Structures algébriques

ESEFA-Agadir

2019

Table des matières

Introduction

Ce document est un cours introductif aux structures algébriques. Il se place à un niveau première année universitaire.

Son esprit est l'identification quasi-complète : Algèbre est l'étude des « structures »de leurs modèles.
Ce document est extrait du web et j'ai choisi et adapté son niveau ainsi que son contenu aux étudiants de l'ecole ESEFA-Agadir nouvellement créée.
Un futur enseignant doit d'abord comprendre les structures fondamentales du savoir mathématique qu'il est appelé à enseigner. C'est dans cet ésprit que s'intègre cet enseignement. Le but étant de former des enseignants hautement qualifiés aussi bien au niveau pédagogique que cognitif.
Les remarques sont les bienvenues.

1 Lois de composition interne et jargon attaché

1.1 Définition

[Loi de Composition Interne]

On appelle loi de composition interne (lci) sur E toute application de $E \times E$ dans E.

La notion de loi de composition interne englobe dans une certaine mesure la notion intuitive d'« opérateur » sur les ensembles classiques.

Une lci sera la plupart du temps notée avec l'un des symboles suivants : $*, +, ., \times$ ... On n'utilisera pas la notation fonctionnelle, mais une notation infixe : au lieu de $*(x, y) = z$, on notera $x * y = z$.

Attention, le choix du symbole pour noter la loi est complètement arbitraire : il n'y a pas de différence théorique entre une loi notée additivement $(+)$, et une loi notée multiplicativement $(\times, ., *)$.

- $+$ est une lci sur $\mathbb{R}$.
- $\times$ est une lci sur $\mathbb{R}$.
- en revanche, $/$ n'est pas une lci sur $\mathbb{R}$, étant donné qu'elle n'est pas définie sur $\mathbb{R} \times \{0\}$. C'est en revanche une lci sur $\mathbb{R}^*$.
- soit E un ensemble. $\cup$ et $\cap$ sont des lci sur $\mathcal{P}(E)$.
- $+$ définie par $\forall (x, x', y, y')^4 \ \ (x, y) + (x', y') = (x + y, x' + y')$ est une lci sur ^{2}.
- $\times$ est une lci sur $\{0, 1\}$.

Dans le cas d'un ensemble fini, on peut écrire une loi sous la forme d'un tableau. Par exemple, pour le dernier exemple :

$\times$	0	1
0	0	0
1	0	1

[Magma]

On appelle magma tout couple $(E, *)$, où $*$ est une lci sur E.

Il s'agit donc simplement d'un ensemble E muni d'une lci $*$.

Il est difficile de dire grand-chose d'un tel ensemble si la loi n'a pas d'autre propriété, i.e. si elle ne *structure* pas plus l'ensemble (le terme de *magma* provient d'ailleurs du fait que le magma n'est pas structuré). On peut délaisser cette appellation devenue à nos jours caduc. En cours, nous avons parlé aussi du *monoide* (magma+élément neutre), mais ces petites structures sont abondonnés dans notre programme (marocain) à cause de leur insuffisanc et caducité.

1.2 Vocabulaire associé

Détaillons maintenant un certain nombre de propriétés que peuvent avoir des lci.

1.2.1 Associativité, comutativité

[Propriété des lci]
Considérons un magma $(E, *)$.

Associativité : $*$ est associative Ssi $\forall (x, y, z) \in E^3 \;\; (x * y) * z = x * (y * z)$.

Dans ce cas le parenthésage n'a pas d'importance, et on pourra noter $x * y * z = (x * y) * z = x * (y * z)$.

Commutativité : $*$ est commutative Ssi $\forall (x, y) \in E^2 \;\; x * y = y * x$.

En pratique, la plupart des lois que nous étudierons seront au moins associatives.

- $+$ est associative et commutative sur $\mathbb{N}$.
- $/$ sur $\mathbb{R}^*$ est n'est ni associative ni commutative : $(1/2)/2 \neq 1/(2/2)$ et $1/2 \neq 2/1$.
- $\cup$ et $\cap$ sont associatives et commutatives dans $\mathcal{P}(E)$

Si la loi est associative et commutative, cela signifie que l'on peut modifier arbitrairement l'ordre des éléments d'un produit : par exemple $x*y*z*t = z*y*t*x$. Ceci nous permet d'introduire la notation $\prod$:

Considérons une famille $(x_i)_{i \in I}$ d'éléments de E indexés par un ensemble fini $I = \{i_1, \dots i_n\}$. On note alors

$$\prod_{i \in I} x_i = x_{i_1} * \cdots * x_{i_n}$$

Si la loi est notée additivement, on écrira plutôt

$$\sum_{i \in I} x_i = x_{i_1} + \cdots + x_{i_n}$$

1.2.2 Elément neutre, inverse

[Neutre]
Soit $(E, *)$ un magma. On appelle élément neutre (ou simplement neutre) de $(E, *)$ tout élément $e \in E$ vérifiant :

$$\forall x \in E \;\; x * e = e * x = x$$

Attention, si le magma n'est pas commutatif, il faut vérifier que les multiplications par le neutre à droite **et** à gauche laissent tout $x \in E$ invariant.

Il y a unicité de l'élément neutre dans un magma.

Soit $(E, *)$ un magma. Soient e et e' des éléments neutres. Alors, comme e est neutre, $e * e' = e$. Mais e' est également neutre, et on a aussi $e * e' = e'$, d'où $e = e'$.

Mais il n'y a pas forcément existence d'un élément neutre...

- Dans $(\mathbb{Z}, +)$, 0 est l'élément neutre.
- Dans $(\mathbb{Z}, \times)$, 1 est l'élément neutre.
- Dans $(\mathcal{P}(E), \cap)$, E est l'élément neutre.
- Dans $(\mathcal{P}(E), \cup)$, $\emptyset$ est l'élément neutre.
- dans $(\mathbb{R}^*, /)$, il n'y a pas d'élément neutre (on pourrait cependant définir une notion de *neutre à droite*. 1 serait alors neutre à droite).

[Inverse]

Soit $(E, *)$ un magma admettant un élément neutre e. On appelle inverse de x tout élément y vérifiant :

$$x * y = y * x = e$$

Un élément qui admet un inverse est dit inversible.

De même que pour le neutre, en cas de non-commutativité, on doit vérifier deux égalités.

Il y a unicité de l'inverse dans un magma associatif.

Soit $(E, *)$ un magma associatif. Soient y et y' des inverses de x. On a alors $x * y' = e$. En composant à gauche par y, on obtient $y * (x * y') = y * e$. Par associativité et définition du neutre, on a donc $(y * x) * y' = y$ d'où $(e) * y' = y$ puis $y = y'$.

