Chapitre 11

Structures algébriques

Sommaire

11.1 Lois de composition

11.1.1 Loi de composition interne

Définition 11.1.1 (loi de composition interne sur un ensemble)
Une *loi de composition interne* sur un ensemble E est une application de $E \times E$ vers E.

Plutôt que de noter par exemple $f(u, v)$ (notation *préfixée*) l'image d'un couple (u, v), on la note $u * v$, $u \,\mathrm{T}\, v$, $u + v$, 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 $*$.

On retiendra qu'une *loi de composition* $*$ sur E est un mécanisme permettant, à partir de deux éléments quelconques x et y de E, de former un élément z de E, noté $z = x * y$ et qu'on pourra appeler *composé de x par y pour la loi $*$*. Il est important qu'une loi soit *partout définie* : le résultat $x * y$ doit donc avoir un sens, quels que soient les éléments x et y de E.

Il arrive souvent qu'on utilise plusieurs fois le mécanisme précédent dans un même calcul. Il faut alors préciser, au moyen de parenthèses, dans quel ordre on a effectué les compositions.

Par exemple l'expression $x * y * z$ est a priori dépourvue de signification, et il faudrait écrire :

– soit $(x * y) * z$ si on a d'abord calculé $a = x * y$ avant de calculer $a * z$.

– soit $x * (y * z)$ si on a d'abord calculé $b = y * z$ avant de calculer $x * b$.

Plus compliqué, une expression comme $x * y * z * t$ possède les cinq parenthésages possibles suivants, qui indiquent chacune une chronologie particulière dans les compositions par la loi $*$:

$$(x * y) * (z * t), \quad ((x * y) * z) * t), \quad (x * (y * z)) * t, \quad x * ((y * z) * t) \quad \text{et} \quad x * (y * (z * t))$$

On appréciera donc qu'une loi de composition possède la propriété suivante :

Définition 11.1.2 (associativité d'une loi de composition)
Soit $*$ une loi de composition sur un ensemble E.
On dit que la loi $*$ est *associative* si, pour tous x, y, z de E, on a : $(x * y) * z = x * (y * z)$.

Quand une loi de composition $*$ est associative, une expression comme $a * b * \ldots * x * y * z$ est définie sans ambiguïté : les parenthèses qui indiquent dans quel ordre on combine les éléments deux à deux sont en effet inutiles. En revanche, l'ordre dans lequel les éléments apparaissent, de gauche à droite, reste important, à moins que...

Définition 11.1.3 (éléments qui commutent pour une loi)
Soit $*$ une loi de composition sur un ensemble E.
Soit x et y deux éléments de E. On dit que x et y *commutent* (pour la loi $*$) si $x * y = y * x$.

Définition 11.1.4 (commutativité d'une loi de composition)
Soit $*$ une loi de composition sur un ensemble E.
On dit que la loi $*$ est *commutative* si, pour tous x et y de E, on a : $x * y = y * x$.

Autrement dit : une loi de composition sur E est commutative si tous les éléments de E commutent deux à deux pour cette loi. Quand une loi $*$ est associative et commutative, non seulement une expression comme $a * b * \ldots * x * y * z$ est définie sans ambiguïté, mais on peut aussi changer l'ordre des termes et notamment regrouper ceux d'entre eux qui sont identiques.
On pourra ainsi noter $x * y * x * y * z * y * x * y = x^3 * y^4 * z$ à condition, pour tout entier strictement positif n, de poser $a^n = a * a * \ldots * a$ (l'élément a apparaissant n fois).

11.1.2 Exemples de lois usuelles

Somme et produit sur les ensembles de nombres :

Les lois $+$ et $\times$ usuelles sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et $\mathbb{C}$ sont associatives et commutatives.
La loi produit $\times$ est le plus souvent notée par simple *juxtaposition* : xy plutôt que $x \times y$.
On peut considérer l'opération « différence » sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et $\mathbb{C}$ (mais pas sur $\mathbb{N}$).
Cette loi, définie par $(x, y) \mapsto x - y$, n'est ni associative ni commutative (donc sans intérêt !).

La loi de composition des applications

Soit E un ensemble, et soit $\mathcal{F}(E)$ l'ensemble des applications de E dans E.
On définit la loi $\circ$ (loi de composition) sur $\mathcal{F}(E)$ par $(f, g) \mapsto f \circ g$.

