Structures algébriques

M. ECH-CHAMMAKHY Mohammed

Introduction

Un peu d'histoire

L'algèbre, dérivé du terme arabe AL-Jabr qui fut trouvé dans un ouvrage d'AL Khawarizmi, est une branche de Mathématiques qui est devenue progressivement l'étude abstraite des structures algébriques. De nos jours, on parle plutôt d'algèbre générale.
La notion de **groupe** est apparue dès la fin du 18e de manière parallèle dans différents domaines des mathématiques. En géométrie, l'ensemble des isométries de l'espace ou du plan a une structure de groupe, et on l'appelle **groupe orthogonal**, vous l'aborderez en détails en SPE. L'ensemble des permutations d'un ensemble fini est un groupe qui fut étudié par Cauchy et Cayley à la fin du 19e siècle, on le décortiquera davantage dans le chapitre sur les déterminants. L'ensemble des transformations qui, en relativité restreinte, permettent de changer de référentiel galiléen tout en préservant les lois de la physique et la vitesse de la lumière, forment un groupe appelé **groupe de Lorenz**. Sans omettre qu'en chimie, les symétries des molécules permettent de leur associer des groupes qui aident à comprendre mieux leurs propriétés.

Introduction

Dans ce chapitre

Dans ce chapitre, on présente le vocabulaire de base de la théorie des groupes, tout en étudiant deux autres structures, anneau et corps, qui sont également omniprésentes en Mathématiques.

Conventions

Conventions

- $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.
- n et p sont des entiers naturels non nuls.
- E est un ensemble non vide.
- E^E ou $F(E,E)$ désigne l'ensemble des fonctions de E vers E.

Loi de composition interne - Magma

Définition

- Soit M un ensemble. On appelle loi de composition interne **(LCI)** sur M toute application ϕ de $M \times M$ dans M.
- Le couple (M, ϕ) est alors appelé **un magma**.

Remarque

- Pour alléger les notations, On écrit plus simplement $\phi(a, b) = a_\phi b$ ou $\phi(a, b) = a \star b$ par exemple, ou encore $\varphi(a, b) = a.b$.
  Dans ce cas, on note tout simplement $(M, \star)$ ou $(M, .)$ pour désigner un magma.
- En général, les LCI sont notées additivement par $+$ ou multiplicativement par . , mais gardez en mémoire qu'il s'agit juste d'une notation.

Loi de composition interne-Magma

Exemples

- Les applications $(x, y) \overset{+}{\longmapsto} x + y$ et $(x, y) \overset{\times}{\longmapsto} xy$ sont des lois de composition interne sur $\mathbb{K}$.
  Ainsi $(\mathbb{K}, +)$ et $(\mathbb{K}, \times)$ sont des magmas.
- Les applications $(M, N) \overset{+}{\longmapsto} M + N$ et $(M, N) \overset{\times}{\longmapsto} MN$ sont des lois de composition interne sur $M_n(\mathbb{K})$.
  Ainsi $(M_n(\mathbb{K}), +)$ et $(M_n(\mathbb{K}), \times)$ sont des magmas.
- L'application $(f, g) \overset{\circ}{\longmapsto} f \circ g$ est une LCI sur E^E.
  Ainsi $(E^E, \circ)$ est un magma.

Partie stable par une LCI

Définition

Soient $(M, \star)$ un magma et $A \subset M$.
On dit que A est stable par $\star$ si : $\quad \forall a, a' \in A, \quad a \star a' \in A$.
Autrement dit, la restriction de $\star$ à $A \times A$, notée $\star\big|_{A\times A}$, est une loi de composition interne sur A.
Dans ce cas, $(A, \star\big|_{A\times A})$ est lui-même un magma.

Partie stable par une LCI

Exemples 1 : Dans $(\mathbb{C}, +)$ et $(\mathbb{C}, \times)$

- **Stabilité par addition :** $\mathbb{N}, \mathbb{Z}, \mathbb{D}, \mathbb{Q}, \mathbb{R}$ sont stables par addition.
- Est-ce que $\{0\}$ et $\mathbb{N}^*$ sont stable par addition ? qu'en est-il de $\mathbb{Z}^*$?
- **Stabilité par produit :** $\mathbb{N}, \mathbb{Z}, \mathbb{D}, \mathbb{Q}, \mathbb{R}$, $\mathbb{N}^*, \mathbb{Z}^*, \mathbb{D}^*, \mathbb{Q}^*, \mathbb{R}^*$ sont stables par produit.
- Est-ce que $\mathbb{R}_+, \mathbb{Q}_+$ sont stables par produit ? qu'en est-il de $\mathbb{R}_-$?

Partie stable par une LCI

Exemples 2 : Dans $(M_n(\mathbb{K}), +)$ et $(M_n(\mathbb{K}), \times)$

- **Stabilité par addition :** L'ensemble des matrices diagonales $D_n(\mathbb{K})$, L'ensemble des matrices triangulaires supérieures, L'ensemble des matrices triangulaires inférieures sont stables par addition.
- L'ensemble des matrices symétriques $S_n(\mathbb{K})$ et L'ensemble des matrices antisymétriques $A_n(\mathbb{K})$ sont stables par addition .
- L'ensemble des matrices inversibles $Gl_n(\mathbb{K})$ **n'est pas stable** par addition :
  Car $I_n \in Gl_n(\mathbb{K})$ et $-I_n \in Gl_n(\mathbb{K})$ mais $I_n - I_n = 0_n$ et $0_n \notin Gl_n(\mathbb{K})$.
- **Stabilité par produit :** L'ensemble des matrices inversibles $Gl_n(\mathbb{K})$, L'ensemble des matrices diagonales $D_n(\mathbb{K})$,L'ensemble des matrices triangulaires supérieures,L'ensemble des matrices triangulaires inférieures sont stables par produit.
- $S_n(\mathbb{K})$ et $A_n(\mathbb{K})$ sont-ils stables par produit ?

Commutativité-Associativité

Définition

Soit $(E, \star)$ un magma.On dit que $\star$ (resp $(E, \star)$) est :

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

Commutativité-Associativité

Proposition : La stabilité garde la commutativité et l'associativité.

Soient $(E, \star)$ un magma et A une partie de E stable par $\star$. Si $(E, \star)$ est commutatif (resp. associatif), alors $(A, \star)$ l'est aussi.