L'inverse x sera souvent noté x^{-1} si la loi est notée multiplicativement $., *$ ou $\times$, et $-x$ si elle est notée additivement.

- dans tout magma muni d'un neutre, le neutre est son propre inverse.
- dans $(\mathbb{Z}, +)$, tout élément x est inversible et admet pour inverse $-x$.
- dans $(\mathbb{R}, \times)$, tout élément x différent de 0 est inversible et a pour inverse $\frac{1}{x}$.
- dans $(\mathbb{Z}, \times)$, seul 1 et -1 sont inversibles, et ont pour inverse eux-mêmes.
- dans $(\mathcal{P}(E), \cap)$, l'inverse de A est A^C.
- dans $(\mathcal{P}(E), \cup)$, l'inverse de A est A^C.

Nous allons maintenant étudier des ensembles un peu plus structurés que les magmas.

2 Groupes

2.1 Définition, propriétés fondamentales

[Groupe]
On appelle groupe tout magma $(G, *)$ tel que
- G est non vide
- $*$ est associative
- $(G, *)$ admet un élément neutre
- tout élément est inversible

Si la loi est commutative, on parlera de plus de *groupe commutatif* ou *groupe abélien*.

On notera la plupart du temps G, H ou K plutôt que E pour un groupe.

En pratique, la loi sera parfois omise s'il n'y a pas d'ambiguïté : au lieu de $x * y$, on pourra noter xy.

- $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ sont des groupes.
- $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{Q}^*, \times)$ sont des groupes.
- $(\mathbb{Z}^*, \times)$ n'est pas un groupe : 2 n'est pas inversible (en fait, seuls 1 et -1 sont inversibles).
- $(\mathbb{R}, \times)$ n'est pas un groupe : 0 n'est pas inversible.
- $(\mathbb{N}, +)$ n'est pas un groupe : aucun élément différent de 0 n'est inversible.
- soit E un ensemble. Si on note $\mathfrak{S}(E)$ l'ensemble des bijections de E dans E, $(\mathfrak{S}(E), \mathrm{o})$ est un groupe (appelé groupe symétrique de E).
- l'ensemble des isométries (i.e. des applications qui préservent les distances) du plan est un groupe.
- $\{0, 1\}$ muni de la loi suivante

$+$	0	1
0	0	1
1	1	0

  est un groupe.

Les propriétés suivantes sont fondamentales pour travailler avec des groupes :

Soit $(G, *)$ un groupe. Alors
- il y a unicité du neutre e.

- il y a unicité de l'inverse.
- $\forall (x,y,z) \in G^3$, $x*y = x*z \Rightarrow y = z$ (simplification à gauche)
- $\forall (x,y,z) \in G^3$, $y*x = z*x \Rightarrow y = z$ (simplification à droite)
- $\forall (x,y) \in G^3$, $(x*y)^{-1} = y^{-1} * x^{-1}$ (inverse d'un produit)
- $\forall x \in G$, $(x^{-1})^{-1} = x$ (inverse de l'inverse)

Attention au changement de sens dans l'inverse du produit.

Les deux premiers points découlent des propriétés des magmas associatifs.

- Soient $(x,y,z) \in G^3$. Supposons $x*y = x*z$. Multiplions les deux membres de l'égalité par x^{-1} à gauche : $x^{-1}*(x*y) = x^{-1}*(x*z)$. Par associativité, on a $(x^{-1}*x)*y = (x^{-1}*x)*z$ puis par définition de l'inverse $e*y = e*z$, soit $y = z$.
- De même pour la simplification à droite.
- Soient x, y dans G. On vérifie simplement que $y^{-1}*x^{-1}$ est l'inverse de $x*y$:
  — $(x*y)*(y^{-1}*x^{-1}) \underset{asso}{=} x*(y*y^{-1})*x^{-1} \underset{inv}{=} x*e*x^{-1} \underset{neut}{=} x*x^{-1} \underset{inv}{=} e$
  — $(y^{-1}*x^{-1})*(x*y) \underset{asso}{=} x^{-1}*(y^{-1}*y)*x \underset{inv}{=} x^{-1}*e*x \underset{neut}{=} x^{-1}*x \underset{inv}{=} e$
- Soit x dans G. On a $x*x^{-1} = x^{-1}*x = e$ par définition. On en déduit sans trop de difficulté que $x^{-1}*x = x*x^{-1} = e$ ce qui signifie exactement que $x = (x^{-1})^{-1}$

On définit la loi $*$ sur $]-1,1[$ par $\forall (x,y) \in]-1,1[^2 \;\; (x*y) = \frac{x+y}{1+xy}$.
Montrer que $(]-1,1[, *)$ est un groupe commutatif.

La loi est interne : soient x et y dans $]-1,1[$.

- On a $x-1<0$ et $y<1$ d'où $x-1<y(x-1)$, soit $x+y<1+xy$
- On a $x+1>0$ et $y>-1$ d'où $-(x+1)>y(x+1)$, soit $x+y>-1-xy$

D'où $x*y \in]-1,1[$.

On montre ensuite que la loi est commutative, ce qui nous fera gagner un peu de temps pour les démonstrations concernant le neutre et l'inversibilité :

$\forall (x,y) \in]-1,1[^2 \;\; (x*y) = \frac{x+y}{1+xy} = \frac{x+y}{1+xy} = (y*x)$ par commutativité de l'addition et de la multiplication dans .

Passons à l'associativité.

$$\forall (x,y,z) \in]-1,1[^2 \;\; (x*y)*z = \frac{\frac{x+y}{1+xy} + z}{1 + z\frac{x+y}{1+xy}} = \frac{x+y+z+xyz}{1+xy+zx+zy}$$

cette expression est symétrique en x, y et z, on a donc bien $(x*y)*z = x*(y*z)$.

On vérifie alors que 0 est un neutre à gauche (et donc à droite par commutativité), puis que $x \in]-1,1[$ admet pour inverse $-x$.

2.1.1 Puissances dans un groupe

Soit $(G, .)$ un groupe, $n \in \mathbb{Z}$ et $a \in G$. On définit a^n
(puissance $n^{\text{ème}}$ de a) de la façon suivante :

$$\begin{cases} a^0 = e \\ a^n = a * a^{n-1} & \text{si } n > 0 \\ a^n = (a^{-n})^{-1} & \text{si } n < 0 \end{cases}$$

Une récurrence immédiate montre que pour tout $a \in G$ et pour tout $n < 0$

$$a^n = (a^{-n})^{-1} = (a^{-1})^{-n}$$

Pour n strictement positif, on a donc $a^n = \underbrace{a * \cdots * a}_{n \text{ fois}}$, et pour n strictement négatif, $a^n = \underbrace{a^{-1} * \cdots * a^{-1}}_{n \text{ fois}}$.

