Table des matières

I Lois de composition . . . 2
I.1 Généralités . . . 2
I.2 Partie stable pour une loi . . . 2
I.3 Homomorphismes . . . 3
I.4 Commutativité et associativité . . . 3
I.5 Distributivité . . . 4
I.6 Elément neutre . . . 4
I.7 Structure de monoïde . . . 5
I.8 Symétrique d'un élément . . . 6
I.9 Eléments simplifiables . . . 7
I.10 Propriétés transportées par un morphisme surjectif . . . 7
II Groupes, sous-groupes . . . 8
II.1 Structure de groupe . . . 8
II.2 Sous-groupes . . . 9
II.3 Morphismes de groupes . . . 11
II.4 Sous-groupe engendré par un élément . . . 11
II.5 Groupes monogènes, groupes cycliques . . . 13
III Le groupe symétrique . . . 14
III.1 Le groupe symétrique . . . 14
III.2 Cycles et transpositions . . . 14
III.3 Décompositions d'une permutation . . . 16
III.4 Signature d'une permutation . . . 17

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 18 pages.

I Lois de composition

I.1 Généralités

Définition

Une *loi de composition* sur un ensemble E est une application de $E \times E$ vers E.

Notations

- Plutôt que *loi de composition*, on dit aussi *opération*, ou plus simplement *loi*.
- Plutôt que de noter par exemple $f(u,v)$ (notation *préfixée*) l'image du couple (u,v), on la note $u * v$, $u \mathsf{T} v$, $u + v$, etc. (notation *infixée*) et on parle alors des lois $*$, T, $+$, etc.
- On note souvent $(E,*)$ pour désigner un ensemble E muni d'une loi de composition $*$.

Exemples

- Les lois $\cup$ (union), $\cap$ (intersection) et Δ (différence symétrique) sur $\mathcal{P}(E)$.
- La loi $\circ$ (loi de composition) sur $\mathcal{F}(E)$, ensemble des applications de E dans E.
- Les lois $+$ et $\times$ sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et $\mathbb{C}$.
  La loi $\times$est notée par *juxtaposition* : ab plutôt que $a \times b$.
- Sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ (ou sur tout ensemble totalement ordonné) les lois min et max (minimum et maximum). Elles sont notées de façon préfixée : $\min(x,y)$, $\max(x,y)$.
- Deux autres lois notées de façon préfixée sont les lois pgcd et ppcm sur $\mathbb{N}$ ou $\mathbb{Z}$.
- La "soustraction" (opération $-$) est une loi de composition sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et $\mathbb{C}$, mais ce n'est pas une loi de composition sur $\mathbb{N}$ (elle n'est pas *partout définie*).
- Si E est muni de la loi $*$ et si X est un ensemble, on définit une loi, encore notée $*$, sur l'ensemble $\mathcal{F}(X,E)$ des applications de E vers X, en posant :

$$\forall (f,g) \in \mathcal{F}(E,X)^2, \forall x \in X, (f*g)(x) = f(x) * g(x)$$

  On définit ainsi $+$ et $\times$ sur l'ensemble des applications de X vers $\mathbb{R}$ (ou $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$).
  Quand $X = \mathbb{N}$, on définit ainsi la loi $*$ sur l'ensemble des suites de E.

I.2 Partie stable pour une loi

Définition

Soit E un ensemble muni de la loi $*$, et F une partie de E.
On dit que F est *stable* pour la loi $*$ si : $\forall (x,y) \in F \times F, x * y \in F$.
La restriction à $F \times F$ de la loi $*$ définit alors une loi de composition sur F, appelée *loi induite*, en général encore notée $*$.

Exemples

- $\mathbb{R}^-$ et $\mathbb{R}^+$ sont deux parties stables de $\mathbb{R}$, pour la loi $+$.
- Pour la loi $\times$, $\mathbb{R}^+$ est encore une partie stable, mais ce n'est pas le cas de $\mathbb{R}^-$.
- Toujours pour la loi $\times$, $[-1,1]$ est une partie stable de $\mathbb{R}$.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 18 pages.

I.3 Homomorphismes

Définition

Soient E et F deux ensembles, munis respectivement des lois $*$ et T.
Soit f une application de E dans F.
On dit que f est un *homomorphisme* (ou un *morphisme*) de $(E,*)$ dans (F,T) si :
$\forall (x,y) \in E^2, f(x*y) = f(x)\mathsf{T}f(y)$.

Cas particuliers

- Un morphisme de $(E,*)$ dans $(E,*)$ est appelé un *endomorphisme* de $(E,*)$.
- Un morphisme bijectif de $(E,*)$ dans (F,T) est appelé un *isomorphisme*.
- Si un tel isomorphisme existe, on dit que $(E,*)$ et (F,T) sont *isomorphes*.
  D'un point de vue mathématique, deux ensembles isomorphes ont exactement les mêmes propriétés, relativement à leurs lois respectives, et peuvent être considérés comme deux représentations différentes d'une même situation.
- Un isomorphisme de $(E,*)$ sur lui-même est appelé un *automorphisme* de $(E,*)$.