Commutativité-Associativité

Exemples

- Les magmas $(\mathbb{C}, +)$ et $(\mathbb{C}, \times)$ sont commutatifs et associatifs. Ainsi par stabilité, $+$ et $\times$ sont commutatives et associatives dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$, $\mathbb{R}$.
- Dans $(M_{n,p}(\mathbb{K}), +)$, $+$ est associative et commutative.
- Pour $n \geq 2$, Dans $(M_n(\mathbb{K}), \times)$, $\times$ est associative et **non commutative**.
- Pour le magma $(P(E), \cup)$, la loi $\cup$ est commutative et associative.
- Dans $(E^E, \circ)$, La LCI $\circ$ est associative mais pas commutative.

Commutativité-Associativité

Notations

- Quand la LCI est associative, on se permet d'enlever les parenthèses, ainsi on note $x \star y \star z$ au lieu de $(x \star y) \star z$ ou $x \star (y \star z)$. On définit alors pour tout entier naturel non nul n et tout élément x d'un magma associatif $(M, \star)$:
  1. En notation additive : $nx = x \star x \star \cdots \star x$
  2. En notation multiplicative : $x^n = x \star x \star \cdots \star x$
- Quand La LCI est associative et commutative, on définit pour tout entier naturel non nul n et pour tous $x_1, \ldots, x_n$ d'un magma associatif et commutatif $(M, \star)$:
  1. En notation additive : $\sum_{k=1}^{n} x_i = x_1 \star x_2 \star \cdots \star x_n$
  2. En notation multiplicative : $\prod_{k=1}^{n} x_i = x_1 \star x_2 \star \cdots \star x_n$

Distributivité

Définition

Soient M un ensemble et $\star$ et $\diamond$ deux LCI sur M. On dit que $\star$ est **distributive** sur $\diamond$ si :

$$\forall x, y, z \in M, \quad x\star(y\diamond z) = (x\star y)\diamond(x\star z) \quad \text{et} \quad (x\diamond y)\star z = (x\star z)\diamond(y\star z).$$

Distributivité

Remarque : La stabilité garde la distributivité

Soient M un ensemble et $\star$ et $\diamond$ deux LCI sur M. et $A \subset M$. On suppose que A est stable par $\star$ et $\diamond$.
Si $\star$ est distributive sur $\diamond$ dans M, alors elle l'est dans A.

Distributivité

Exemples

- Dans $\mathbb{K}$, $\times$ est distributive sur $+$, il en est de même pour $\mathbb{N}, \mathbb{Z}, \mathbb{D}, \mathbb{Q}$.
- Dans $M_n(\mathbb{K})$, $\times$ est distributive sur $+$.
- Dans l'ensemble des suites réelles $\mathbb{R}^{\mathbb{N}}$, $\times$ est distributive sur $+$.
- Dans $P(E)$, l'intersection est distributive sur l'union.

Élément neutre

Définition

Soient $(M, \star)$ un magma et $e \in M$. On dit que e est un **élément neutre** pour $\star$ dans M (ou de $(M, \star)$) si :

$$\forall x \in M, \quad x \star e = e \star x = x.$$

Élément neutre

Proposition : Unicité de l'élément neutre en cas d'existence

Soit $(M, \star)$ un magma.
Si $(M, \star)$ possède un élément neutre, celui-ci est **unique**.
On le note souvent :

- En notation additive : 0_M ou 0.
- En notation multiplicative : 1_M ou 1.

Preuve

Prenez "deux" éléments neutres, appliquez la définition et concluez qu'ils sont égaux.

Élément neutre

Exemples

- Les magmas $(\mathbb{C}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ et $(\mathbb{N}, +)$ admettent 0 pour élément neutre.
- 1 est l'élément neutre de $\times$ dans $(\mathbb{C}, \times)$, $(\mathbb{R}, \times)$, $(\mathbb{Q}, \times)$, $(\mathbb{Z}, \times)$ et $(\mathbb{N}, \times)$
- $(\mathbb{N}^*, +)$ admet-il un élément neutre ?
- Le magma $(\mathcal{M}_{n,p}(\mathbb{K}), +)$ admet la matrice nulle $O_{n,p}$ pour élément neutre.
- La matrice I_n est l'élément neutre de $(\mathcal{M}_n(\mathbb{K}), \times)$.
- Dans $(\mathcal{P}(E), \cup)$, La LCI admet $\emptyset$ pour élément neutre.
- L'application Id_E est l'élément neutre de la composition $\circ$ dans E^E.

Élément neutre

Remarque

La stabilité **ne garde pas** l'élément neutre :
Donnons nous B une partie stable par $\star$ dans un magma $(A, \star)$, si $\star$ admet un élément neutre dans A, rien ne garantit qu'elle admet un dans B, en outre, il se peut qu'elle a un autre élément neutre !
Prenez par exemple $(\mathbb{N}, +)$ et $(\mathbb{N}^*, +)$.

Symétrique/inverse

Définition

Soient $(M, \star)$ un magma possédant un élément neutre noté e, et $x \in M$. On dit que x est inversible ou symétrisable dans $(M, \star)$ (ou pour $\star$) s'il existe un élément $x' \in M$, appelé un *inverse/symétrique* de x, tel que :

$$x \star x' = x' \star x = e.$$

Symétrique/inverse

Proposition : Unicité de l'inverse en cas d'existence sous l'hypothèse de l'associativité

Si $(M, \star)$ est un magma **associatif** et si x est inversible dans M, alors x possède un unique inverse.
On le note x^{-1} en notation multiplicative et $-x$ en notation additive, dans ce cas on parle plutôt de l'*opposé* de x.

Symétrique/inverse

Remarque

La stabilité ne garde pas l'inversibilité, un exemple vaut mieux qu'un long discours :
Dans $(\mathbb{Z}, +)$, 1 est inversible d'inverse $-1 \in \mathbb{Z}$,
D'autre part, $\mathbb{N}$ est stable par $+$ dans $\mathbb{Z}$,
Pourtant 1 n'a pas d'inverse dans $(\mathbb{N}, +)$.

Symétrique/inverse

Exemples

- Le seul élément de $(\mathbb{N}, +)$ qui admet un opposé est 0.
- Dans $(\mathbb{C}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, et $(\mathbb{Z}, +)$ Tout élément possède un opposé.
- Les deux seuls éléments de $\mathbb{Z}^*$ muni de la multiplication qui admettent un inverse sont 1 et -1.
- Tout élément $\frac{p}{q} \in \mathbb{Q}^*$ admet un inverse donné par $\frac{q}{p}$.
- Dans $M_n(\mathbb{K})$ muni de l'addition, toute matrice a un opposé.
- Dans $(M_n(\mathbb{K}), \times)$, L'ensemble des matrices inversibles est noté (comme vous le savez) $GL_n(\mathbb{K})$, et la matrice nulle n'est pas inversible.
- Soit $f \in F(E, E)$, muni de la loi de composition. Alors f est inversible si et seulement si elle est bijective.
- Quels sont les inversibles pour l'union et l'intersection dans $P(E)$?