- $e^n = e$ pour tout $n \in \mathbb{Z}$.
- Si a et b commutent, $(ab)^n = a^n b^n$ pour tout $n \in \mathbb{Z}$.
- Si a et b ne commutent pas, on ne peut rien dire en général. Si $n > 0$, $(ab)^n = abababab \ldots$

Si la loi est notée additivement, on parlera plutôt de *multiple* de a, et on notera na au lieu de a^n.

Avec cette notation, on aura alors :

$$\begin{cases} 0a = e \\ na = a + (n-1)a & \text{si } n > 0 \\ na = -(-n)a & \text{si } n < 0 \end{cases}$$

Attention, na **n'est pas** le produit de n par a. a est un élément du groupe, alors que n est un entier. Il s'agit d'une *loi de composition externe*.

Les puissances dans les groupes ont les même propriétés que les puissances réelles que vous connaissez.

Soit $(G, *)$ un groupe, $a \in G$ et (p, q) in $\mathbb{Z}^2$. Alors,

- $a^p * a^q = a^{p+q}$
- $(a^p)^q = a^{pq}$

Montrons juste le premier point, nous verrons plus tard comment en déduire le second.

- Commençons par le cas où p et q sont positifs, et raisonnons par récurrence sur $n = p + q$.

Initialisation : Si $n = 0$, $p = q = 0$, et le résultat est immédiat.

Hérédité : Supponsons le résultat vrai pour n. Soient p et q dans $\mathbb{Z}$ tels que $p + q = n + 1$. Supposons par exemple $p \neq 0$.

On écrit

$$a^p * a^q = a * (a^{p-1} * a^q) = a * a^n = a * a^{n+1}$$

d'où le résultat.

- Le cas où p et q sont négatifs en découle immédiatement.
- Supposons $p > 0$ et $q < 0$. Si par exemple $|p| \geq |q|$, on écrit $p = -q + r$ avec $r \geq 0$.
  On a alors d'après le cas positif $a^p = a^{-q} * a^r$. En multipliant par a^q, on obtient : $a^p * a^q = a^q * a^{-q} * a^r$. Or a^{-q} est l'inverse de a^q. D'où $a^p * a^q = a^r = a^{p+q}$

2.2 Sous-groupe

[Sous-groupe]

Soit $(G, *)$ un groupe. On appelle sous-groupe de $(G, *)$ tout groupe de la forme $(H, *)$ où $H \subset G$.

Un sous-groupe est donc simplement un sous-ensemble qui est un groupe **pour la même loi** [1]. En particulier, $*$ doit être une loi interne sur H, i.e. H doit être stable par $* : \forall (x, y) \in H^2 \;\; x * y \in H$.

- Si $(G, *)$ un groupe, e son élément neutre. G et $\{e\}$ sont des sous-groupes de G, appelés *sous-groupes triviaux* de G.
- $(\mathbb{Z}, +)$ est un sous-groupe de $(, +)$, qui est lui-même un sous-groupe de $(, +)$.
- $(2\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$
- $(2\mathbb{Z} + 1, +)$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$: $+$ n'est pas une lci dessus.
- L'ensemble des rotations du plan est un sous-groupe du groupe des isométries du plan.

Soit $(G, *)$ un groupe d'élément neutre e. Soit $H \subset G$.
Si $(H, *)$ est un sous-groupe de $(G, *)$ alors

- $e \in H$ et est le neutre de H
- H est stable par produit
- H est stable par passage à l'inverse

- $(H, *)$ admet un neutre e'. On a alors $e' * e' = e'$. e' est inversible dans G, donc par simplification à droite par e'^{-1}, $e' = e$.

1. plus précisément pour la loi induite

- La stabilité par produit traduit simplement le fait que la loi est interne.
- Soit $h \in H$. Notons h' son inverse dans H. On a $h * h' = h' * h = e$. En regardant ces égalités dans G, on a donc par définition de l'inverse $h' = h^{-1}$.

On peut se démander si ces propriétés sont caractéristiques d'un sous-groupe. C'est bien le cas :

Soit $(G, *)$ un groupe d'élément neutre e. Soit $H \subset G$.
$(H, *)$ est un sous-groupe de $(G, *)$ Ssi
- $e \in H$ et est le neutre de H
- H est stable par produit
- H est stable par passage à l'inverse

Supposons que les trois propriétés soient vérifiées, et montrons que $(H, *)$ est un sous-groupe de $(G, *)$. Il suffit donc en fait de montrer que $(H, *)$ est un groupe.
- $*$ est une lci sur H par stabilité par produit.
- $e \in H$, donc H est non vide.
- $*$ est associative sur G donc a fortiori sur H.
- e est le neutre de G, i.e. $\forall g \in G \quad g * e = e * g = g$. En particulier, $\forall h \in H \quad h * e = e * h = h$. De plus $e \in H$, donc e est le neutre de $(H, *)$.
- Soit $h \in H$. h possède un inverse h^{-1} dans G. Mais par hypothèse, $h^{-1} \in H$ et $h * h^{-1} = h^{-1} * h = e$, et donc h est inversible dans h.

En pratique, on peut même compacter cette caractérisation :

Soit $(G, *)$ un groupe d'élément neutre e. Soit $H \subset G$.
$(H, *)$ est un sous-groupe de $(G, *)$
Ssi
- $e \in H$
- $\forall (x, y) \in H^2 \quad x * y^{-1} \in H \quad (1)$

La stabilité par produit et par passage à l'inverse implique trivialement (1).

Réciproquement, si on a (1), soit $x \in H$, alors $x^{-1} = e * x^{-1} \in H$, d'où la stabilité par inverse. Si $(x, y) \in H^2$, on a $y^{-1} \in H$, puis $x * y = x * (y^{-1})^{-1} \in H$ d'où la stabilité par produit.

En pratique, on utilisera l'une de ces caractérisations pour montrer qu'un ensemble est un sous-groupe.

En fait, elle est tellement pratique à manipuler que l'on l'utilisera même parfois pour montrer qu'un ensemble est un groupe : on essayera d'inclure cet ensemble dans un groupe plus grand, et on montrera simplement qu'il s'agit d'un sous-groupe.