Cette loi est associative, mais elle n'est pas commutative (sauf si E est réduit à un singleton).

Même si la loi $\circ$ n'est pas commutative, il existe des applications f et g qui commutent entre elles, c'est-à-dire qui vérifient $g \circ f = f \circ g$.

Par exemple, en géométrie du plan, les rotations de même centre commutent deux à deux.

Lois sur l'ensemble des parties d'un ensemble

Soit E un ensemble. Les lois $\cup$ (union), $\cap$ (intersection) et Δ (différence symétrique) sur $\mathcal{P}(E)$ sont toutes trois commutatives et associatives.

En revanche, la « différence ensembliste » définie sur $\mathcal{P}(E)$ par $A \setminus B = A \cap \overline{B} = \{x \in A,\ x \notin B\}$, n'est ni associative ni commutative.

Maximum et minimum sur un ensemble totalement ordonné

Soit E un ensemble muni d'une relation d'ordre total note $\leqslant$.

Les lois min et max (minimum et maximum) sont notées de façon préfixée : $\min(x, y)$ et $\max(x, y)$.

Ces deux lois sont associatives et commutatives.

Pgcd et ppcm sur les entiers

Les lois pgcd et ppcm sur $\mathbb{N}$ ou $\mathbb{Z}$ sont commutatives et associatives.

Elles sont notées de façon tantôt préfixe ($\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$), tantôt infixe ($a \wedge b$ et $a \vee b$).

C'est l'associativité qui permet de noter, sans ambiguïté : $\begin{cases} a \wedge b \wedge c \wedge \cdots \\ a \vee b \vee c \vee \cdots \end{cases}$ pour tous entiers $a, b, c, \ldots$

Addition et produit « modulo n »

Si n est un entier strictement positif, notons $\mathbb{N}_n = \{0, 1, 2, \ldots, n-1\}$.

$\mathbb{N}_n$ est donc l'ensemble des restes possibles dans la division euclidienne par n.

On peut définir deux lois sur $\mathbb{N}_n$ à partir des lois $+$ et $\times$ de $\mathbb{N}$, en calculant le résultat modulo n.

Ces deux lois sont associatives et commutatives.

Par exemple, dans $\mathbb{N}_{15}$, on a $11 + 23 = 4$ (car $34 \equiv 4\ [15]$) et $11 \cdot 23 = 13$ (car $11 \cdot 23 = 253 \equiv 13\ [15]$).

Voici la table des lois $+$ et $\times$ dans l'ensemble $\mathbb{N}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (la première ligne et la première colonne de chaque tableau ne sont pas considérées comme faisant partie de la table : elles sont simplement un rappel de la valeur des éléments de $\mathbb{N}_{10}$).

$+$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Table de l'addition dans $\mathbb{N}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$\times$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Table du produit dans $\mathbb{N}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Loi sur l'ensemble des fonctions à valeurs dans $(E, *)$

Soit E un ensemble muni d'une loi $*$, et soit X un ensemble quelconque.

On définit une loi, encore notée $*$, sur l'ensemble $\mathcal{F}(X, E)$ des applications de X vers E.

On pose pour cela : $\forall (f, g) \in \mathcal{F}(X, E)^2,\ \forall x \in X,\ (f * g)(x) = f(x) * g(x)$.

On vérifie que si la loi $*$ sur E est associative (resp. commutative), alors la loi $*$ sur $\mathcal{F}(X, E)$ est encore associative (resp. commutative).

On définit par exemple les lois $+$ et $\times$ sur l'ensemble des applications de X vers $\mathbb{R}$ (ou $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$).

Autre exemple : si $X = \mathbb{N}$ et $E = \mathbb{R}$, on définit la somme $s = u + v$ et le produit $p = uv$ de deux suites $(u_n)_{n\geqslant 0}$ et $(v_n)_{n\geqslant 0}$ de nombres réels en posant, pour tout n de $\mathbb{N}$: $s_n = u_n + v_n$ et $p_n = u_n v_n$.

11.1.3 Élément neutre et inversibilité

Définition 11.1.5

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, pour tout élément x de E, on a : $x * e = e * x = x$.

Remarque : si on sait que la loi $*$ est commutative, l'égalité $x * e = e * x$ est automatiquement réalisée.