Symétrique/inverse

Théorème : Inversibilité dans un magma associatif

Soient $(M, \star)$ un magma associatif possédant un élément neutre noté e et $a, x, y, z \in M$.

1. **Inverse de l'inverse :** Si x est inversible dans M alors l'inverse x^{-1} de x est également inversible, et l'on a :
$$(x^{-1})^{-1} = x.$$
2. **Produit :** Si x et y sont inversibles, alors $x \star y$ l'est aussi, et l'inverse de $x \star y$ est donné par :
$$(x \star y)^{-1} = y^{-1} \star x^{-1}.$$
3. **Puissances négatives :** Pour tout $n \in \mathbb{N}$, si x est inversible, alors x^n l'est aussi, et :
$$(x^n)^{-1} = (x^{-1})^n.$$

Preuve

Prouvons les deux premiers points.

1. Supposons que x est inversible dans $(M, \star)$, et posons $y = x^{-1}$.
   Comme $y \star x = x \star y = e$, y est également inversible dans M. On a donc : $x = y^{-1} = \left(x^{-1}\right)^{-1}$.
2. Supposons que x et y sont inversibles dans $(M, \star)$. Alors, par associativité de $\star$, on a :
   $(x \star y) \star \left(y^{-1} \star x^{-1}\right) = x \star \left(y \star y^{-1}\right) \star x^{-1}$.
   Or, par définition de l'inverse : $y \star y^{-1} = e$ (e est l'élément neutre).
   Il vient donc : $(x \star y) \star \left(y^{-1} \star x^{-1}\right) = x \star e \star x^{-1} = x \star x^{-1} = e$.
   De même, on montre que : $\left(y^{-1} \star x^{-1}\right) \star (x \star y) = e$.
   Ainsi, $x \star y$ est inversible dans M, et son inverse est donné par : $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

Symétrique/inverse

Rédaction

Maintenant que vous avez appris de fixer les variables avant de les utiliser : Dans la preuve précédente, (re)fixer le magma M et/ou les éléments x, y, e n'est pas nécessaire, si ce n'est qu'une une **perte de temps** dans un DS ou un concours.
Lorsque l'énoncé fixe déjà une variable, il faut éviter de la refixer. En effet, cela peut entraîner des erreurs, comme oublier une condition imposée par l'énoncé sur cette même variable.

Symétrique/inverse

Proposition : Simplification par un élément inversible :

Soient $(M, \star)$ un magma associatif possédant un élément neutre noté e et $a, x, y \in M$.

- Si $a \star x = a \star y$ et si a est inversible, alors $x = y$.
- Si $x \star a = y \star a$ et si a est inversible, alors $x = y$.

Symétrique/inverse

Preuve

Montrons le premier point.

Supposons que $a \star x = a \star y$ et a est inversible, on a :

$$\begin{aligned}
x &= e \star x \quad \text{(par définition de l'élément neutre)} \\
&= (a^{-1} \star a) \star x \quad \text{(a est inversible)} \\
&= a^{-1} \star (a \star x) \quad \text{(par associativité)} \\
&= a^{-1} \star (a \star y) \quad \text{(par hypothèse)} \\
&= (a^{-1} \star a) \star y \quad \text{(par associativité)} \\
&= e \star y \\
&= y.
\end{aligned}$$

Bilan

Rédaction

Pour montrer que $\star$ est commutative :

1. Soit $(x, y) \in E^2$,
2. On montre que $x \star y = y \star x$,
3. Donc $\star$ est commutative.

Pour montrer que $\star$ est associative :

1. Soit $(x, y, z) \in E^3$,
2. On montre que $x \star (y \star z) = (x \star y) \star z$,
3. Donc $\star$ est associative.

Pour montrer que $e \in E$ est l'élément neutre de $\star$ dans E :

1. Soit $x \in E$,
2. On montre que $e \star x = x$ **et** $x \star e = x$,(sauf si $\star$ est commutative, une des deux suffit à condition de mentionner la commutativité)
3. Donc e est l'élément neutre de $(E, \star)$

Bilan

Rédaction

Pour montrer que $x \in E$ est inversible pour $\star$ dans E :
Premier cas : on connait déjà l'inverse $y \in E$

1. On vérifie $x \star y = e$
2. On vérifie $y \star x = e$ (sauf si $\star$ est commutative, une des deux suffit à condition de mentionner la commutativité)
3. On mentionne (vérifie) que $y \in E$.
4. On conclut que y est l'inverse de x dans E.

Deuxième cas : on cherche nous-même l'inverse
Dans ce cas, on résout les équations $x \star y = e$ et $y \star x = e$ d'inconnue y dans E (sauf si $\star$ est commutative, auquel cas une équation suffit). En cas d'existence, on cherche la solution qui vérifie les deux (unique si $\star$ est associative)

Exercice

Loi Produit

Soient $(M, \star)$ et $(M', \bullet)$ deux magmas. On définit une loi interne $\boxdot$ sur le produit $M \times M'$ en posant,
pour tous $(x, x') \in M \times M'$ et $(y, y') \in M \times M'$:
$(x, x') \boxdot (y, y') = (x \star y, x' \bullet y')$.

1. **Commutativité :** Prouver que Si $(M, \star)$ et $(M', \bullet)$ sont commutatifs, alors $\boxdot$ est commutative.
2. **Associativité :** Montrer que Si $(M, \star)$ et $(M', \bullet)$ sont associatifs, alors $\boxdot$ est associatif.
3. **Élément neutre :** Supposons que $(M, \star)$ et $(M', \bullet)$ admettent chacun un élément neutre notés respectivement 1_M et $1_{M'}$.
   Prouver que $\boxdot$ admet un élément neutre dans $M \times M'$ donné par :
   $1_{M \times M'} = (1_M, 1_{M'})$
4. Donner vous-même un énoncé sur l'inversibilité pour la loi Produit et démontrer le.

Définition

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

1. la loi $\star$ est associative ;
2. G (ou $(G, \star)$) possède un élément neutre (pour $\star$) ;
3. tout élément x de G est inversible **dans** G (pour $\star$).

Si de plus la loi $\star$ est commutative, on dit que le groupe est **abélien** (ou **commutatif**).
Le cardinal d'un groupe fini est appelé **l'ordre** de G.