Notons $\mathbb{U} = \{x \in \mathbb{C} \mid |x| = 1\}$. Montrons que $(\mathbb{U}, \times)$ est un groupe. $\mathbb{U}$ est inclus dans $\mathbb{C}$, donc nous allons montrer qu'il s'agit d'un sous groupe de $(\mathbb{C}, \times)$.

- On a clairement $1 \in \mathbb{U}$.
- Soit x et x' dans $\mathbb{U}$. On a $|xx'^{-1}| = \frac{|x|}{|x'|} = 1$ et $xx' \in \mathbb{U}$.
  Ce groupe est appelé *groupe unimodulaire*.

Pas besoin d'aller redémontrer l'associativité, l'existence d'un inverse, etc...

2.2.1 Exemple fondamental : les sous-groupes de $\mathbb{Z}$

Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les $(n\mathbb{Z}, +)$ où $n \in \mathbb{N}$.

- Soit $n \in \mathbb{N}$. Nous allons commencer par montrer que $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$ en utilisant 2.2. Soient a et b dans $n\mathbb{Z}$. Il existe a' et b' dans $\mathbb{Z}$ tels que $a = na'$ et $b = nb'$. On a alors $a - b = n(a' - b') \in n\mathbb{Z}$.
- Soit G un sous-groupe de $(\mathbb{Z}, +)$. Posons $G^+ = G \cap \mathbb{Z}^{+*}$. Si G^+ est vide, on voit facilement G est réduit à $\{0\}$: en effet, $G \cap \mathbb{Z}^{-*}$ est également vide, sans quoi on peut inverser un de ses éléments pour trouver un élément dans G^+. On a dans ce cas $G = 0\mathbb{Z}$.
  Sinon, posons $a = \min G^+$. Nous allons montrer que $G = a\mathbb{Z}$.

  $a\mathbb{Z} \subset G$ **:** on a $a \in G$ par définition. Par stabilité, nous avons aussi $a + a = 2a \in G$. Par récurrence, on montre que $na \in G$ pour tout $n \in \mathbb{N}^*$. Par ailleurs, par stabilité par passage à l'inverse, $(-n)a \in G$ pour tout $n \in \mathbb{N}^*$. Comme de plus $0 \in G$, on a bien $a\mathbb{Z} \subset G$.

  $G \subset a\mathbb{Z}$ **:** Soit $x \in G$. Effectuons la division euclidienne de x par a : $x = aq + r$, avec $0 \leq r < a$. a et x sont dans G, donc $r = x - aq$ également. La définition de a impose alors $r = 0$, i.e. $x \in a\mathbb{Z}$.

2.3 Morphismes de groupe

Un morphisme (du grec ancien morf'h) est une application respectant la structure d'un ensemble. Dans le cas des morphismes de groupe, on a la définition suivante :

[Morphisme de groupe]

Soient $(G, *)$ et $(G', *')$ deux groupes. On appelle morphisme de groupe de G dans G' toute application $\phi : G \mapsto G'$ telle que

$$\forall (x, y) \in G^2 \quad \phi(x * y) = \phi(x) *' \phi(y)$$

Attention à ne pas s'emmeler les pinceaux entre les différents ensembles et les différentes lois. x et y sont des éléments de G. On doit donc leur appliquer la loi

$*$. En revanche, $\phi(x)$ et $\phi(y)$ sont des éléments de G', et on doit leur appliquer la loi $*'$.

Cette définition est suffisante pour qu'un morphisme de groupe se comporte bien vis-à-vis de l'élément neutre et de l'inversion.

Soit ϕ un morphisme de groupe de $(G, *)$ dans $(G', *')$. Alors
- $\phi(e) = e'$
- $\forall x \in G \;\; \phi(x)^{-1} = \phi(x^{-1})$

- ϕ étant un morphisme, $\phi(e) = \phi(e * e) = \phi(e) *' \phi(e)$ d'où en simplifiant $\phi(e) = e'$
- Soit $x \in G$. $\phi(x) *' \phi(x^{-1}) = \phi(x * x^{-1}) = \phi(e) = e'$. De même, $\phi(x^{-1}) *' \phi(x) = e'$, et $\phi(x^{-1})$ est l'inverse de $\phi(x)$.

Par ailleurs, on montre facilement par récurrence que les morphismes se comportent bien vis-à-vis des puissances :

Soit ϕ un morphisme de groupe de $(G, *)$ dans $(G', *')$. Alors
$\forall p \in \;\; \forall x \in G \;\; \phi(x)^p = \phi(x^p)$

- L'identité est un morphisme de tout groupe dans lui même.
- Soit $(G, *)$ un groupe d'élément neutre e. L'application $\phi : x \mapsto e$ est un morphisme de G dans lui-même : pour tout $(x, y) \in G^2$, $\phi(x) * \phi(y) = e * e = e = \phi(x * y)$.
- exp est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}^{+*}, \times)$: soit $(x, y) \in \mathbb{R}$, $\exp(x+y) = \exp(x) \times \exp(y)$.
- ln est un morphisme de $(\mathbb{R}^{+*}, \times)$ dans $(\mathbb{R}, +)$: soit $(x, y) \in \mathbb{R}$, $\ln(x \times y) = \ln(x) + \ln(y)$.

Pour finir, un résultat sur la composée de deux morphismes :

La composée de deux morphismes de groupe est un morphisme de groupe.

Soient $(G, *), (G', *')$ et $(G'', *'')$ trois groupes, et $\phi : GG'$ et $\phi' : G'G''$ deux morphismes. Nous allons montrer que $\phi' \text{o} \phi$ est un morphisme.

Soient x et y dans G. ϕ étant un morphisme, $\phi(x * y) = \phi(x) *' \phi(y)$. ϕ' étant un morphisme, on a $\phi'(\phi(x * y)) = \phi'(\phi(x)) *'' \phi'(\phi(y))$, d'où $\phi' \text{o} \phi(x) *'' \phi' \text{o} \phi(y) = \phi' \text{o} \phi(x * y)$.

Dans la suite du chapître, nous noterons les multiplications par ., et nous les omettrons dans les calculs pour abréger les notations. Attention, il faut tout de même avoir conscience des ensembles dans lesquels les objets manipulés se situent.

2.3.1 Morphismes et sous-groupes

On a la propriété fondamentale suivante, qui indique que les morphismes se comportent bien vis-à-vis des sous-groupes :

Soit ϕ un morphisme de groupe de $(G, .)$ dans $(G', .)$.
- L'image d'un sous-groupe de G par ϕ est un sous-groupe de G'.
- L'image réciproque d'un sous-groupe de G' par ϕ est un sous-groupe de G.