Proposition 11.1.1 (unicité de l'élément neutre)

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

Démonstration

Si e et f sont deux éléments neutres pour la loi $*$, alors $e * f = e = f$.

Conventions de vocabulaire

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 souvent 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'ambiguïté).

Quelques exemples

- 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).
- Soit X un ensemble quelconque, et soit 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.

– 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 $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$: les lois min et max n'ont pas d'élément neutre.

Définition 11.1.6 (inversibilité d'un élément)
Soit E un ensemble muni d'une loi associative $*$.
On suppose qu'il existe un élément neutre e.
On dit qu'un élément x est *inversible* (pour la loi $*$) s'il existe x' dans E tel que $x * x' = x' * x = e$.
Si un tel élément x' existe, il est unique.
On le note en général x^{-1}, et on l'appelle l'*inverse* (ou le *symétrique*) de x pour la loi $*$.

Proposition 11.1.2 (inversibilité du produit de deux éléments inversibles)
Soit E un ensemble muni d'une loi associative $*$.
On suppose qu'il existe un élément neutre e.
Soit x et y deux éléments de E, inversibles pour la loi $*$, d'inverses respectifs x^{-1} et y^{-1}.
Alors $x * y$ est inversible, et son inverse est $(x * y)^{-1} = y^{-1} * x^{-1}$.

Remarque : attention à la permutation dans la formule précédente, si la loi $*$ n'est pas commutative.

Notation additive

Dans le cas d'une loi $+$ (nécessairement commutative, d'élément neutre 0), on ne parle pas d'inverse ou de symétrique, mais d'*opposé*, et l'élément en question n'est pas noté x^{-1} ou x' mais $-x$.

L'opposé de x est donc l'unique élément de E tel que $x + (-x) = 0$.

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

En notation additive, la propriété $(x * y)^{-1} = y^{-1} * x^{-1}$ devient $-(x + y) = -y - x = -x - y$.

Propriétés et remarques

– S'il n'y a pas de neutre dans E pour la loi $*$, alors la notion d'élément inversible n'a aucun sens.
– On a demandé à la loi $*$ d'être associative pour garantir l'*unicité du symétrique* si existence.
– L'élément neutre e de E pour la loi $*$ est inversible et il est son propre inverse (car $e * e = e$).

Exemples

– Dans $(\mathbb{N}, +)$ seul l'entier 0 possède un opposé.
Bien sûr, tous les éléments de $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ possèdent un opposé.
Les éléments inversibles de $(\mathbb{R}, \times)$ sont les éléments non nuls (idem avec $(\mathbb{Q}, \times)$ et $(\mathbb{C}, \times)$).
Le seul élément inversible de $(\mathbb{N}, \times)$ est 1. Les seuls éléments inversibles de $(\mathbb{Z}, \times)$ sont -1 et 1.
– Dans $(\mathcal{F}(E), \circ)$, une application est inversible si et seulement si elle est bijective.
Son inverse est alors sa bijection réciproque f^{-1}. La notation f^{-1} ne prête donc pas à confusion.
– Dans le cas des applications de $\mathbb{R}$ dans $\mathbb{R}$, on ne confondra le produit fg et la composition $f \circ g$.
On sait que le neutre pour la loi $\circ$ est Id_E, et que f est inversible pour cette loi si f est bijective.
En revanche, le neutre pour la loi produit est l'application constante $x \mapsto 1$, et f est inversible pour cette loi (c'est-à-dire il existe une application g telle que $fg = 1$) si et seulement si f ne s'annule jamais. L'inverse de f (pour le produit !) est alors l'application $1/f$.

11.1.4 Distributivité

Définition 11.1.7
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 :
– d'une part $x * (y \,\mathrm{T}\, z) = (x * y) \,\mathrm{T}\, (x * z)$ (distributivité *à gauche*)
– d'autre part $(x \,\mathrm{T}\, y) * z = (x * z) \,\mathrm{T}\, (y * z)$ (distributivité *à droite*)

