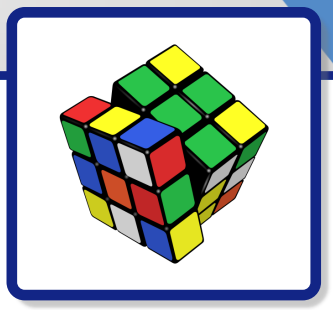
Algèbre II : Notes de cours - Partie 1

Hamza El Mahjour

Licence 1 : SMI/SMA/SMPC

Table des matières

2. Structures usuelles : groupes, anneaux et corps



Il est impossible d'être mathématicien sans être poète dans l'âme.

— Sofia Kovalevskaya

2.1 Groupes

On commencera ce chapitre par un exemple simple que nous manipulons chaque jour : l'addition des nombres entiers relatifs ! Il est évident pour vous que $5+3=8$ et $-176+76=100$. Mais, ce ne sont pas les résultats de ces opérations qui nous intéressent, plutôt les types de manipulations que nous pouvons appliquer dessus. Si je nomme x un nombre et y un autre nombre, on constate que $x+y$ doit aussi être un nombre qui est le résultat de la somme $x+y$ donc $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ implique que $x+y \in \mathbb{Z}$. On peut constater aussi que les nombres opposés sont de somme nulle, par exemple $5+(-5)=0$. Donc, pour chaque x de $\mathbb{Z}$ il existe $-x$ de $\mathbb{Z}$ tel que $x+(-x)=0$. On sait aussi que pour tout x dans $\mathbb{Z}$ on a $x+0=0+x=x$, on peut dire que 0 est un élément 'neutre' qui ne change pas le résultat de l'opération $+$ quand il est combiné avec n'importe quel autre nombre. Bien sûr, on est aussi d'accord que $7+((-8)+5)=(7+(-8))+5=4$. Plus généralement $(x+y)+z=x+(y+z)$ pour tout x, y et z dans $\mathbb{Z}$. Pour récapituler, on peut dire que l'ensemble $\mathbb{Z}$ muni de l'opération $+$ vérifie les axiomes suivants :

(i) $\forall x, y \in \mathbb{Z}, \quad x+y \in Z$,
(ii) $\forall x \in \mathbb{Z}, \exists y := -x \in \mathbb{Z}, \quad x+(-x)=0$,
(iii) $\exists\, 0 \in \mathbb{Z}, \forall x \in Z,\ 0+x=x+0=x$,
(iv) $\forall x, y$ et z dans $\mathbb{Z}$, $\quad (x+y)+z = x+(y+z)$.

Il serait intéressant si nous pouvons étendre ces propriétés pour des ensembles plus abstraits où les éléments ne sont pas des nombres mais des ensembles ou des fonctions ! Mais avant de généraliser, remarquons que les axiomes précédents ne sont pas forcément toujours réalisables pour n'importe quel ensemble et n'importe

quelle opération, on sera peut être déçue que certains ensembles très simples et aussi des opérations simples échouent certains axiomes précédents. Prenons $(\mathbb{N}, +)$ l'ensemble des entiers naturels muni de l'addition, on constate que le deuxième axiome n'est pas valide, car on ne peut pas additionner deux entiers naturels non-nuls et obtenir une somme nulle. Gardons cette fois le même ensemble muni de la soustraction usuelle on remarque que $2 - 3 = -1$ or $-1 \notin \mathbb{N}$.

Définition 2.1. *Soit E un ensemble quelconque. On dit que $\star$ est une **loi de composition interne** si*

$$\forall (x, y) \in E \times E, \qquad x \star y \in E.$$

Donc l'axiome (i) on lui attribue un nom comme indiqué dans la définition, c'est à dire qu'en combinant/composant deux éléments de E, on doit être sûr que le résultat de cette composition reste dans E.

Exemple 2.1.

1. *L'addition usuelle sur $\mathbb{R}$ est une loi de composition interne. De même pour $\mathbb{C}, \mathbb{Z}$ ou $\mathbb{Q}$.*
2. *L'intersection $\bigcap$ et l'union $\bigcup$ définis sur $\mathcal{P}(E)$ l'ensemble des parties de E représentent tous les deux des lois de composition interne.*
3. *Sur l'ensemble des fonctions numériques de $\mathbb{R}$ dans $\mathbb{R}$, chacune des opérations suivantes forme une loi de composition interne*

Cette loi de composition interne est essentielle pour pouvoir construire la première structure algébrique de ce cours qui est un **groupe**.