Utilisons 2.2.
- Soit H un sous-groupe de G. $e \in H$ donc $e' = \phi(e) \in Im(\phi)$
  Soient y et y' dans $\phi(H)$. Montrons que yy'^{-1} est dans $\phi(H)$.
  Soient x et x' dans H tels que $\phi(x) = y$ et $\phi(x') = y'$. ϕ étant un morphisme, on a $yy'^{-1} = \phi(x)\phi(x')^{-1} = \phi(x)\phi(x'^{-1}) = \phi(xx'^{-1}) \in \phi(H)$ car $xx'^{-1} \in H$ par 2.2.
- Soit H' un sous-groupe de G'. $\phi(e) = e'$ et $e' \in H'$, donc $e \in \phi^{-1}(H')$.
  Soient x et x' dans $\phi^{-1}(H')$. On a $\phi(xx'^{-1}) = \phi(x)\phi(x')^{-1} \in H'$ par 2.2, et donc $xx'^{-1} \in \phi^{-1}(H')$.

2.3.2 (iso/endo/auto)-morphismes

Quelques cas particuliers de morphismes de groupes :

On appelle endomorphisme de groupe un morphisme de groupe entre un groupe et lui-même.

On appelle isomorphisme de groupe un morphisme de groupe bijectif.

On appelle automorphisme de groupe un isomorphisme d'un groupe dans lui-même.

Si un isomorphisme existe entre deux groupes, cela signifie que l'on peut complètement transporter la structure de l'un sur l'autre.

L'inverse d'un isomorphisme de groupe est un isomorphisme de groupe.

Soit ϕ un isomorphisme de $(G, .)$ dans $(G', .)$.

ϕ^{-1} est clairement bijective.

Soient x' et y' dans G'. Considérons $a = \phi^{-1}(x'y')$, et $b = \phi^{-1}(x')\phi^{-1}(y')$. On a $\phi(a) = x'y'$, et $\phi(b) = \phi(\phi^{-1}(x'))\phi(\phi^{-1}(y')) = x'y'$.

Par bijectivité de ϕ, $a = b$.

- exp et ln dans les exemples précédents sont des isomorphismes.

- Soit $(G, .)$ un groupe, et $g \in G$. L'application $\phi : x \mapsto gxg^{-1}$ est un automorphisme : en effet, $\phi(x).\phi(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = \phi(xy)$, et f est de plus bijective, de réciproque $x \mapsto g^{-1}xg$ (f est ce que l'on appelle un *automorphisme intérieur*).

Montrer que l'ensemble des automorphismes d'un groupe $(G, .)$ muni de la loi o est un groupe.

2.3.3 Un morphisme fondamental

Soit $(G, .)$ un groupe, et $a \in G$. L'application $f : p \in \mapsto a^p$ est un morphisme de groupe.

C'est la première partie de la proposition 2.1.1.
Cette proposition montre, d'après 2.3, la seconde partie de la proposition 2.1.1.

2.4 Noyau et image

[Noyau, image]
Soit ϕ un morphisme de groupe de $(G, .)$ dans $(G', .)$. Soit e' le neutre de $(G', .)$.
- On appelle image de ϕ et on note $Im(\phi)$ l'ensemble $\phi(G)$.
- On appelle noyau de ϕ et on note $Ker(\phi)$ [2]l'ensemble $\phi^{-1}(\{e'\})$.

Soit ϕ un morphisme de groupe de $(G, .)$ dans $(G', .)$.
- L'image de ϕ est un sous-groupe de G'.
- Le noyau de ϕ est un sous-groupe de G.

C'est un cas particulier de 2.3.1, appliquée aux sous-groupes triviaux.
Ces propriétés sont très utile pour montrer qu'un ensemble est un groupe : si on arrive à l'exprimer comme image ou comme antécédent d'un groupe connu par un morphisme de groupe, c'est gagné.

Considérons le morphisme défini en 2.3.3.
- Son noyau est un sous-groupe de , ce qui signifie qu'il existe un unique $p \in$ tel que $\{n \in \ | \ a^n = e\} = p$.
  p est alors appelé *ordre* de a.
- Son image est un sous-groupe de G, ce qui signifie que pour tout $a \in G$, $\{\ldots, a^{-2}, a^{-1}, e, a, a^2 \ldots\}$ est un sous-groupe de G.

2. de l'allemand *kernel* : noyau

Ce sous-groupe est appelé *sous-groupe engendré* par a.

La propriété suivante démontre la force de la notion de morphisme, et l'intérêt d'introduire de la structure sur des ensembles.

Un morphisme de groupe est injectif si et seulement si son noyau est réduit à l'élément neutre.

- Le sens direct est trivial : si le noyau n'est pas réduit à un seul élément, e' a plusieurs antécédents.
- Soit $\phi : (G, .) \mapsto (G', .)$, tel que $Ker(\phi) = \{e\}$. Soient x et y dans G tels que $\phi(x) = \phi(y)$. On a alors $\phi(x)\phi(y)^{-1} = e'$ d'où $\phi(xy^{-1}) = e'$. Par hypothèse, $xy^{-1} = e$ et donc $x = y$.

On n'utilisera donc **jamais** la définition classique de l'injectivité pour démontrer l'injectivité d'un morphisme de groupe.

2.5 Engendrement

Commençons par un résultat important sur les sous-groupes.

Soit $(G, .)$ un groupe, et $(H, .)$ et $(K, .)$ deux sous-groupes de G. Alors $(H \cap K, .)$ est un sous-groupe de G.

Immédiat d'après la caractérisation des sous-groupes.

Cette propriété se généralise à tout intersection de sous-groupes.

Elle légitime la définition suivante :

Soit $(G, .)$ un groupe, et $A \in \mathcal{P}(G)$. On appelle sous-groupe engendré par A et on note $< \mathbf{A} >$ l'intersection de tout les sous-groupes de $(G, .)$ contenant A.

Il s'agit du plus petit (au sens de l'inclusion) sous-groupe de $(G, .)$ contenant A.

- $< \emptyset >= \{e\}$
- $< e >= \{e\}$
- $< G >= G$
- $\forall a \in G \quad < a >= \{\ldots, a^{-2}, a^{-1}, e, a, a^2 \ldots\}$: on retombe sur la définition donnée dans l'exemple de la section 2.4.

  — $\{\ldots, a^{-2}, a^{-1}, e, a, a^2 \ldots\}$ est bien un sous-groupe de G contenant a.

  — Montrons qu'il est le plus petit : soit H un sous-groupe de G contenant a. H contient trivialement e. Par stabilité par produit, H contient $a^2 = aa$, puis $a^3 = a^2a$, etc...Par stabilité par passage à l'inverse, H

contient a^{-1} et de même toutes les puissances négatives de a. Donc $\{\ldots, a^{-2}, a^{-1}, e, a, a^2 \ldots\} \subset H$.