Exemples

1. Les magmas $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens.
2. Les magmas $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes abéliens.
3. $(\mathbb{C}, \times)$ n'est pas un groupe, car 0 n'est pas inversible.
4. $(\mathbb{N}, +)$ n'est pas un groupe car 1 n'est pas inversible par exemple.
5. $(\mathbb{Z}^*, \times)$ est-il un groupe ?
6. $(M_n(\mathbb{K}), +)$ est un groupe abélien.
7. $(M_n(\mathbb{K}), \times)$ n'est pas un groupe. Pourquoi ?
8. Prouver que le groupe linéaire $(Gl_n(\mathbb{K}), \times)$ est un groupe. (non abélien si $n \geq 2$)
9. $(\mathbb{R}^{\mathbb{R}}, +)$ est un groupe abélien. Justifier-le.

Remarque

- En théorie, les groupes sont généralement notés multiplicativement, et il se peut qu'on ne précise pas la loi, en écrivant par exemple " soit G un groupe", dans ce cas on écrit xx' pour désigner le "produit" de x et x'.
- Quand on parle des groupes $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, cela sous entend qu'on parle de la loi $+$, et lorsqu'on parle de $\mathbb{Q}^*$, $\mathbb{R}^*$ ou $\mathbb{C}^*$, il s'agit de la loi $\times$
- On dira tout simplement $M_n(\mathbb{K})$ pour désigner $(M_n(\mathbb{K}), +)$, et $Gl_n(\mathbb{K})$ pour désigner $(Gl_n(\mathbb{K}), \times)$.

Règles de calcul dans un groupe

Propriétés

Soit G un groupe. Les propriétés suivantes se déduisent des paragraphes précédents.

- L'élément neutre est unique.
- Tout élément possède un unique inverse.
- Pour tout élément x de G, on a $(x^{-1})^{-1} = x$.
- **Règle de simplification** :

$$\forall (a, x, y) \in G^3 : \quad ax = ay \Rightarrow x = y \quad \text{et} \quad xa = ya \Rightarrow x = y.$$

- Soit $(a, b) \in G^2$. L'équation $ax = b$ possède une unique solution :

$$x = a^{-1}b.$$

- $\forall (x, y) \in G^2$, $(xy)^{-1} = y^{-1}x^{-1}$.

Règles de calcul dans un groupe

Propriétés : Puissances dans un groupe

Soit $(G, \cdot)$ un groupe et $a \in G$. On définit la famille $(a^n)_{n\in\mathbb{Z}}$ par les relations suivantes :

- **Initialisation :** $a^0 = 1_G$ (ou en notation additive $0a = 0_G$) ;
- **Itération :** pour tout $n \in \mathbb{N}$, $a^{n+1} = a \cdot a^n$ (pour $n \in \mathbb{N}^*$, $a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ fois}}$) ; (ou en notation additive $(n+1)a = a + na$)
- **Symétrique :** pour tout $n \in \mathbb{Z}$ avec $n < 0$, $a^n = (a^{-n})^{-1}$ (ou en notation additive $na = -(-na)$)

On dispose ainsi des formules suivantes qui se démontrent aisément par récurrence :

$$\forall n, m \in \mathbb{Z}, \quad a^n \cdot a^m = a^{n+m},$$

$$\forall n, m \in \mathbb{Z}, \quad (a^n)^m = a^{n\cdot m}.$$

Définition : Groupe symétrique

Soit E un ensemble non vide. On appelle **permutation** de E toute bijection de E sur E et **groupe symétrique** de E l'ensemble S_E des permutations de E.
Si $E = [[1, n]]$, On note S_E par S_n au lieu de $S_{[[1,n]]}$, on rappelle que l'ordre de S_n est $n!$.

Construction de groupes

Théorème : le Groupe symétrique est un groupe

Soit E un ensemble non vide. Le magma $(S_E, \circ)$, où $\circ$ désigne la composition des applications, est un groupe (en général non abélien)

Preuve

- $\circ$ est une loi de composition interne dans S_E : Pour tout $(f, g) \in (S_E)^2$, $f \circ g$ et $g \circ f$ sont encore des bijections sur E, ainsi S_E est stable par $\circ$ dans E^E
- Puisque$\circ$ est associative E^E ; et $(S_E, \circ)$ est stable dans $(E^E, \circ)$, alors $\circ$ est associative dans S_E.
- S_E possède un élément neutre Id_E.
- Toute permutation f de S_E possède un inverse dans S_E : son application réciproque f^{-1}, qui est bien une bijection de E vers E.

Construction de groupes

Définition-Théorème : Groupe produit

Soient $G_1, \ldots, G_n$ des groupes. Muni de la loi produit définie dans la page 32, $G_1 \times \cdots \times G_n$ est un groupe appelé **le groupe produit** de $G_1, \ldots, G_n$.

Preuve

Il suffit d'écrire.

Sous-groupes

Définition : Sous-groupe

Soient G un groupe et H une partie de G stable par produit. On dit que H est un sous-groupe de G si H est un groupe pour la loi de G.

Sous-groupes

Théorème : Caractérisation des sous-groupes

Soient G un groupe et H une partie de G. Les assertions suivantes sont équivalentes :

(i) H est un sous-groupe de G.

(ii) $\begin{cases} 1_G \in H, \\ H \text{ est stable par produit-inverse : } \forall h, h' \in H,\ h^{-1}h' \in H. \end{cases}$

(iii) $\begin{cases} 1_G \in H, \\ H \text{ est stable par produit : } \forall h, h' \in H,\ hh' \in H, \\ H \text{ est stable par inverse : } \forall h \in H,\ h^{-1} \in H. \end{cases}$

Preuve

On va prouver seulement l'équivalence entre (i) et (ii), mais implicitement on va passer par (iii).
$(i) \Rightarrow (ii)$: Supposons que H est un sous-groupe de G.

1. Prouvons que $1_H = 1_G$.
   D'une part $1_H 1_G = 1_H$ puisque 1_G est l'élément neutre de G.
   D'autre part $1_H 1_H = 1_H$ vu que 1_H est le neutre de H, ainsi $1_H 1_G = 1_H 1_H$.
   Or, en simplifiant par 1_H car G est un groupe, on déduit que $1_G = 1_H \in H$.
   Conclusion : $1_G \in H$.