Définition 2.2. *Soit $(E, \star)$ l'ensemble E muni de loi de composition interne $\star$. Si*
(a) $\forall x, y, z \in E \quad (x \star y) \star z = x \star (y \star z)$ *(associativité),*
(b) $\exists e \in E, \forall x \in E, \quad x \star e = e \star x = x$ *(élément neutre),*
(c) $\forall x \in E, \exists \bar{x} \in E, \quad x \star \bar{x} = \bar{x} \star x = e$ *(opposé ou inverse[1]),*
*alors on dit que $(E, \star)$ est un **groupe**. Si de plus $x \star y = y \star x$, on dit qu'il est un groupe **commutatif** ou **abélien**[2].*

On peut tester avec des exemples et découvrir si les ensembles définis forment bien un groupe ou pas.

Exemple 2.2.

1. *$(\mathbb{Z}, +)$ est un groupe, on la discutait dans l'introduction. De même sont $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.*

2. *L'ensemble* $F = \{-1, 1, i, -i\} \subset \mathbb{C}$ *muni de la multiplication usuelle des nombres complexes est bien un groupe (Vérifier comme exercice).*
3. *Il existe des groupes multiplicatifs bien sûr comme* $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ *et* $(\mathbb{C}^*, \cdot)$.

Remarque 2.1. *L'opposé est généralement noté* $-x$ *tandis que l'inverse est noté* x^{-1}.

2.1.1 Groupe symétrique

On va maintenant étudier un ensemble particulier de groupes qui sont les groupes de symétries. La notion de symétrie nous est familière car elle a une interprétation géométrique claire. On en connaît par exemple la symétrie axiale et la symétrie centrale. C'est pourquoi, pour se baser sur un outil tangible, nous préférons commencer par un exemple très simple et très riche. On étudiera un triangle équilatéral en nommant ses sommets consécutivement 1,2 et 3. Plus précisément on va appliquer des transformations géométriques sur le triangle qui permettent de garder le même triangle en changeant seulement les noms des sommets. La symétrie axiale et la rotation sont utilisés afin d'accomplir cet objectif comme le montre la figure 2.1. Pour formaliser l'approche géométrique précédente, on considère l'ensemble des transformations $\mathcal{S} = \{\mathrm{Id}, \mathrm{Ax}_1, \mathrm{Ax}_2, \mathrm{Ax}_3, \mathrm{R}_{120°}, \mathrm{R}_{-120°}\}$. Puisque nous avons besoin d'un groupe, on doit attribuer $\mathcal{S}$ une loi de composition interne, on va travailler avec la loi "$\circ$" qui compose des applications. Maintenant nous allons résumer les différentes composées des transformations de $\mathcal{S}$ dans le tableau 2.1. On remarque dans ce tableau que chaque élément combiné avec un autre donne un élément du même ensemble. Ceci confirme que $\circ$ est une loi de composition interne pour $\mathcal{S}$. De plus, en prenant n'importe quel élément $T \in \mathcal{S}$ on a $T \circ Id = Id \circ T = T$, c'est à dire que la transformation Id (qui garde chaque sommet dans sa place initial) est un élément neutre pour la loi $\circ$, en effet on appelle Id l'application "identité". On remarque aussi que pour chaque ligne et chaque colonne il existe une unique case contenant l'élément Id, c'est à dire que chaque transformation à une transformation inverse qui renvoie vers l'élément neutre. L'associativité est une propriété intrinsèque à la loi "$\circ$ (voir l'annexe sur la théorie des ensembles). On en conclut que $(\mathcal{S}, \circ)$ est un groupe fini composé de six éléments. On va voir dans la suite qu'il existe une manière plus élégante de définir et représenter ce cas particulier de la famille des **groupes symétriques**.

mini-exercice : Trouvez l'élément opposé/inverse de chaque élément de $(\mathcal{S}, \circ)$.