Exemples et remarques

– Si la loi $*$ est commutative, chacune des deux distributivités (à gauche ou à droite) implique l'autre.
– Dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, on a toujours $x(y+z) = xy + xz$: la loi $\times$ est distributive par rapport à la loi $+$.
En revanche la loi $+$ n'est pas distributive par rapport à la loi $\times$.
– Dans $\mathcal{P}(E)$, les lois $\cup$ et $\cap$ sont distributives l'une par rapport à l'autre.
On a en effet toujours les égalités : $\begin{cases} A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{cases}$
Toujours dans $\mathcal{P}(E)$, la loi $\cap$ est distributive par rapport à la loi Δ.
Mais réciproquement, la loi Δ n'est pas distributive par rapport à la loi $\cap$.
– Les propriétés de distributivité, d'associativité, de commutativité sont utiles aux développements.
Il est par exemple clair que $(a+b)(c+d) = ac + ad + bc + bd$ pour tous réels a, b, c, d.
Mais si A, B, C, D sont quatre parties d'un ensemble E, les mêmes propriétés permettent d'écrire :
d'une part : $(A \cup B) \cap (C \cup D) = (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D)$
d'autre part : $(A \cap B) \cup (C \cap D) = (A \cup C) \cap (A \cup D) \cap (B \cup C) \cap (B \cup D)$

11.1.5 Partie stable pour une loi

Définition 11.1.8
Soit E un ensemble muni d'une loi $*$, et soit 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, qu'on appelle *loi induite sur F par celle de E*, et qu'en général on note encore $*$.

Quelques exemples dans $(\mathbb{R}, +)$ ou $(\mathbb{R}, \times)$

L'intervalle $\mathbb{R}^+ = [0, +\infty[$ est stable, à la fois pour l'addition et pour le produit.

L'intervalle $[-1, 1]$ est stable pour le produit, mais pas pour l'addition.

L'intervalle $[-2, 2]$ n'est stable ni pour le produit, ni pour l'addition.

L'intervalle $\mathbb{R}^- =]-\infty, 0]$ est stable pour l'addition, mais pas pour le produit.

L'ensemble des rationnels est une partie stable de $\mathbb{R}$, pour les deux lois $+$ et $\times$.

Remarques en cas de loi induite

Soit F une partie stable de E pour la loi $*$.
Si on munit F de la loi induite (toujours notée $*$), on dispose donc à la fois de $(E,*)$ et de $(F,*)$.

- Si la loi $*$ sur E est commutative (resp. associative), il en est de même de la loi induite $*$ sur F.
- Si e est neutre dans $(E,*)$, et si e est dans F, alors bien sûr e est encore neutre dans $(F,*)$.
  Mais attention, il est possible qu'il y ait un neutre e' dans F et qu'il n'y ait pas de neutre dans E. Il est possible aussi qu'il y ait un neutre e dans E, mais que e n'appartienne pas à F (dans ces conditions, il est possible que F possède lui-même son propre neutre, ou qu'il n'en possède pas !).
- Supposons qu'un élément e de F soit neutre dans $(E,*)$, donc neutre dans $(F,*)$.
  Soit x un élément de F. Si on examine l'inversibilité de x pour la loi $*$, il faut savoir sans ambiguïté si on parle d'inversibilité dans F (pour la loi $*$ induite) ou dans E (pour la loi $*$ initiale).
  Par exemple 2 est inversible dans $(\mathbb{R},\times)$, mais pas dans $(\mathbb{Z},\times)$ (car $1/2$ n'existe pas dans $\mathbb{Z}$!).

11.2 Groupes et sous-groupes

11.2.1 Structure de groupe

Définition 11.2.1
Soit G un ensemble muni d'une loi de composition $*$.
On dit que $(G,*)$ est un *groupe* si :
- la loi $*$ est associative, et il y a un élément neutre e.
- tout élément de G possède un inverse.

Si de plus la loi $*$ est commutative, on dit que $(G,*)$ est un groupe *commutatif* (ou encore *abélien*).

Premières remarques

- Par définition un groupe est toujours non vide (puisqu'il y a au moins l'élément neutre).
- Si la loi est notée $+$, on dit que $(G,+)$ est un *groupe additif*. Le neutre est noté 0. On rappelle qu'une loi $+$ est toujours supposée commutative, et qu'on note $-x$ l'opposé (plutôt que l'inverse) de x.
- En cas de loi produit (notation $\times$ ou par juxtaposition), on dit que $(G,\times)$ est un *groupe multiplicatif*.