2. Prouvons le deuxième point sur la stabilité par produit-inverse.
   Pour ceci on montrera en premier lieu la stabilité par inverse.
   Soit $h \in H$. Notons h' l'inverse de h dans H pour le distinguer de l'inverse h^{-1} de h dans G.
   Ainsi, $h^{-1} = h^{-1}1_G = h^{-1}1_H = h^{-1}(hh') = (h^{-1}h)h' = 1_G h' = h' \in H$.
   Conclusion : $h^{-1} \in H$ **et** H **et stable par inverse**

Preuve

Concluons :
Puisque H est un sous-groupe de G, H est stable par produit par définition et on vient de prouver que $1_G \in H$ et H est stable par passage à l'inverse.
Ainsi, pour tout $h, h' \in H$, $h^{-1} \in H$ par stabilité par inverse,
puis par stabilité par produit, on déduit que $\forall h, h' \in H, \quad h^{-1}h' \in H$. **CQFD**
$(ii) \Rightarrow (i)$: Réciproquement, supposons que $1_G \in H$ et que :
$\forall h, h' \in H, \quad h^{-1}h' \in H \quad (*)$.

- Comme $1_G \in H$: $\forall h \in H, h^{-1} = h^{-1}1_G \in H$ d'après (*), ainsi H est stable par inverse.
  D'autre part, d'après (*) : $\forall h, h' \in H, hh' = (h^{-1})^{-1}h' \in H$, d'où la stabilité par produit.
- Puisque H est stable par produit, il est associatif. $1_G \in H$, donc H admet un élément neutre. Et finalement, Tout élément dans H est inversible dans H, car celui-ci est stable par inverse.

Conclusion : H est un sous-groupe de G.

Sous-groupes

Remarque

En notation additive, le théorème précédent devient : Soient G un groupe et H une partie de G. Les assertions suivantes sont équivalentes :

(i) H est un sous-groupe de G.

(ii) $\begin{cases} 0_G \in H, \\ H \text{ est stable par différence : } \forall h, h' \in H,\ h - h' \in H. \end{cases}$

(iii) $\begin{cases} 0_G \in H, \\ H \text{ est stable par addition : } \forall h, h' \in H,\ h + h' \in H, \\ H \text{ est stable par opposé : } \forall h \in H,\ -h \in H. \end{cases}$

Sous-groupes

Exemples

1. $\mathbb{Z}$, $\mathbb{D}$ et $\mathbb{Q}$ sont des sous-groupes de $\mathbb{R}$ pour l'addition.
2. $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ pour l'addition.
3. $\mathbb{Q}^*$ et $\mathbb{R}^*$ sont des sous groupes de $(\mathbb{C}^*, \times)$.
4. L'ensemble des bijections croissantes est un sous-groupe du groupe des bijections de $\mathbb{R}$ dans $\mathbb{R}$.
5. $M_n(\mathbb{Q})$ est un sous-groupe de $M_n(\mathbb{R})$ pour l'addition.
6. $S_n(\mathbb{R})$ et $A_n(\mathbb{R})$ sont des sous-groupes de $M_n(\mathbb{R})$.
7. Pour tout groupe G, G lui-même et $\{1_G\}$ sont deux sous-groupes de G. Un sous-groupe de G distinct de G et 1_G s'appelle un **sous-groupe propre** de G.

Sous-groupes

Remarque

Afin de prouver qu'un magma est un groupe, on n'utilise **jamais** la définition.
On montre en effet que c'est un sous-groupe d'un groupe connu, et c'est la caractérisation qui doit devenir votre 'best friend'.

Exemples

On rappelle que $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\} = \{z \in \mathbb{C} \mid \exists \theta \in \mathbb{R} : z = e^{i\theta}\}$
Prouvons que $(\mathbb{U}, \times)$ est un groupe, pour ceci, il suffit de prouver que c'est un sous-groupe de $\mathbb{C}^*$:

1. Déjà $\mathbb{U}$ est inclus dans $\mathbb{C}^*$. $(|0| = 0)$
2. Comme $|1| = 1$, il est clair que $1 \in \mathbb{U}$.
3. Soient $x, y \in \mathbb{U}$. On a $\left|xy^{-1}\right| = |x| \cdot \left|y^{-1}\right| = |x| \cdot \frac{1}{|y|} = 1 \times \frac{1}{1} = 1$, donc $xy^{-1} \in \mathbb{U}$.

Conclusion : $\mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*, \times)$ et $(\mathbb{U}, \times)$ admet par conséquent une structure de groupe.

Sous-groupes

Exercice

1. On rappelle que $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$.
   Prouver que c'est un sous-groupe de $\mathbb{C}^*$. Rappeler son ordre.
2. Soit G un groupe. Posons $Z(G) = \{h \in G \mid \forall g \in G, \quad gh = hg\}$
   Montrer que $Z(G)$ est un sous-groupe **abélien** de G.
   $Z(G)$ s'appelle **le centre ou le commutateur** de G, c'est la partie des éléments de G qui commutent avec tous les autres éléments de G.
3. Soient E un ensemble non vide et $x \in E$.
   Démontrer que $\text{Stab}(x) = \{\sigma \in S_E \mid \sigma(x) = x\}$ est un sous-groupe de S_E.
   La notation Stab provient du terme **Stabilisateur**, pour dire tout simplement que c'est l'ensemble des permutations σ de S_E qui stabilisent x, i.e. dont x est un point fixe.

Sous-groupes

Théorème : Toute intersection de sous-groupes est un sous-groupe

Soient G un groupe, I un ensemble non vide et $(H_i)_{i\in I}$ une famille de sous-groupes de G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

On rappelle que $\bigcap_{i\in I} H_i = \{x \mid \forall i \in I,\ x \in H_i\}$

Preuve

Posons $K = \bigcap_{i \in I} H_i$.

1. Déjà $K \subset G$.
2. pour tout $i \in I$, puisque H_i est un sous-groupe de G, H_i contient 1_G, donc $1_G \in K$.
3. soient $x, x' \in K$. Pour tout $i \in I$, H_i contient x et x', donc aussi $x^{-1}x'$ en tant que sous-groupe de G. Par conséquent, $x^{-1}x' \in K$.

Conclusion : $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

Morphisme de groupes

Définition

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

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

On dit de plus que f est un :

- **endomorphisme de groupe** lorsque $G_1 = G_2$,
- **isomorphisme de groupes** lorsque f est bijective, auquel cas G_1 et G_2 sont dits isomorphes.
- **automorphisme de groupe** lorsque f est à la fois un endomorphisme et un isomorphisme de groupes.

