}(E, E)$.*

Définition. *Soit $\star$ une loi de composition interne sur un ensemble E.*
On dit que la loi $\star$ est associative si $\forall (x, y, z) \in E^3,\ (x \star y) \star z = x \star (y \star z)$
On dit que la loi $\star$ est commutative si $\forall (x, y) \in E^2,\ x \star y = y \star x$
On dit que la loi $\star$ admet $e \in E$ comme élément neutre si $\forall x \in E,\ x \star e = e \star x = x$

Exemple. *L'union et l'intersection sont associatives et commutatives. Elles admettent un élément neutre qui est $\emptyset$ pour l'union et E pour l'intersection.*
La composition de deux applications de E dans E est associative, mais pas commutative. Elle admet Id_E comme élément neutre.

Proposition. *Si $\star$ est une loi de composition interne sur E admettant un élément neutre, alors celui-ci est unique.*

Définition. *Soit $\star$ une loi de composition interne sur un ensemble E admettant e comme élément neutre.*
On dit qu'un élément $x \in E$ admet un inverse pour la loi $\star$ s'il existe un élément $y \in E$ tel que $x \star y = y \star x = e$.

Exemple. *Seul $\emptyset$ est inversible pour la loi $\cup$ sur $\mathcal{P}(E)$. De même, seul E est inversible pour la loi $\cap$. Dans l'ensemble $\mathcal{F}(E, E)$ muni de la composition, les éléments inversibles sont exactement les fonctions bijectives.*

Proposition. *(*)*
Soit $\star$ une loi de composition interne associative sur un ensemble E admettant un élément neutre. Soit $x \in E$. Si x admet un inverse pour la loi $\star$, alors cet inverse est unique. On le note x^{-1}.

Remarque : L'hypothèse d'associativité est primordiale.

Proposition. *(*) Soit $\star$ une loi de composition interne associative sur un ensemble E admettant un élément neutre. Si x et y sont deux éléments de E inversibles, alors $x \star y$ est également inversible et $(x \star y)^{-1} = y^{-1} \star x^{-1}$.*

Remarque : L'hypothèse d'associativité est primordiale.

II. Groupes

1. Définitions et premiers exemples

Définition. *Soit G un ensemble et $\star$ une loi de composition interne sur G.*
On dit que $(G,\star)$ est un groupe (ou que l'ensemble G est un groupe pour la loi $\star$) si :
– la loi $\star$ est associative ;
– la loi $\star$ admet un élément neutre ;
– tout élément de G admet un inverse pour la loi $\star$.
De plus, on dit que le groupe $(G,\star)$ est commutatif ou abélien si la loi $\star$ est commutative.

Exemple. *$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{Q}^*,\times)$, $(\mathbb{R},+)$, $(\mathbb{R}^*,\times)$, $(\mathbb{U},\times)$, $(\mathbb{U}_n,\times)$ sont des groupes commutatifs.*
Le groupe $(Bij(E),\circ)$ n'est pas commutatif dès que E contient trois éléments.

Proposition. *Dans un groupe, tout élément est simplifiable.*
Plus précisément si $(G,\star)$ est un groupe, alors pour tout $(x,y,z)\in E^3$, on a :

$$x\star y = x\star z \Rightarrow y=z \quad et \quad y\star x = z\star x \Rightarrow y=z$$

Définition. *Soit $(G,\star)$ un groupe et H une partie de G.*
On dit que H est un sous-groupe de G si
– la partie H est stable pour la loi $\star$ i.e. $\forall (x,y)\in H^2$, $x\star y\in H$.
– H est un groupe pour la loi induite par $\star$.

Proposition. *(*) Soit $(G,\star)$ un groupe.*
Un ensemble H est un sous-groupe de G si, et seulement si, :
– H est une partie de G i.e. $H\subset G$;
– $e_G\in H$;
– H est stable par $\star$ i.e. $\forall (h,h')\in H^2$, $h\star h'\in H$;
– H est stable par passage à l'inverse i.e. $\forall h\in H$, $h^{-1}\in H$.

Remarque. *La condition $e_G\in H$ peut être remplacée par $H\neq\emptyset$.*

Remarque. *En pratique, on montre qu'un ensemble est un groupe en prouvant qu'il s'agit d'un sous-groupe d'un groupe classique.*

Remarque : Si H est un sous-groupe de G, alors ils ont le même élément neutre i.e. $e_H=e_G$ et pour tout $x\in H$, l'inverse de x dans H est égal à l'inverse de x dans G.