Exemples usuels

- Les ensembles $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes additifs.
- Les ensembles $(\mathbb{Q}^*,\times)$, $(\mathbb{Q}^{+*},\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{R}^{+*},\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes multiplicatifs.
- L'ensemble $\mathcal{U}=\{z\in\mathbb{C},\ |z|=1\}$ est un groupe multiplicatif.
  Il en est de même de l'ensemble $\mathcal{U}_n=\{z\in\mathbb{C},\ z^n=1\}$ des racines n-ièmes de l'unité.

Définition 11.2.2 (groupe des permutations d'un ensemble E)
Soit E un ensemble. On note $\mathcal{S}_E$ l'ensemble des bijections de E dans E (on dit les *permutations* de E).
Alors $\mathcal{S}_E$ est un groupe pour la loi de composition des applications.

Remarque : dès que l'ensemble E possède au moins trois éléments, le groupe $\mathcal{S}_E$ est non commutatif.

Définition 11.2.3 (puissances entières d'un élément)
Soit $(G, *)$ un groupe multiplicatif, d'élément neutre e, et soit x un élément de G.
On définit les puissances entières x^n ($n \in \mathbb{Z}$) de x de la manière suivante :
– on pose $x^0 = e$.
– pour tout n de $\mathbb{N}^*$, on pose $x^n = x * x^{n-1}$, c'est-à-dire $x^n = x\,x\,\cdots x$ (n fois).
– pour tout n de $\mathbb{N}^*$, on pose $x^{-n} = (x^n)^{-1}$, ou ce qui revient au même : $x^{-n} = (x^{-1})^n$.

Avec ces notations, on a : $x^n\,x^m = x^{n+m}$, et $(x^n)^m = x^{nm}$ pour tout x de G et tous m, n de $\mathbb{Z}$.

Si les deux éléments x et y commutent, alors $(x * y)^n = x^n * y^n$ (attention, c'est faux si $x * y \neq y * x$).

En notation additive, on ne note plus x^n mais nx, pour tout n de $\mathbb{Z}$.

Dans un groupe additif $(G, +)$, on considérera donc $3x$, par exemple, non pas comme le produit de 3 par x, mais comme un raccourci pour désigner $x + x + x$.

Proposition 11.2.1 (dans un groupe tout élément est simplifiable)
Soit G un groupe pour la loi $*$.
Pour tous éléments x, y, z de G, on a les implications $\begin{cases} (x * y = x * z) \;\Rightarrow\; y = z \\ (y * x = z * x) \;\Rightarrow\; y = z \end{cases}$
On exprime cette propriété en disant que dans un groupe tout élément est simplifiable.

Attention, cette propriété cesse d'être vraie si on n'est pas dans un groupe (il peut exister des éléments « non simplifiables »). Par exemple, dans $(\mathbb{R}, \times)$, on n'a pas l'implication $0x = 0y \Rightarrow x = y$ (mais en revanche tout réel non nul est simplifiable pour le produit).

Dans tout ensemble E muni d'une loi $*$, les implications $\begin{cases} y = z \;\Rightarrow\; (x * y = x * z) \\ y = z \;\Rightarrow\; (y * x = z * x) \end{cases}$ sont toujours vraies (et elles sont mêmes évidentes, et sans grand intérêt).

Proposition 11.2.2
Soit G un groupe pour la loi $*$. Soit a un élément de G.
L'application $g_a : x \mapsto a * x$ (dite « multiplication à gauche par a ») est bijective.
Sa bijection réciproque est $g_{a^{-1}} : x \mapsto a^{-1} * x$ (c'est-à-dire la multiplication à gauche par a^{-1}).
L'application $d_a : x \mapsto x * a$ (dite « multiplication à droite par a ») est bijective.
Sa bijection réciproque est $d_{a^{-1}} : x \mapsto x * a^{-1}$ (c'est-à-dire la multiplication à droite par a^{-1}).

On peut réécrire le résultat précédent en termes de résolutions d'équations dans un groupe.

Proposition 11.2.3 (équations $a \star x = b$ et $x * a = b$ dans un groupe)
Soit G un groupe pour la loi $*$. Soit a, b deux éléments de G.
L'équation $a * x = b$ possède une solution unique, à savoir $x = a^{-1} * b$.
L'équation $x * a = b$ possède une solution unique, à savoir $x = b * a^{-1}$.