Morphisme de groupes

Remarque

1. La précision dans morphisme **de groupes** n'est pas superflue ; quand il y aura plus de deux structures sur G, on aura besoin de savoir de quel type de morphisme on parle.
   Cependant, Dans la suite, jusqu'à la partie sur les anneaux, on va omettre cette précision, et on désigne par "morphisme" un morphisme de groupes.
2. La notion d'isomorphisme est fondamentale en Mathématiques. Un isomorphisme de groupes permet de transmettre les propriétés algébriques de l'un à l'autre, en particulier, quand on a un groupe dont l'étude est simple, on la privilégiera et conclura quant à l'autre par isomorphisme.
   Dans cette optique, on cherche souvent à établir l'existence d'isomorphisme avec des groupes connus. Il s'agit d'un problème de classification : on dispose déjà d'une classification de groupes abéliens finis, et de quelques autres groupes, toutefois ; cela reste une problématique qui occupe à l'heure actuelle de nombreux mathématiciens.

Morphisme de groupes

Exemples

- Puisque pour tous $x, y \in \mathbb{R}_+^*$, $\ln(xy) = \ln(x) + \ln(y)$, alors la fonction ln est un isomorphisme de groupes de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$.
- La fonction exp est un isomorphisme de groupes entre $\mathbb{R}$ et $\mathbb{R}_+^*$.
- $z \mapsto |z|$ est un endomorphisme de groupe de $\mathbb{C}^*$
- Soit a un élément d'un groupe G. L'application $k \mapsto a^k$ est un morphisme de groupes de $(\mathbb{Z}, +)$ vers $(G, \cdot)$.
- l'application trace $M \mapsto tr(M)$ est un morphisme de groupes de $M_n(\mathbb{K})$ vers $\mathbb{K}$.
- Soient G un groupe commutatif et $n \in \mathbb{Z}$. L'application $x \mapsto x^n$ est un endomorphisme de groupe de G, car pour tous $x, y \in G$, on a $(x \cdot y)^n = x^n \cdot y^n$ par commutativité.
- Pour tout $\alpha \in \mathbb{R}^*$, la fonction puissance $x \mapsto x^\alpha$ est un automorphisme de groupe de $\mathbb{R}_+^*$.

Morphisme de groupes

Propriétés

- **Composition** : Soient G, G' et G'' trois groupes et $f : G \longrightarrow G'$ et $g : G' \longrightarrow G''$ deux morphismes de groupes. Alors $g \circ f$ est un morphisme de groupes de G dans G''.
- **Éléments neutres et inverses :** Soient G et G' deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes. Alors $f(1_G) = 1_{G'}$ et pour tout $x \in G$: $\quad f\left(x^{-1}\right) = f(x)^{-1}$.
- **Images directe et réciproque d'un sous-groupe :** Soient G et G' deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes. Pour tout sous-groupe H de G, $f(H)$ est un sous-groupe de G', et pour tout sous-groupe H' de G', $f^{-1}(H')$ en est un de G.

Preuve

Montrons les deux premières propriétés.

- Soient $x, y \in G$: $g \circ f(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = g \circ f(x) g \circ f(y)$.
- On a $f(1_G) f(1_G) = f(1_G 1_G) = f(1_G) = f(1_G) 1_{G'}$, ainsi en simplifiant par $f(1_G)$, on obtient que $f(1_G) = 1_{G'}$.
  D'autre part, soit $x \in G$,
  on a $f\left(x^{-1}\right) f(x) = f\left(x^{-1}x\right) = f(1_G) = 1_{G'}$,
  d'où $f\left(x^{-1}\right) = f(x)^{-1}$.

Image et noyau d'un morphisme de groupes

Définition

Soient G et G' deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes.

- **Image :** On rappelle que $f(G) = \{y \in G' \mid \exists x \in G,\ f(x) = y\}$
  $f(G)$ s'appelle l'image de f et on le note $\operatorname{Im} f$.
- **Noyau** On rappelle que $f^{-1}(\{1_{G'}\}) = \{x \in G \mid \quad f(x) = 1_{G'}\}$.
  $f^{-1}(\{1_{G'}\})$ s'appelle le noyau de f, et on le note $\operatorname{Ker} f$.

Image et noyau d'un morphisme de groupes

Propriétés

Soient G et G' deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes.

- $\mathrm{Im}\, f$ est un sous-groupe de G'
- $\mathrm{Ker}\, f$ est un sous-groupe de G.
- f est surjectif si et seulement si $\mathrm{Im}\, f = G'$.
- f est injectif sur G si et seulement si $\mathrm{Ker}\, f = \{1_G\}$.

Image et noyau d'un morphisme de groupes

Preuve

Les deux premiers points se déduisent des propriétés sur les morphismes de groupes, le troisième point est par définition de la surjectivité.
Il ne reste à montrer donc que le dernier point sur l'injectivité.

- Supposons que f est injectif, alors pour tout $x \in \operatorname{Ker} f$: $\quad f(x) = 1_{G'} = f(1_G), \quad$ donc $x = 1_G$ par injectivité.
  Conclusion : $\operatorname{Ker} f \subset \{1_G\}$, mais $1_G \in \operatorname{Ker} f$, d'où l'égalité :
  $\operatorname{Ker} f = \{1_G\}$
- Réciproquement, supposons que $\operatorname{Ker} f = \{1_G\}$ et montrons que f est injectif. Soient $x, x' \in G$. Si $f(x) = f(x')$, alors
  $f\left(x^{-1}x'\right) = f(x)^{-1}f(x') = f(x)^{-1}f(x) = 1_{G'}$, donc
  $x^{-1}x' \in \operatorname{Ker} f = \{1_G\}$, Ainsi, $x = x'$, d'où l'injectivité de f.

Image et noyau d'un morphisme de groupes

Remarque

Prouver l'injectivité avec la méthode classique est quasiment interdit pour les **morphismes** de groupes, il faudra dorénavant montrer que $\operatorname{Ker} f = \{1_G\}$.

Isomorphisme de groupes

Propriétés

- **Composition :** La composée de deux isomorphismes de groupes est un isomorphisme de groupes.
- **Réciproque :** Soient G et G' deux groupes et $f : G \longrightarrow G'$ un isomorphisme de groupes de G sur G'. Alors f^{-1} est un isomorphisme de groupes de G' sur G.

Isomorphisme de groupes

Définition-Théorème : L'ensemble des automorphismes d'un groupe est un groupe pour la composition

Si G est un groupe, on note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. $(\mathrm{Aut}(G), \circ)$ est un groupe, et c'est un sous-groupe du groupe symétrique S_G.

Définition

On appelle anneau tout triplet $(A, +, \times)$ constitué d'un ensemble A et de deux lois internes $+$ et $\times$ sur A tels que :

- $(A, +)$ est un groupe commutatif dont l'élément neutre est noté 0_A ou 0 ,
- $(A, \times)$ est un magma associatif avec un élément neutre noté 1_A ou 1 ,
- la multiplication $\times$ est distributive par rapport à l'addition $+$.