Rappelons que l'**ordre** de a dans G est l'unique entier p tel que $\forall n \;\; a^n = e \Leftrightarrow n \in p$.

Soit $(G, .)$ un groupe, et $a \in G$. Soit a l'ordre de n. Alors

- si $n = 0$, $< A >$ est infini et isomorphe à .
- sinon, $< A >$ est fini et égal à $\{e = a^0, a = a^1, \ldots a^{n-1}\}$

- Supposons $n = 0$.
  L'application $f : p \in \mapsto a^p \in < a >$ est un morphisme de groupe trivialement surjectif. Par définition de l'ordre, $f(p) = e \Leftrightarrow p = 0$, ce qui d'après 2.4 montre l'injectivité.
- Supposons $n \neq 0$.
  $\{e, a, \ldots a^{n-1}\}$ est trivialement inclus dans $< a >$.
  On a $a^n = e$. Soit $p \in Z$. On peut écrire par division euclidienne de p par n, $p = nq + r$, avec $0 \leq r < n$.
  On a alors $a^p = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r \in \{e, a, \ldots a^{n-1}\}$, d'où l'inclusion réciproque.

- Un groupe est dit monogène Ssi il est engendré par un unique élément, i.e. Ssi $\exists a \in G \;\; G =< a >$.
- Un groupe est dit cyclique Ssi il est monogène et fini.

Tout groupe monogène infini est isomorphe à $(, +)$.

Corollaire immédiat de la proposition ci-dessus.

Par ailleurs, nous verrons dans le chapître sur l'arithmétique que l'on peut aussi facilement régler le cas des groupes cycliques, qui sont isomorphes à $(\mathbb{Z}/n\mathbb{Z}, +)$, n étant l'ordre du groupe.

3 Anneaux

3.1 Définitions et propriétés

[Anneau]

Soit A un ensemble muni de deux lci $\times$ et $+$. On dit que $(A, +, \times)$ est un anneau Ssi

- $(A, +)$ est un groupe commutatif.
- $\times$ est associative.
- $\times$ est distibutive sur $+$:

$$\forall (x, y, z) \in A^3 \;\; x \times (y + z) = x \times y + x \times z \text{ et } (y + z) \times x = y \times x + z \times x$$

- $\times$ admet un élément neutre.

Si $\times$ est commutative, on parlera d'anneau commutatif.

L'élément neutre de $+$ sera notée en général 0, et celui de $\times$ sera noté 1.

Attention, ces notations sont conventionnelles, elles ne veulent pas dire qu'un anneau contient les entiers 0 et 1...

Par ailleurs, on notera souvent A ou B un anneau.

- $(, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{Z}, +, \times)$ sont des anneaux.
- $(\mathbb{R}[X], +, \times)$ est un anneau – appelé *anneau des polynômes* sur .
- $(\mathbb{R}(X), +, \times)$ est un anneau – appelé *anneau des fractions rationnelles* sur .
- $(\mathbb{S}R, +, \times)$ muni des lois d'addition et de multiplication terme-à-terme est anneau.
- $(\mathbb{R}^{\mathbb{R}}, +, \times)$ muni des lois d'addition et de multiplication usuelles est un anneau.
- $\{0, 1\}$ muni des lois suivantes

$+$	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

est un anneau.

Quelques propriétés des anneaux :

- 0 est absorbant, i.e.

$$\forall x \in A \;\; 0.x = 0$$

- $$\forall (x, y) \in A^2 \;\; (-x).y = -(x.y) = x.(-y)$$

- Soit $x \in A$. $0.x \underset{0\ neutre}{=} (0+0)x \underset{distr}{=} 0x + 0x$. Par simplification, on a alors $0x = 0$.
- Soient $(x, y) \in A^2$. $(-x)y + xy \underset{distr}{=} (-x + x)y = 0y \underset{0\ abs}{=} 0$. $(A, +)$ étant commutatif, $(-x)y = -(xy)$. On prouve de même l'autre égalité.

[Anneau intègre]
Un anneau $(A, +, \times)$ est dit intègre Ssi

$$\forall (a, b) \in A^2 \ \ ab = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Reprenons les exemples ci-dessus :

- $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{Z}, +, \times)$ sont des anneaux intègres.
- $(\mathbb{R}[X], +, \times)$ est un anneau intègre.
- $(, +, \times)$ anneau non-intègre : $(0, 1, 0, 1 \dots) \times (1, 0, 1, 0 \dots) = (0, 0, 0, 0 \dots)$.
- $(\mathbb{R}^{\mathbb{R}}, +, \times)$ est un anneau non-intègre : $1_{\{1\}} \times 1_{\{0\}} = 0$

3.2 Calcul dans des anneaux

[Distributivité par rapport à $\sum$]
Soit $(a_i)_{i \in I}$ une famille finie déléments de A. Soit $x \in A$.
Alors

$$x \sum_{i \in I} a_i = \sum_{i \in I} x a_i$$

et

$$(\sum_{i \in I} a_i) x = \sum_{i \in I} a_i x$$

Par récurrence triviale sur le cardinal de I.

On a également dans tout anneau les formules suivantes :

Soient $(a, b) \in A^2$ deux éléments **qui commutent** (i.e. ab=ba). Soit $n \in \mathbb{N}$.
Alors

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

En particulier,

$$a^n - 1 = (a-1)\sum_{i=0}^{n-1} a^i$$

On montre cette propriété à l'aide d'un simple calcul :

$$(a-b)\sum_{i=0}^{n-1} a^i b^{n-i-1} = \sum_{i=0}^{n-1} a^{i+1} b^{n-i-1} - \sum_{i=0}^{n-1} a^i b^{n-i} = \sum_{i=1}^{n} a^i b^{n-i} - \sum_{i=0}^{n-1} a^i b^{n-i} = a^n - b^n$$

Soient $(a, b) \in A^2$ deux éléments **qui commutent** (i.e. ab=ba). Soit $n \in \mathbb{N}$. Alors

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

Par récurrence sur n.

Initialisation : par convention, $(a+b)^0 = a^0 = b^0 = 1$, d'où le résultat.