Proposition. *(*) Soit $(G_1,\star_1)$ et $(G_2,\star_2)$ deux groupes.*
On définit sur l'ensemble $G_1\times G_2$ la loi produit $\star$ par :

$$\forall (x_1,y_1,x_2,y_2)\in G_1^2\times G_2^2,\quad (x_1,x_2)\star(y_1,y_2)=(x_1\star_1 y_1, x_2\star_2 y_2)$$

Muni de cette loi, l'ensemble $G_1\times G_2$ est un groupe. On l'appelle groupe produit.

Exemple. *Muni de l'addition usuelle $\mathbb{R}^n$ a une structure de groupe.*

Proposition. *(*) Soit $(G,\star)$ un groupe et D un ensemble quelconque.*
À tout $(f,g)\in G^D\times G^D$, on associe $f\circledast g : D\to G$, $x\mapsto f(x)\star g(x)$
Muni de la loi $\circledast$, G^D est un groupe.

Proposition. *(*) Soit $(G,\star)$ un groupe et $(H_i)_{i\in I}$ une famille quelconque de sous-groupes de G, alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.*

Remarque : En particulier, l'intersection de deux sous-groupes est un sous-groupe.

Proposition. *(*) L'union de deux sous-groupes n'est un sous-groupe que si l'un des sous groupes est inclus dans l'autre.*

Corollaire. *(*) Pour toute partie A de G, il existe un plus petit sous-groupe au sens de l'inclusion contenant A. Il est appelé sous-groupe engendré par A.*

Proposition. *(*) Le sous-groupe de G engendré par un élément $g \in G$ se note $< g >$ et on a*

$$< g >= \{g^n, n \in \mathbb{Z}\}$$

où $g^0 = e_G$ et pour tout $n \in \mathbb{N}^*$, on a $g^n = \underbrace{g \star ... \star g}_{n\ fois}$ et $g^{-n} = \underbrace{g^{-1} \star ... \star g^{-1}}_{n\ fois}$

2. Morphismes de groupes

Définition. *Soit $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes et f une application de G_1 dans G_2. On dit que f est un morphisme de groupes si*

$$\forall (x, y) \in G_1^2, \quad f(x \star_1 y) = f(x) \star_2 f(y)$$

On dit que f est un isomorphisme de groupes si f est un morphisme de groupes et si f est bijective.
On dit que f est un automorphisme de $(G_1, \star_1)$ si f est un isomorphisme de $(G_1, \star_1)$ dans lui même.

Exemple. *Les applications suivantes sont des morphismes de groupes :*

- $\exp : (\mathbb{R}, +) \to (\mathbb{R}^{*+}, \times),\ x \mapsto e^x$,
- $\ln : (\mathbb{R}^{*+}, \times) \to (\mathbb{R}, +),\ x \mapsto \ln(x)$,
- $(\mathbb{R}, +) \to (\mathbb{U}, \times),\ x \mapsto e^{ix}$.
- $(\mathbb{C}, +) \to (\mathbb{C}^*, \times),\ x \mapsto e^x$.

Proposition. *(*) Soient $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes et e_1 et e_2 leur éléments neutres. Si f un morphisme de $(G_1, \star_1)$ dans $(G_2, \star_2)$, alors on a*

$$f(e_1) = e_2 \quad et \quad \forall x \in G_1,\ f(x^{-1}) = f(x)^{-1}$$

Proposition. *(*) Soit $(G_1, \star_1)$, $(G_2, \star_2)$ et $(G_3, \star_3)$ trois groupes.*
Si f et g sont des morphismes de groupes respectivement de G_1 dans G_2 et de G_2 dans G_3, alors $g \circ f$ est un morphisme de groupes de G_1 dans G_3.

Proposition. *(*) Soit f un isomorphisme de $(G_1, \star_1)$ dans $(G_2, \star_2)$ alors son inverse f^{-1} est un isomorphisme de $(G_2, \star_2)$ dans $(G_1, \star_1)$*

Proposition. *(*) L'ensemble $Aut(G)$ des automorphismes d'un groupe G est un groupe pour la composition.*

Proposition. *(*) Soit f un morphisme de $(G_1, \star_1)$ dans $(G_2, \star_2)$ alors*
- *L'image par f de tout sous-groupe de $(G_1, \star_1)$ est un sous-groupe de $(G_2, \star_2)$, c'est-à-dire que si H_1 est un sous-groupe de G_1, alors $f(H_1) = \{f(x), x \in H_1\}$ est un sous-groupe de G_2.*
- *L'image réciproque par f de tout sous-groupe de $(G_2, \star_2)$ est un sous-groupe de $(G_1, \star_1)$, c'est-à-dire que si H_2 est un sous-groupe de G_2, alors $f^{-1}(H_2) = \{x \in G_1 : f(x) \in H_2\}$ est un sous-groupe de G_1.*

Définition. *Soit f un morphisme de $(G_1, \star_1)$ dans $(G_2, \star_2)$. On appelle image de f l'ensemble*

$$\mathrm{Im}f = \{f(x), x \in G_1\} = f(G_1)$$

et noyau de f l'ensemble $\mathrm{Ker}f = \{x \in G_1 : f(x) = e_{G_2}\} = f^{-1}(\{e_{G_2}\})$
D'après la proposition précédente, ce sont des groupes.