Proposition *(Isomorphisme réciproque)*

Soit f un isomorphisme de $(E,*)$ sur (F,T).
Alors f^{-1} est un isomorphisme de (F,T) sur $(E,*)$.

Exemples

- Le "passage au complémentaire" est un isomorphisme de $(\mathcal{P}(E),\cup)$ sur $(\mathcal{P}(E),\cap)$.
  Il est son propre isomorphisme réciproque.
- L'application $x \to \exp(x)$ est un isomorphisme de $(\mathbb{R},+)$ sur $(\mathbb{R}^{+*},\times)$.
  L'application $x \to \ln(x)$ est l'isomorphisme réciproque, de $(\mathbb{R}^{+*},\times)$ sur $(\mathbb{R},+)$.

I.4 Commutativité et associativité

Définition

Soit $*$ une loi sur un ensemble E.
On dit que la loi $*$ est *commutative* si : $\forall (x,y) \in E^2, x*y = y*x$.
On dit que la loi $*$ est *associative* si : $\forall (x,y,z) \in E^3, (x*y)*z = x*(y*z)$.

Exemples

- Les lois $+$ et $\times$ sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et $\mathbb{C}$, sont commutatives et associatives.
- Il en est de même avec les lois min et max sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.
- Même chose avec les lois $\cup$, $\cap$, Δ sur $\mathcal{P}(E)$.
- La loi $-$ (sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et $\mathbb{C}$) n'est ni commutative, ni associative.
- La loi $\circ$ (composition des applications) est associative sur $\mathcal{F}(E)$. Elle n'est pas commutative dès que E possède au moins deux éléments (considérer les applications constantes).
- Si X est un ensemble et si E est muni de $*$ commutative (resp. associative), alors la loi $*$ définie sur $\mathcal{F}(X,E)$ par $\forall x \in X, (f*g)(x) = f(x)*g(x)$ est commutative (resp. associative).

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 18 pages.

Remarques

– Même si la loi $*$ sur E n'est pas commutative, il peut se trouver des éléments x et y de E qui vérifient $x*y=y*x$. On dit alors que x et y *commutent*.
Par exemple, dans un plan affine euclidien $\mathcal{P}$, les rotations de même centre commutent deux à deux (pour la loi $\circ$).

– Quand une loi $*$ est associative, une expression comme $a*b*\ldots*x*y*z$ est définie sans ambiguité : les parenthèses qui indiquent dans quel ordre on combine les éléments deux à deux sont en effet inutiles.
Si de plus la loi $*$ est commutative, alors on peut changer l'ordre des termes et en particulier regrouper ceux d'entre eux qui sont identiques.
On notera ainsi $x*y*x*y*z*y*x*y=x^3*y^4*z$, à condition de poser, pour tout n de $\mathbb{N}$, $a^n=a*a*\ldots*a$ (a apparaissant n fois).

– L'associativité permet de noter :
$\begin{cases}\min(x,y,z,\ldots) \text{ ou } \max(x,y,z,\ldots) \text{ pour tous réels } x,\ y,\ z, \text{ etc.}\\ \text{ppcm}(a,b,c,\ldots) \text{ ou } \text{pgcd}(a,b,c,\ldots) \text{ pour tous entiers } a,\ b,\ c, \text{ etc.}\end{cases}$

I.5 Distributivité

Définition

Soit E un ensemble muni de deux lois $*$ et T.
On dit que la loi $*$ est *distributive* par rapport à la loi T si, pour tous x,y,z de E :
$\begin{cases}x*(y\mathsf{T}z)=(x*y)\mathsf{T}(x*z) & \text{(distributivité } \textit{à gauche}\text{)}\\ (x\mathsf{T}y)*z=(x*z)\mathsf{T}(y*z) & \text{(distributivité } \textit{à droite}\text{)}\end{cases}$

Exemples et remarques

– Si la loi $*$ est commutative, l'une de ces deux propriétés implique l'autre.

– Dans $\mathcal{P}(E)$, les lois $\cup$ et $\cap$ sont distributives l'une par rapport à l'autre.

– Dans $\mathcal{P}(E)$, la loi $\cap$ est distributive par rapport à la loi Δ.
En revanche la loi Δ n'est pas distributive par rapport à la loi $\cap$.

– Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, la loi $\times$ est distributive par rapport à la loi $+$.