Hérédité : supposons le résultat vrai pour n. Écrivons

$$\begin{aligned}
(a+b)^{n+1} &= a(a+b)^n + b(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{i+1} b^{n-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n+1-i} \\
&= \sum_{i=1}^{n+1} \binom{n}{i-1} a^i b^{n+1-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n+1-i} \\
&= 1 + 1 + \sum_{i=1}^{n} \left(\binom{n}{i} + \binom{n}{i-1} \right) a^i b^{n+1-i} = 1 + 1 + \sum_{i=1}^{n} \binom{n+1}{i} a^i b^{n+1-i} \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i}
\end{aligned}$$

3.3 Sous-anneau

[Sous-anneau]

Soit $(A, +, \times)$ un anneau. On appelle sous-anneau de $(A, +, .)$ tout anneau de la forme $(B, +, \times)$ où $B \subset A$.

Un sous-anneau est donc simplement un sous-ensemble qui est un anneau **pour les mêmes lois**. En particulier, B doit être stable par $\times$ et $+$.

- Pour tout $n \in \mathbb{N}$, $({}_n[X], +, \times)$, l'ensemble des polynômes de degré au plus n est un sous-anneau de $([X], +, \times)$.
- $(\mathcal{C}^0(,), +, \times)$ est un sous-anneau de $(', +, \times)$.
- $(\mathcal{S}_0(), +, \times)$ – l'ensemble des suites de limite nulle – est un sous-anneau de $(, +, \times)$.

Soit $(A, +, \times)$ un anneau. Soit $B \subset A$.
$(B, +, \times)$ est un sous-anneau de $(A, +, \times)$ Ssi
- $(B, +)$ est un sous groupe de $(A, +)$
- $1_A \in B$
- B est stable par produit

La notion de sous-anneau n'est en fait pas aussi puissante que celle de sous-groupe [3]. C'est pourquoi vous verrez plus tard que l'on préfère utiliser une notion différente appelée « idéal ».

3.4 Morphisme d'anneau

[Morphisme d'anneau]
Soient $(A, +, \times)$ et $(A', +', \times')$ deux anneaux. On dit que $\phi : AA'$ est un morphisme d'anneaux de $(A, +, \times)$ vers $(A', +', \times')$ Ssi
- ϕ est un morphisme de groupe de $(A, +)$ vers $(A', +')$
- $\phi(1_A) = 1_{A'}$
- $\forall (a, b) \in A^2 \;\; \phi(a \times b) = \phi(a) \times' \phi(b)$

Tout comme dans le cas des morphismes de groupe, les morphismes d'anneau transportent les structures :

- L'image d'un sous-anneau par un morphisme d'anneau est un sous-anneau.
- L'image réciproque d'un sous-anneau par un morphisme d'anneau est un sous-anneau.

Soit ϕ un morphisme de $(A, +, \times)$ dans $(A', +', \times')$
- Soit $(B, +, \times)$ un sous-anneau de $(A, +, \times)$
  - ϕ est aussi un morphisme de groupe, et donc $(\phi(B), +')$ est un sous-groupe de $(A', +)$.
  - $\phi(1_A) = 1_{A'}$ d'où $1_{A'} \in \phi(B)$.
  - Soient $(a' = \phi(a), b' = \phi(b)) \in \phi(B)$. On a $a' \times' b' = \phi(a) \times' \phi(b) = \phi(a \times b) \in \phi(B)$.
- Soit $(B', +, \times)$ un sous-anneau de $(A', +, \times)$

3. disons seulement pour les lecteurs ayant déjà étudié les factorisations par les sous-groupes que les sous-anneaux ne permettent pas de factoriser les anneaux

— ϕ est aussi un morphisme de groupe, et donc $(\phi^{-1}(B'), +')$ est un sous-groupe de $(A, +)$.
— $\phi(1_A) = 1_{A'} \in B'$ d'où $1_A \in \phi^{-1}(B')$.
— Soient $(a, b) \in \phi^{-1}(B')$. On a $\phi(a \times b) = \phi(a) \times' \phi(b) \in B'$, d'où $a \times b \in \phi^{-1}(B')$.

Comme pour les morphismes de groupes, on définit également les *isomorphismes*, *endomorphismes* et *automorphismes* d'anneaux.

La conjugaison de $\mathbb{C}$ dans $\mathbb{C}$ est un automorphisme d'anneau : en effet,
- $\bar{1} = 1$
- $\forall (z, z') \in C^2 \ \ \overline{z - z'} = \overline{z} - \overline{z'}$
- $\forall (z, z') \in C^2 \ \ \overline{zz'} = \overline{z}\overline{z'}$

3.4.1 Un morphisme fondamental

Nos considérations sur les puissances dans les groupes montrent immédiatement que :

Pour tout anneau $(A, +, \times)$, $\phi : z \mapsto z.1$, est un morphisme d'anneau ϕ de dans A.

ϕ étant en particulier un morphisme de groupe, son noyau est un sous-groupe de , et est donc de la forme n pour un certain n.

Ce n est appelé **caractéristique** de l'anneau, et joue un rôle très important en théorie des anneaux.

4 Corps

[Corps]

Soit un ensemble K muni de deux lci $+$ et $\times$. On dit que $(K, +, \times)$ est un corps Ssi

- $(K, +, \times)$ est un anneau
- $0 \neq 1$ (un corps n'est pas réduit à un seul élément)
- tout élément de K différent de 0_K admet un inverse pour la loi multiplicative.

Nous dirons par ailleurs que le corps est commutatif si la loi . est commutative.

Il s'agit donc d'une structure plus fine que la structure d'anneau.

Dans la mesure où nous n'étudierons que des corps commutatifs, nous omettrons l'épithète, et parlerons de *corps* pour un corps commutatif.

On note $K^* = K \backslash \{0_K\}$. Muni de cette notation, on peut proposer la définition équivalente suivante :

[Corps]

Soit un ensemble K muni de deux lci $+$ et .. On dit que $(K, +, \times)$ est un corps Ssi

- $(K, +)$ est un groupe commutatif.
- $(K^*, \times)$ est un groupe commutatif.
- $\times$ est distributive sur $+$.

- $(\mathbb{R}, +, \times)$, $(, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps.
- en revanche, $(\mathbb{Z}, +, \times)$ n'est pas un corps : 2 n'est pas inversible.
- $((X), +, \times)$ est un corps on parlera donc de *corps des fractions rationnelles*
- en revanche, $(\mathbb{R}[X], +, \times)$ n'est pas un corps : tout polynôme de degré plus grand que 1 n'est pas inversible.
- L'ensemble $\{0, 1\}$ muni des lois $+$ et $\times$ définies par

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

  est un corps : 1 est inversible, et est son propre inverse. Il s'agit du plus petit corps possible.