Si le magma $(A, \times)$ est commutatif, on dit que l'anneau $(A, +, \times)$ est commutatif.
Les inversibles de A sont ses inversibles au sens de la multiplication.

Anneaux

Exemples

- Les triplets $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ ou tout simplement $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, et $\mathbb{C}$ sont des anneaux commutatifs. Ce n'est pas le cas de $(\mathbb{N}, +, \times)$.
- Pour $n \geq 2$, $M_n(\mathbb{K})$ est un anneau non commutatif.
- Si E est un ensemble, l'ensemble $F(E, \mathbb{R})$ des applications définies sur E et à valeurs dans $\mathbb{R}$, muni de l'addition et du produit des fonctions, est un anneau commutatif.
- L'ensemble des fonctions polynômiales de $\mathbb{R}$ dans $\mathbb{R}$, muni de l'addition et du produit des fonctions, est un anneau commutatif.
- L'ensemble des suites réelles (ou complexes) muni de l'addition et de la multiplication des suites, est un anneau commutatif.
- Le triplet $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif d'éléments neutres $\overline{0}$ pour $+$ et $\overline{1}$ pour $\times$.

Notations

On considère un anneau $(A, +, \times)$. Soit un élément $a \in A$ et un entier $n \in \mathbb{N}$. On note

$$na = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ fois}} & \text{si } n \neq 0, \\ 0 & \text{si } n = 0. \end{cases}$$

$$(-n)a = n(-a) = (-a) = \underbrace{(-a) + \cdots + (-a)}_{n \text{ fois}}$$

$$a^n = \begin{cases} \underbrace{a \times \cdots \times a}_{n \text{ fois}} & \text{si } n \neq 0, \\ 1 & \text{si } n = 0. \end{cases}$$

a^{-n} n'a de sens que si a est inversible pour $\times$. On a alors $a^{-n} = (a^{-1})^n$.

Propriétés : Règles de calcul dans un anneau

Soient A un anneau et $a, b \in A$.

1. $a \times 0_A = 0_A \times a = 0_A$.
2. Pour tout $n \in \mathbb{Z}$: $n(ab) = (na)b = a(nb)$.
   En particulier : $-(ab) = (-a)b = a(-b)$.
3. $(-a)(-b) = ab$. En particulier : $(-1_A)^2 = 1_A$.
4. Pour tout $n \in \mathbb{N}$, si a et b **commutent**, i.e. si $ab = ba$:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \quad \text{(Formule du binôme)}$$

et

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

Preuve

Prouvons les deux premiers points.

1. Puisque $a \times 0_A + a \times 0_A = a \times (0_A + 0_A) = a \times 0_A$, alors en simplifiant par $a \times 0_A$ dans le groupe $(A, +)$: $a \times 0_A = 0_A$. On montre de même, $0_A \times a = 0_A$.
2. Soit $n \in \mathbb{N}$.
   On a $n(ab) = ab + \ldots + ab = a(b + \ldots + b) = a(nb)$ par distributivité de $\times$ sur $+$.
   Pour $n = -1$, $ab + a(-b) = a(b - b) = a \times 0_A = 0_A$
   D'où, $-(ab) = a(-b)$.
   Soit n un entier naturel négatif, alors $-n \in \mathbb{N}$, ainsi d'après ce qu'on vient de prouver, on déduit que :
   $n(ab) = (-n)(-(ab)) = (-n)((-a)b) = ((-n)(-a))b = (na)b$

Règles de calcul dans un anneau

Exercice

Soit un anneau $(A, +, \times)$. On dit qu'un élément $a \in A$ est **nilpotent** s'il existe un entier $n \in \mathbb{N}^*$ tel que $a^n = 0$.
Le plus petit entier n vérifiant $a^n = 0$ s'appelle **l'indice de nilpotence** de l'élément a.
Prouver que si a est nilpotent, alors $1 - a$ est inversible dans A et donner son inverse.

Anneau intègre

Définition

Soit un anneau $(A, +, \times)$. On dit que cet anneau est intègre si et seulement si :

1. $A \neq \{0\}$;
2. $\forall (x, y) \in A^2,\ xy = 0 \implies x = 0$ ou $y = 0$.

Anneau intègre

Exemples

1. Les anneaux $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ et $\mathbb{Z}$ sont intègres
2. L'anneau $M_n(\mathbb{K})$ n'est pas intègre, car le produit de deux matrices non nulles peut être nul. (Essayez d'en donner un exemple !)
3. Soient $A_1, \ldots, A_n$ des anneaux. Muni de sa loi produit, $A_1 \times \ldots \times A_n$ est un anneau appelé l'anneau produit de $A_1, \ldots, A_n$.
   L'anneau produit $\mathbb{Z}^2$ est-il intègre ?
4. L'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ n'est pas intègre. Justifier-le.

Anneau intègre

Remarque

Dans un anneau intègre, on peut « simplifier » à gauche et à droite :
Si $(a, x, y) \in A^3$, avec $ax = ay$, et si $a \neq 0$, alors $x = y$, que a soit inversible ou non.
Cette propriété est généralement fausse dans un anneau quelconque !

Sous-Anneaux

Définition

Soient A un anneau et B une partie de A stable par addition et produit. On dit que B est un **sous-anneau** de A si $1_A \in B$ et si B est un anneau pour les lois de A.

Théorème : Caractérisation des sous-anneaux

Soient A un anneau et B une partie de A. Les assertions suivantes sont équivalentes :

(i) B est un sous-anneau de A.

(ii)
$$\begin{cases} 1_A \in B. \\ B \text{ est stable par différence : } \forall b, b' \in B, \quad b - b' \in B. \\ B \text{ est stable par produit : } \forall b, b' \in B, \quad bb' \in B. \end{cases}$$

Preuve

La même que celle de la caractérisation des sous-groupes.

Sous-Anneaux

Exemples

- $\mathbb{Z}$ et $\mathbb{Q}$ sont des sous-anneaux de $\mathbb{R}$.
- $M_n(\mathbb{Z})$ est un sous-anneau de $M_n(\mathbb{R})$.
- Pour tout anneau A, A est un sous-anneau de A.
- $\mathcal{C}(\mathbb{R}, \mathbb{R})$, l'ensemble des fonctions continues de $\mathbb{R}$ vers $\mathbb{R}$ est un sous-anneau de $\mathbb{R}^{\mathbb{R}}$.
- L'anneau des suites réelles bornées est un sous-anneau de l'anneau des suites réelles.