– Si X est un ensemble et si E est muni de deux lois $*$ et T ($*$ étant distributive par rapport à T), on définit des lois homonymes sur $\mathcal{F}(X,E)$:
$\forall\, x\in X,(f*g)(x)=f(x)*g(x)$, et $(f\mathsf{T}g)(x)=f(x)\mathsf{T}g(x)$.
Alors, dans $\mathcal{F}(E,X)$, $*$ est encore distributive par rapport à T.

– La distributivité de $*$ par rapport à T (supposée ici associative) permet d'écrire :
$(a\mathsf{T}b)*(c\mathsf{T}d)=(a*c)\mathsf{T}(a*d)\mathsf{T}(b*c)\mathsf{T}(b*d)$.

I.6 Elément neutre

Définition

Soit E un ensemble muni d'une loi de composition $*$. Soit e un élément de E.
On dit que e est *élément neutre*, pour la loi $*$, si : $\forall\, a\in E, a*e=e*a=a$.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 18 pages.

Remarque

Si la loi $*$ est commutative, l'égalité $a * e = e * a$ est automatiquement réalisée.

Proposition *(Unicité de l'élément neutre)*

L'élément neutre de E pour la loi $*$, s'il existe, est unique.

Remarques

- Il est beaucoup plus juste de dire que c'est E qui *possède* un élément neutre e pour la loi $*$, plutôt que de dire que c'est la loi $*$ qui possède l'élément neutre e.
- La notation $+$ peut être employée en dehors des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: elle doit cependant être réservée aux lois commutatives. Dans ce cas, l'élément neutre, s'il existe, sera noté 0. De même, pour une loi noté multiplicativement (ou par juxtaposition), on pourra noter 1 l'élément neutre éventuel (s'il n'y a pas de risque d'ambiguité).

Exemples et remarques

- Dans $\mathcal{P}(E)$: $\emptyset$ est neutre pour la loi $\cup$ (et pour la loi Δ), et E est neutre pour la loi $\cap$.
- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$: 0 est neutre pour la loi $+$ et 1 est neutre pour la loi $\times$.
- Dans $\mathcal{F}(E)$: l'application Identité id_E est neutre pour la loi $\circ$ (composition).
- Dans $\mathbb{N}$: 0 est neutre pour la loi max, et il n'y a pas de neutre pour la loi min.
- Dans $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$: les lois min et max n'ont pas d'élément neutre.
- Soit X un ensemble quelconque, et E un ensemble muni d'une loi $*$ avec un neutre e.
  On munit $\mathcal{F}(X, E)$ de la loi $*$, définie par :
  $\forall (f, g) \in \mathcal{F}(X, E)^2, \forall x \in X, (f * g)(x) = f(x) * g(x)$.
  Alors l'application constante, qui à tout x de E associe e, est neutre pour cette loi.
  Ainsi, sur l'ensemble $\mathcal{F}(\mathbb{N}, \mathbb{K})$ des suites (à valeurs dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$), la suite constante 0 est neutre pour l'addition, et la suite constante 1 est neutre pour le produit.

I.7 Structure de monoïde

Définition

Soit E un ensemble muni d'une loi $*$. On dit que E possède une structure de *monoïde* pour la loi $*$, ou encore que $(E, *)$ est un monoïde, si : $\begin{cases} \text{La loi } * \text{ est associative.} \\ \text{Il existe un élément neutre } e. \end{cases}$

Exemples et remarques

- De par la définition, un monoïde est toujours non vide.
- $(\mathbb{N}, +)$ et $(\mathbb{N}, \times)$ sont des monoïdes (idem en remplaçant $\mathbb{N}$ par $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$).
- $(\mathcal{P}(E), \cup)$, $(\mathcal{P}(E), \cap)$ et $(\mathcal{P}(E), \Delta)$ sont des monoïdes.
- $(\mathcal{F}(E), \circ)$ est un monoïde.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 18 pages.

– Si $(E, *)$ est un monoïde, et si X est un ensemble, $(\mathcal{F}(X, E), *)$ est un monoïde.
En particulier, l'ensemble $(\mathcal{F}(\mathbb{N}, E), *)$ des suites à valeurs dans le monoïde E, muni de la loi homonyme $*$, est lui-même un monoïde.

– Si $(E, *)$ est un monoïde, et si F est une partie stable de E contenant le neutre e, alors $(F, *)$ (avec la loi induite) est encore un monoïde.

I.8 Symétrique d'un élément

Définition

Soit $(E, *)$ un monoïde d'élément neutre e. Soit x un élément de E.

On dit que x est *symétrisable* (ou *inversible*) pour la loi $*$, s'il existe un élément x' de E tel que $x * x' = x' * x = e$.

Si un tel élément x' existe, il est unique. On l'appelle le *symétrique* (ou l'*inverse*) de x.