11.2.2 Sous-groupe : définition, caractérisation

Définition 11.2.4 (sous-groupe d'un groupe)
Soit $(G,*)$ un groupe et soit H une partie non vide de G.
On dit que H est un *sous-groupe* de $(G,*)$ si :
– l'ensemble H est stable pour la loi $*$: $\forall (x,y) \in H^2,\ x*y \in H$.
– l'ensemble H est « stable pour le passage à l'inverse » : $\forall x \in H,\ x^{-1} \in H$.

Remarque : on n'oubliera pas la condition disant que H est une partie *non vide* de G.
La proposition suivante dit qu'un sous-groupe, c'est un groupe à part entière (le mot « sous » n'a donc rien de péjoratif : il se réfère simplement à l'inclusion des ensembles).

Proposition 11.2.4
Soit H un sous-groupe de $(G,*)$. On munit H de la loi induite.
Alors $(H,*)$ est lui-même un groupe.
Les deux groupes $(G,*)$ et $(H,*)$ ont le même neutre (qui est donc élément de H).
Si x est élément de H, l'inverse x^{-1} de x est le même (du point de vue de G ou de celui de H).

Proposition 11.2.5 (caractérisation des sous-groupes)
Soit $(G,*)$ un groupe et soit H une partie non vide de G.
H est un sous-groupe de $(G,*)$ si et seulement si : $\forall (x,y) \in H^2,\ x*y^{-1} \in H$.
En notation additive : H est un sous-groupe de $(G,+)$ si et seulement si : $\forall (x,y) \in H^2,\ x-y \in H$.

Exemples
– Soit $(G,*)$ un groupe de neutre e. Alors $\{e\}$ et G en sont deux sous-groupes (dits *triviaux*).
– Dans $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, chacun est un sous-groupe du suivant.
– C'est la même chose avec $(\{-1,1\},\times)$, $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{C}^*,\times)$.
– De même, $(\mathbb{R}^{+*},\times)$ est un sous-groupe de $(\mathbb{R}^*,\times)$.
– L'ensemble $\mathcal{U}$ des nombres complexes de module 1 est un sous-groupe de $(\mathbb{C}^*,\times)$.
– L'ensemble $\mathcal{U}_n$ des racines n-ièmes de l'unité est un sous-groupe de $(\mathcal{U},\times)$.

Proposition 11.2.6 (intersection de sous-groupes)
Une intersection quelconque de sous-groupes de G est encore un sous-groupe de G.

Remarque : c'est faux pour la réunion ! Plus précisément, si H et K sont deux sous-groupes de G, $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$ (et alors $H \cup K = K$ ou $H \cup K = H$).

Proposition 11.2.7 (sous-groupes de $(\mathbb{Z},+)$)
On rappelle que si n est un élément de $\mathbb{N}$, on note $n\mathbb{Z} = \{kn, k \in \mathbb{Z}\}$.
Les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$, avec n dans $\mathbb{N}$.

11.3 Structures d'anneau et de corps

11.3.1 Structure d'anneau

Définition 11.3.1 (structure d'anneau)
Soit A un ensemble muni de deux lois de composition, notées $+$ et $\times$.
On dit que $(A, +, \times)$ est un *anneau* si :
– $(A, +)$ est un groupe commutatif (son neutre est en général noté 0).
– La loi $\times$ est associative et distributive par rapport à l'addition.
– Il existe un élément neutre pour le produit $\times$ (en général noté 1).
Si de plus la loi $\times$ est commutative, on dit que $(A, +, \times)$ est un *anneau commutatif*.

Exemples
– $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
– Soit $(A, +, \times)$ un anneau de neutres 0 (pour la loi $+$) et 1 (pour la loi $\times$).
Il est possible que les deux éléments 0 et 1 de A soient identiques !
Mais dans ce cas A se réduit à $\{0\}$ (anneau nul, sans grand intérêt).

Proposition 11.3.1 (groupe des éléments inversibles d'un anneau)
Soit $(A, +, \times)$ un anneau.
L'ensemble des éléments de A qui sont inversibles pour le produit est un groupe pour la loi $\times$.

Exemples
Le groupe des inversibles de l'anneau $(\mathbb{Z}, +, \times)$ se réduit à la paire $\{-1, 1\}$.
Le groupe des inversibles de l'anneau $(\mathbb{R}, +, \times)$ est l'ensemble de tous les réels non nuls.