Exercice

Prouver que L'ensemble des entiers de Gauss défini par $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$.

Groupe des inversibles

Théorème

Soit A un anneau. L'ensemble des inversibles de A est un groupe pour la multiplication.
On le note $\mathrm{U}(A)$ ou $A^\times$, il s'appelle également **groupe des unités de** A.

Preuve

Cette fois, malheureusement on ne peut pas appliquer la caractérisation des sous-groupes, vu qu'on ne connait pas un groupe contenant $A^\times$.
On vérifie que c'est une partie stable par produit, donc c'est un magma, l'associativité se déduit par stabilité, 1_A est son élément neutre vu que celui-ci est en particulier inversible dans A et donc il est dans $A^\times$, et par définition, l'inverse d'un élément de A est dans $A^\times$.

Groupe des inversibles

Exemples

- $\mathrm{U}(\mathbb{Z}) = \{-1, 1\}$
- $\mathrm{U}(\mathbb{Q}) = \mathbb{Q}^*$
- $\mathrm{U}(\mathbb{R}) = \mathbb{R}^*$
- $\mathrm{U}\left(M_n(\mathbb{K})\right) = \mathrm{GL}_n(\mathbb{K})$.
- Quels sont les inversibles de l'anneau des entiers de Gauss ?

Morphisme d'anneaux

Définition

Soient A et A' deux anneaux. On appelle morphisme d'anneaux de A dans A' toute application $f : A \longrightarrow A'$ telle que :

$$\begin{cases} f(1_A) = 1_{A'}, \\ \forall x, y \in A,\ f(x+y) = f(x) + f(y), \\ \forall x, y \in A,\ f(xy) = f(x)f(y). \end{cases}$$

Remarque

On définit comme dans le cas des groupes les notions d'endomorphisme d'anneau, isomorphisme d'anneaux, et automorphisme d'anneau.

Morphisme d'anneaux

Exemples

1. L'application $x \mapsto x$ est un automorphisme d'anneau de $\mathbb{R}$.
2. L'application $z \mapsto \bar{z}$ est un automorphisme d'anneau de $\mathbb{C}$.
3. Soit $P \in \mathrm{GL}_n(\mathbb{K})$. L'application $M \mapsto PMP^{-1}$ est un automorphisme d'anneau de $\mathrm{M}_n(\mathbb{K})$.
4. L'application $x \longmapsto \bar{x}$ est un morphisme surjectif d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$. Elle s'appelle **la surjection canonique** de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$

Morphisme d'anneaux

Propriétés

Les propriétés suivantes se démontrent comme pour les groupes.
Soient A et A' deux anneaux et $f : A \longrightarrow A'$ un morphisme d'anneaux.

- **Loi** $+$: f est un morphisme de groupes additifs de A dans A'.
  Ainsi, $f(0_A) = 0_{A'}$ et pour tout $x \in A$: $\quad f(-x) = -f(x)$.
- **Loi** $\times$: $f_{|_{U(A)}}$ est un morphisme de groupes multiplicatifs de $\mathrm{U}(A)$ dans $\mathrm{U}(A')$.
  Ainsi, pour tout $x \in \mathrm{U}(A)$: $\quad f\left(x^{-1}\right) = f(x)^{-1}$.
- Pour tout $a \in A$, $p \in \mathbb{N}$ et $n \in \mathbb{Z}$:
  1. $f(na) = nf(a)$,
  2. $f(a^p) = f(a)^p$
- L'image directe par f de tout sous-anneau de A est un sous-anneau de A'.
- L'image réciproque selon f de tout sous-anneau de A' est un sous-anneau de A.

Morphisme d'anneaux

Propriétés

- **Image :** L'image de f est notée $\operatorname{Im} f$ et c'est un sous-anneau de A'. En outre, f est surjectif de A sur A' si et seulement $\operatorname{Im} f = A'$.
- **Noyau :** On appelle noyau de f son noyau en tant que morphisme de groupes additifs de A :
  $\operatorname{Ker} f = f^{-1}(\{0_{A'}\}) = \{x \in A \mid \quad f(x) = 0_{A'}\}$.
  En outre, f est injectif sur A si et seulement si $\operatorname{Ker} f = \{0_A\}$.
- **Composition :** La composée de deux morphismes d'anneaux est un morphisme d'anneaux.
- **Isomorphismes :** La composée de deux isomorphismes d'anneaux est un isomorphisme d'anneaux et la réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.

Morphisme d'anneau

Remarque

- Ker f n'est pas en général un sous-anneau de A.
- On fait attention à la bonne définition du noyau d'un morphisme d'anneaux, on prend en effet l'élément neutre la structure additive et non pas multiplicative.

Corps

Définition

On appelle corps tout anneau commutatif non nul dans lequel tout élément non nul est inversible.

Corps

Exemples

- $\mathbb{C}, \mathbb{R}$ et $\mathbb{Q}$ sont des corps.
- $\mathbb{Z}$ n'est pas un corps, car ses seuls inversibles sont 1 et -1.
- $M_n(\mathbb{K})$ n'est pas un corps, pour $n \geq 2$.
- $\mathbb{Z}/3\mathbb{Z}$ est un corps mais $\mathbb{Z}/4\mathbb{Z}$ ne l'est pas ; la classe de 2 n'est pas inversible dans ce dernier.

Corps

Propriété

Tout corps est un anneau intègre

Preuve

Soient K un corps, $a, b \in K$.
Si $ab = 0_K$ avec $a \neq 0_K$, alors $b = 0_K$ après division par a (i.e après multiplication par son inverse).

Sous-corps

Définition

On appelle sous-corps d'un corps $(K, +, \times)$ toute partie L de K vérifiant :

1. L est un sous-anneau de $(K, +, \times)$;
2. $\forall x \in L, x \neq 0_K \implies x^{-1} \in L$.

Sous-corps

Exemples

- $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-corps de $\mathbb{C}$.
- Pour tout corps K, K est un sous-corps de K.
- Prouver que $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{R}$.

Morphisme de corps

Définition

Soit K et L deux corps et f une application de K dans L. On dit que f est un morphisme de corps si et seulement si c'est un morphisme d'anneaux.

Morphisme de corps

Propriétés

Soit $f : K \longrightarrow L$ un morphisme de corps.

1. Si K_0 est un sous-corps de K, alors $f(K_0)$ est un sous-corps de L.
2. Si L_0 est un sous-corps de L, alors $f^{-1}(L_0)$ est un sous-corps de K.

Morphisme de corps

Exercice

Prouver qu'un morphisme de corps est injectif.