Proposition. *(*) Soit f un morphisme de groupes de $(G_1, \star_1)$ dans $(G_2, \star_2)$ alors :*
- *f est surjective si et seulement si* $\mathrm{Im}f = G_2$
- *f est injective si et seulement si* $\mathrm{Ker}f = \{e_{G_1}\}$

Remarque : La première propriété n'ait qu'une traduction de la définition.

III. Anneaux

1. Définitions et premiers exemples

Définition. *On dit que $(A,+,\times)$ est un anneau si $+$ et $\times$ sont deux lois de composition interne sur A telles que*
– *$(A,+)$ est un groupe commutatif*
– *$\times$ est associative*
– *$\times$ est distributive par rapport à $+$.*
– *$\times$ admet un élément neutre.*
On note 0_A l'élément neutre de la loi $+$ et 1_A celui de la loi $\times$.
A est dit commutatif si la loi $\times$ est commutative.

Exemples : $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{R}^{\mathbb{R}},+,\times)$ sont des anneaux .

Proposition. *Soit $(A,+,\times)$ un anneau et A^* l'ensemble des éléments de A admettant un inverse alors $(A^*,\cdot)$ est un groupe appelé groupe unité.*

Remarque : Le groupe unité de $(\mathbb{Z},+,\cdot)$ est $\{-1,1\}$, celui de $(\mathbb{R},+,\cdot)$ est $\mathbb{R}\setminus\{0\}$ et celui de $(\mathbb{R}^{\mathbb{R}},+,\times)$ est $\{f\in\mathbb{R}^{\mathbb{R}} : \forall x\in\mathbb{R},\, f(x)\neq 0\}$.

Définition. *Soit $(A,+,\times)$ un anneau et $B\subset A$. On dit que B est un sous-anneau de A si*
– *la partie B est stable pour les lois $+$ et $\times$*
– *B est un anneau pour les lois induites.*
– *$1_B = 1_A$.*

Proposition. *(*) Soit $(A,+,\times)$ un anneau. B est un sous-anneau de A si, et seulement si :*
– *$B\subset A$*
– *$1_A\in B$*
– *B est stable par $+$ et $\times$ i.e. $\forall (b,b')\in B^2$, $b+b'\in B$ et $b\times b'\in B$*
– *B est stable par passage à l'inverse pour la loi $+$ i.e. $\forall b\in B$, $-b\in B$*

Remarque. *En pratique, on montre qu'un ensemble est un anneau en prouvant qu'il s'agit d'un sous-anneau d'un anneau classique.*

Proposition. *(*) Soit $(A_1,+_1,\times_1)$ et $(A_2,+_2,\times_2)$ deux anneaux.*
On définit sur l'ensemble $A_1\times A_2$ les lois $+$ et $\times$ par :

$$\forall (x_1,y_1,x_2,y_2)\in A_1^2\times A_2^2,\ (x_1,x_2)+(y_1,y_2)=(x_1+_1y_1,x_2+_2y_2) \text{ et } (x_1,x_2)\times(y_1,y_2)=(x_1\times_1 y_1,x_2\times_2 y_2)$$

Muni de ces lois, l'ensemble $A_1\times A_2$ est un anneau. On l'appelle anneau produit.

Proposition. *(*) Soit $(A,+,X)$ un anneau et D un ensemble quelconque.*
À tout $(f,g)\in A^D\times G^D$, on associe

$$f\bigoplus g : D\to G,\ x\mapsto f(x)+g(x) \text{ et } f\bigotimes g : D\to A,\ x\mapsto f(x)\times g(x)$$

Muni des lois $\bigoplus$ et $\bigotimes$, A^D est un groupe.