Notation additive

Dans le cas d'une loi $+$ (nécessairement commutative, d'élément neutre 0), le symétrique d'un élément x est appelé son *opposé*, et est noté $-x$.

Pour tous éléments x et y (x possédant un opposé), on note $y - x$ plutôt que $y + (-x)$.

Notation multiplicative

Dans le cas d'une loi multiplicative $\times$ (éventuellement notée par juxtaposition), le symétrique d'un élément x est en général appelé son *inverse*, et est noté x^{-1}.

Si ce produit est commutatif et si on note 1 son neutre, on peut écrire $\dfrac{1}{x}$ plutôt que x^{-1}.

Le produit yx^{-1} peut alors être noté $\dfrac{y}{x}$ (notamment dans les ensembles de nombres).

Propriétés et remarques

– Soit $(E, *)$ un monoïde, de neutre e. Alors e est inversible et est son propre inverse.

– Si x et y sont inversibles, leur composé $x * y$ est inversible et $(x * y)^{-1} = y^{-1} * x^{-1}$ (attention à l'ordre des facteurs si la loi $*$ n'est pas commutative).

– Si F est une partie stable du monoïde $(E, *)$ contenant le neutre e (un "sous-monoïde" de $(E, *)$) et si x appartient à F, alors l'inversibilité de x doit être examinée relativement à l'appartenance de x :
Si x est inversible dans F, il est inversible dans E (avec le même inverse).
La réciproque est fausse : pour le produit, 2 est inversible dans $\mathbb{R}$ mais pas dans $\mathbb{Z}$.

Exemples

– Dans $(\mathbb{N}, +)$ seul 0 est symétrisable.
Mais tous les éléments de $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ le sont.

– Les éléments inversibles de $(\mathbb{R}, \times)$ sont les éléments non nuls.
C'est la même chose avec $(\mathbb{Q}, \times)$ et $(\mathbb{C}, \times)$.
Le seul élément inversible de $(\mathbb{N}, \times)$ est 1. Ceux de $(\mathbb{Z}, \times)$ sont -1 et 1.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 18 pages.

– On se place dans l'ensemble $\mathcal{F}(\mathbb{N},\mathbb{R})$ des suites à valeurs dans $\mathbb{R}$.
Toutes les suites (u_n) sont symétrisables pour l'addition : l'opposé de la suite de terme général u_n est la suite de terme général $-u_n$.
Seules les suites ne s'annulant jamais sont symétrisables pour le produit : l'inverse de la suite de terme général u_n est alors la suite de terme général $\dfrac{1}{u_n}$.

– Dans $(\mathcal{F}(E),\circ)$, une application est inversible si et seulement si elle est bijective.
Son inverse est alors sa bijection réciproque. La notation f^{-1} est donc justifiée.

I.9 Eléments simplifiables

Définition

Soit E un ensemble muni d'une loi $*$. Soit x un élément de E.
On dit qu'un élément x de E est *simplifiable* (ou encore *régulier*) si :

$$\forall\,(y,z)\in E^2 : \begin{cases} x*y=x*z \Rightarrow y=z & (1)\\ y*x=z*x \Rightarrow y=z & (2)\end{cases}$$

Remarques

– x est simplifiable $\Leftrightarrow$ les applications $t\to x*t$ et $t\to t*x$ sont injectives de E dans E.

– On pourrait traduire (1) en disant : x est simplifiable *à gauche*.
De même, (2) signifie : x est simplifiable *à droite*.

– Quand la loi $*$ est commutative, les propriétés (1) et (2) sont équivalentes.

Propriétés et exemples

– Si la loi $*$ est associative, et si a et b sont simplifiables, alors $a*b$ est simplifiable.

– Si $(E,*)$ est un monoïde et si x est inversible, alors x est simplifiable.
Il suffit par exemple de composer par x^{-1} à gauche pour simplifier x dans l'égalité $x*y=x*z$.

– La réciproque de cette propriété est fausse. En effet, dans $(\mathbb{Z},\times)$ par exemple, tous les éléments non nuls sont simplifiables, mais seuls -1 et 1 sont inversibles.

– Dans $(\mathcal{P}(E),\cup)$, seul $\emptyset$ est inversible, donc simplifiable.
De même, seul E est inversible, donc simplifiable dans $(\mathcal{P}(E),\cap)$.

I.10 Propriétés transportées par un morphisme surjectif

Soit f un morphisme de $(E,*)$ sur (F,T).

– L'ensemble image $f(E)$ est stable pour T.
Dans la suite de cette sous-section, on suppose que f est surjectif de E sur F.

– Si e est neutre dans $(E,*)$ alors $f(e)$ est neutre dans (F,T).
Si x' est le symétrique de x dans $(E,*)$ alors $f(x')$ est celui de $f(x)$ dans (F,T).

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.
Extrait gratuit de document, le document original comporte 18 pages.