4.1 Sous-corps

On commence à avoir l'habitude :

[Sous-corps]

Soit $(K, +, \times)$ un corps. On appelle sous-corps de $(K, +, .)$ tout corps de la forme $(K', +, \times)$ où $K' \subset K$.

et de même que pour les groupes et les anneaux, on obtient un caractérisation, dont la démonstration est laissée en exercice.

Soit $(K, +, \times)$ un corps. Soit $K' \subset K$.
$(K', +, \times)$ est un sous-corps de $(K, +, \times)$ Ssi
- K' contient 1_K.
- $(K', +)$ est un sous groupe de $(K, +) : \forall (x, y) \in K'^2 \;\; x - y \in K'$
- $(K'^*, \times)$ est un sous-groupe de $(K^*, \times) : \forall (x, y) \in (K'^*)^2 \;\; xy^{-1} \in K'^*$

- $(\mathbb{Q}, +, \times)$ est un sous-corps $(\mathbb{R}, +, \times)$, qui est un sous-corps de $(\mathbb{C}, +, \times)$.
- $\{a + ib \mid (a, b) \in \mathbb{Q}^2\}$ est un sous-corps de $\mathbb{C}$.

4.2 Morphismes de corps

[Morphisme de corps]
Soient $(K, +, \times)$ et $(K', +', \times')$ deux corps. On dit que $\phi : KK'$ est un morphisme de corps de $(K, +, \times)$ vers $(K', +', \times')$ Ssi ϕ est un morphisme d'anneau de $(K, +, \times)$ vers $(K', +', \times')$.
Toutes les propriétés des morphismes d'anneaux se transposent donc. On peut montrer que l'on a de plus préservation de l'inverse pour $\times$ par tout morphisme de corps, et que les images et images réciproques de sous-corps sont des sous-corps.

La conjugaison est un automorphisme de corps sur .

Montrer que les seuls automorphismes de corps **continus** sur $\mathbb{C}$ sont l'identité et la conjugaison.

Soit ϕ un automorphisme de corps continu sur $\mathbb{C}$.
On a déjà $\phi(1) = 1$, d'où l'on déduit par la propriété 2.3 sur les morphismes et les multiples que $\forall p \in \mathbb{Z} \;\; \phi(p) = \phi(p.1) = p.\phi(1) = p.1 = p$.
En passant à l'inverse, et par stabilité par produit, on obtient facilement $\forall x \in \mathbb{Q} \;\; \phi(x) = x$.
Par continuité de ϕ et densité de $\mathbb{Q}$ dans $\mathbb{R}$, on en déduit : $\forall x \in \mathbb{R} \;\; \phi(x) = x$.
ϕ est donc l'identité sur $\mathbb{R}$.
Considérons maintenant l'image de i par ϕ, $a = \phi(i)$.
On a $a^2 = \phi(i)^2 = \phi(i^2) = \phi(-1) = -1$.
On a donc $a = i$ ou $a = -i$.
- Si $a = i$, soit $z = c+id \in \mathbb{C}$. On a $\phi(z) = \phi(c+id) = \phi(c)+a\phi(d) = c+id = z$ et ϕ est l'identité.

- Si $a = -i$, soit $z = c + id \in \mathbb{C}$. On a $\phi(z) = \phi(c + id) = \phi(c) + a\phi(d) = c - id = \overline{z}$ et ϕ est la conjugaison.

Réciproquement, ces deux applications sont bien des morphismes de corps.

4.3 De $\mathbb{Z}$ vers $\mathbb{Q}$: L'anneau des fractions

Ce paragraphe peut être laissé pour une lecture ultérieure.
Nous allons présenter une fa con de construire le *corps* à partir de l'anneau $\mathbb{Z}$. Cette méthode se généralise aux anneaux généraux.

Considérons $(\mathbb{Z} \times \mathbb{Z}^*)$ et $\sim$ une relation binaire sur cet ensemble, définie par $\forall((a,b)(c,d)) \in (\mathbb{Z} \times \mathbb{Z}^*)^2 \;\; (a,b) \sim (c,d)$ Ssi $ad = bc$.

On vérifie facilement en calculant un peu que

$\sim$ est une relation déquivalence.

On peut alors définir $\mathbb{Q}$ comme $\mathbb{Z}/\sim$ avec les lois suivantes :

$$\mathcal{O}(a,b) + \mathcal{O}(c,d) = \mathcal{O}(ad + bc, bd)$$

$$\mathcal{O}(a,b).\mathcal{O}(c,d) = \mathcal{O}(ac, bd)$$

Soit, en notant comme on le fait traditionnellement $\frac{a}{b}$ au lieu de $\mathcal{O}(a,b)$,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b}.\frac{c}{d} = \frac{ac}{bd}$$

Il faut vérifier que ces lois sont *bien définies*, c'est à dire que si l'on a $\mathcal{O}(a,b) = \mathcal{O}(a',b')$ et $\mathcal{O}(c,d) = \mathcal{O}(c',d')$, on a bien $\mathcal{O}(ad + bc, bd) = \mathcal{O}(a'd' + b'c', b'd')$, et de même pour le produit – sans quoi les définition de l'addition et de la multiplication sont incorrectes.

Faisons-le par exemple pour l'addition : supposons donc $\mathcal{O}(a,b) = \mathcal{O}(a',b')$ et $\mathcal{O}(c,d) = \mathcal{O}(c',d')$, soit $(a,b) \sim (a',b')$ et $(c,d) \sim (c',d')$.

Alors, par définition de $\sim$, on a $ab' = a'b$ et $cd' = c'd$.

On cherche à montrer que $b'd'(ad + bc) = bd(a'd' + b'c')$, soit $ab'\ dd' + bb'\ cd' = a'b\ dd' + bb'\ c'd$, ce qui découle immédiatement des égalités ci-dessus.

$(, +, \times)$ est un corps.

La démonstration est purement calculatoire, mais ne présente pas de difficulté. Les points à vérifier sont les suivants :

- $(,+)$ est un groupe abélien.
  - $+$ est associative.
  - $+$ est commutative.
  - $\frac{0}{1}$ est élément neutre.
  - tout élément admet un inverse (l'inverse de $\frac{x}{y}$ est $\frac{-x}{y}$).
- $.$ est associative.
- $.$ admet un neutre $(\frac{1}{1})$.
- $.$ est distributive sur $+$.
- Tout élément différent de $\frac{0}{1}$ admet un inverse.
- $.$ est commutative.

Cette construction ne repose que sur les propriétés d'anneau de $\mathbb{Z}$, et peut donc être généralisée à n'importe quel anneau A. On parle alors de *corps des fractions* de l'anneau A.

Par exemple, (X) est formellement construit de cette manière à partir de $[X]$.