Proposition. *(*) Soit $(A,+,\star)$ un anneau et $((A_i,+,\star))_{i\in I}$ une famille de sous-anneaux de A alors $\bigcap_{i\in I}A_i$ est un sous-anneau de A.*

Corollaire. *(*) Soit $(A,+,\star)$ un anneau et B une partie de A. Il existe un plus petit sous-anneau au sens de l'inclusion contenant B. Il est appelé sous-anneau engendré par B.*

2. Morphisme d'anneaux

Définition. *Soit $(A_1, +_1, \star_1)$ et $(A_2, +_2, \star_2)$ deux anneaux et $f \in A_2^{A_1}$.*
On dit que f est un morphisme d'anneaux si
- $\forall (x, y) \in A_1^2, \quad f(x +_1 y) = f(x) +_2 f(y)$
- $\forall (x, y) \in A_1^2, \quad f(x \star_1 y) = f(x) \star_2 f(y)$
- $f(1_{A_1}) = 1_{A_2}$

On dit que f est un isomorphisme d'anneaux si f est un morphisme d'anneaux et si f est bijective.
On dit que f est un automorphisme d'un anneau A si f est un morphisme d'anneaux de A dans A.

Proposition. *(*) Soit $(A_1, +_1, \star_1)$, $(A_2, +_2, \star_2)$ et $(A_3, +_3, \star_3)$ trois anneaux.*
Si f et g sont des morphismes d'anneaux respectivement de $(A_1, +_1, \star_1)$ dans $(A_2, +_2, \star_2)$ et de $(A_2, +_2, \star_2)$ dans $(A_3, +_3, \star_3)$ alors $g \circ f$ est un morphisme d'anneaux de $(A_1, +_1, \star_1)$ dans $(A_3, +_3, \star_3)$.

Proposition. *(*) Soit f un isomorphisme d'anneaux de $(A_1, +_1, \star_1)$ dans $(A_2, +_2, \star_2)$ alors f^{-1} est un isomorphisme d'anneaux de $(A_2, +_2, \star_2)$ dans $(A_1, +_1, \star_1)$*

Corollaire. *(*) Soit $(A, +, \star)$ un anneau alors l'ensemble des automorphismes d'anneaux de A est un groupe pour le loi $\circ$.*

Proposition. *(*) Soit f un morphisme d'anneaux de $(A_1, +_1, \star_1)$ dans $(A_2, +_2, \star_2)$. Alors :*
- *l'image par f de tout sous-anneau de $(A_1, +_1, \star_1)$ est un sous-anneau de $(A_2, +_2, \star_2)$;*
- *l'image réciproque par f de tout sous-anneau de $(A_2, +_2, \star_2)$ est un sous-anneau de $(A_1, +_1, \star_1)$.*

3. Calculs dans un anneau

Proposition. *Soit $(A, +, \star)$ un anneau, alors*
- $\forall x \in A \quad x \star 0_A = 0_A \star x = 0_A$
- $\forall (x, y) \in A^2, \quad -(x \star y) = (-x) \star y = x \star (-y)$

Définition. *Soit $(A, +, \star)$ un anneau, on définit la suite $(n\,a)_{n\in\mathbb{N}}$ par*
- $0\,a = 0_A$
- $\forall n \in \mathbb{N}, \quad (n+1)\,a = n\,a + a$

et la suite $(a^n)_{n\in\mathbb{N}}$ par
- $a^0 = 1_A$
- $\forall n \in \mathbb{N}, \quad a^{n+1} = a^n \cdot a$

Pour tout entier n, on note $(-n)\,a = -(n\,a)$ et, si a est inversible, $a^{-n} = (a^n)^{-1} = \left(a^{-1}\right)^n$.

Proposition. *(Binôme de Newton)(*)*
Soit $(A, +, \times)$ un anneau et $(a, b) \in A^2$ tels que $a \times b = b \times a$ alors pour tout entier n,

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

Proposition. *(Égalité de Bernoulli) (*)*
Soit $(A, +, \times)$ un anneau et $(a, b) \in A^2$ tels que $a \times b = b \times a$ alors pour tout entier n,

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

4. Corps

Définition. *On dit que $(K, +, \times)$ est un corps si $(K, +, \times)$ est un anneau commutatif tel que tout élément de K distinct de 0_A admet un inverse pour la loi $\times$.*

Proposition. *$(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps.*

Définition. *Soit $(K, +, \times)$ un corps. On dit que K' est un sous-corps de $(K, +, \times)$ si K' est un sous-anneau de K et si K' est un corps pour les lois induites.*

Proposition. *Soit $(K, +, \times)$ un corps et $K' \subset K$ alors K' est un sous-corps de $(K, +, \times)$ si, et seulement si,*
– *K' est un sous-anneau de $(K, +, \cdot)$*
– *$\forall x \in K' \setminus \{0\}$, $x^{-1} \in K'$*