11.3.2 Calculs dans un anneau

Soit $(A, +, \times)$ un anneau (on note 0 le neutre pour $+$, et 1 le neutre pour $\times$).
Rappelons qu'on note $a - b$ plutôt que $a + (-b)$.
On rappelle également que, pour tout n de $\mathbb{N}^*$, la notation na désigne $a + a + \cdots + a$ (n fois).
Pour tout (a, b, c) de A^3, et tout entier relatif m, on a :

$$a0 = 0a = 0, \qquad \begin{cases} (-a)b = a(-b) = -(ab) \\ (-a)(-b) = ab \end{cases}, \qquad \begin{cases} a(b-c) = ab - ac \\ (a-b)c = ac - bc \end{cases}$$

Sommes et produits, développements
Pour tous $a_m, a_{m+1}, \ldots, a_n$ de A, on écrit : $a_m + a_{m+1} \cdots + a_n = \sum_{k=m}^{n} a_k$ et $a_m\, a_{m+1} \cdots a_n = \prod_{k=m}^{n} a_k$
Si $m > n$, on pose $\sum_{k=m}^{n} a_k = 0$ et $\prod_{k=m}^{n} a_k = 1$ (somme et produit « vides »).

Pour tout b de A, on a : $b\Big(\sum_{k=m}^{n} a_k\Big) = \sum_{k=m}^{n} (ba_k)$, et $\Big(\sum_{k=m}^{n} a_k\Big)b = \sum_{k=m}^{n} (a_k b)$.

Plus généralement : $\Big(\sum_{j=m}^{n} a_j\Big)\Big(\sum_{k=p}^{q} b_k\Big) = \sum_{j=m}^{n}\Big(a_j \sum_{k=p}^{q} b_k\Big) = \sum_{j=m}^{n}\sum_{k=p}^{q} a_j b_k.$

Proposition 11.3.2 (factorisation de $a^n - b^n$ dans un anneau)
Soit $(A, +, \times)$ un anneau, et soit a, b deux éléments de A. On suppose que $ab = ba$.
Alors, pour tout n de $\mathbb{N}^*$, on a l'égalité : $a^n - b^n = (a-b)\Big(\sum_{k=0}^{n-1} a^{n-1-k} b^k\Big)$.

Cas particuliers (toujours si $ab = ba$) : $a^2 - b^2 = (a-b)(a+b)$, et $a^3 - b^3 = (a-b)(a^2+ab+b^2)$.

Puisque 1 commute avec tous les éléments de A, on a toujours la factorisation :

$$\forall\, a \in A,\ \forall\, n \in \mathbb{N}^*,\ 1 - a^n = (1-a)\sum_{k=0}^{n-1} a^k = (1-a)(1 + a + a^2 + \cdots + a^{n-1})$$

Proposition 11.3.3 (formule du binôme dans un anneau)
Soit $(A, +, \times)$ un anneau, et soit a, b deux éléments de A. On suppose que $ab = ba$.
Alors, pour tout entier naturel n, on a la « formule du binôme » : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k}$.

Remarque sur l'importance de l'hypothèse $ab = ba$

Dans les deux propositions précédentes, l'hypothèse selon laquelle a et b commutent est essentielle.

Évidemment, cela est automatiquement vérifié dans un anneau commutatif.

Si les deux éléments a et b ne commutent pas, le développement de $(a+b)^n$ est beaucoup plus compliqué.

On trouve par exemple : $\begin{cases}(a+b)^2 = a^2 + ab + ba + b^2 \\ (a+b)^3 = a^3 + a^2 b + aba + ab^2 + ba^2 + bab + b^2 a + b^3\end{cases}$

De même, si $ab \neq ba$, le produit $(a+b)(a-b)$ se développe en $a^2 - ab + ba - b^2$.

11.3.3 Structure de corps

Définition 11.3.2
Soit K un ensemble muni de deux lois $+$ et $\times$.
On dit que $(K, +, \times)$ est un *corps* si $(K, +, \times)$ est un anneau *commutatif* non réduit à $\{0\}$, et si tous les éléments non nuls de K sont inversibles pour le produit.

Exemples

$(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps, mais pas $(\mathbb{Z}, +, \times)$.

L'ensemble $\{r + s\sqrt{2}, (r,s) \in \mathbb{Q}^2\}$ est un corps, contenant strictement $\mathbb{Q}$, contenu strictement dans $\mathbb{R}$.