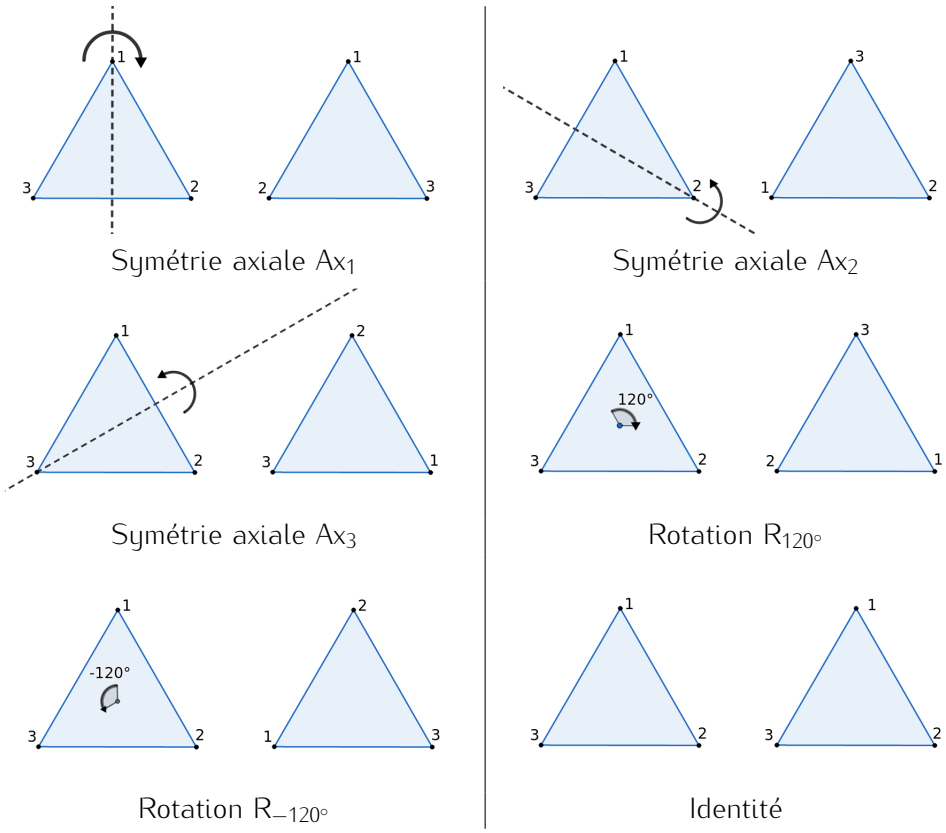


FIGURE 2.1 – Transformations préservant la forme et la position du triangle en interchangeant l'ordre des sommets.

$\circ$	Id	Ax_1	Ax_2	Ax_3	$R_{120°}$	$R_{-120°}$
Id	Id	Ax_1	Ax_2	Ax_3	$R_{120°}$	$R_{-120°}$
Ax_1	Ax_1	Id	$R_{-120°}$	$R_{120°}$	Ax_3	Ax_2
Ax_2	Ax_2	$R_{-120°}$	Id	$R_{120°}$	Ax_3	Ax_1
Ax_3	Ax_3	$R_{120°}$	$R_{-120°}$	Id	Ax_1	Ax_2
$R_{120°}$	$R_{120°}$	Ax_3	Ax_1	Ax_2	$R_{-120°}$	Id
$R_{-120°}$	$R_{-120°}$	Ax_2	Ax_3	Ax_1	Id	$R_{120°}$

TABLE 2.1 – Composées des transformations de l'ensemble $\mathcal{S}$.

Définition 2.3. *Soit Ω un ensemble fini ou infini. On définit*

$$\mathrm{Perm}(\Omega) = \{f : \Omega \longrightarrow \Omega, \quad f \text{ est bijective}\}.$$

On a utilisé "Perm" pour indiquer qu'il s'agit de l'ensemble des permutations possibles au sein d'un ensemble. Une bijection d'un ensemble fini dans lui même n'est autre qu'une substitution de la position de ces éléments.

Théorème 2.1

L'ensemble Perm(Ω) muni de la composition $\circ$ est un groupe.

Démonstration.

1. Il est claire, en appliquant le Théorème ?? (voir l'annexe) que $\circ$ est une loi de composition interne pour l'ensemble Perm(Ω).
2. On a déjà montré dans l'annexe qu'il existe une application bijective Id (l'identité) qui fait que $f \circ Id = Id \circ f = f$ pour tout f bijective. Donc Id est un élément neutre dans Perm.
3. On a aussi montré dans l'annexe que chaque bijection f admettait une bijection inverse f^{-1} telle que $f^{-1}f = ff^{-1} = Id$.
4. Par construction, $h \circ (g \circ f) = (h \circ g) \circ f$ donc $\circ$ est une loi associative.

Par ce qui précède on conclut que (Perm(Ω), $\circ$) est un groupe. □

Quand card (Perm(Ω) $= n < \infty$, on l'appelle **groupe de permutation** et on le note généralement $\mathfrak{S}_n$. En revenant un autre exemple de triangles équilatéral sur lequel on applique des transformations qui permutent ses sommets. Cette idée pourrait être exprimé autrement. On considère l'ensemble des sommets $S_3 = \{1, 2, 3\}$, si on considère le groupe $\mathfrak{S}_3 = (S, \circ)$. Dans ce qui on énumère les bijections possibles de S_3 dans S_3. Pour représenter les bijections de manière plus élégante on écrira $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ qui veut dire la bijection $\sigma_1 : S \longrightarrow S$ telle que $\sigma_3(1) = 2, \sigma_3(2) = 1$ et $\sigma_3(3) = 3$. Remarquez que cette permutation échange les sommets 1 et 2 et ne change pas le sommet 3, c'est en effet la symétrie axiale Ax_3. La notation intorduite est simple et on peut compter toutes les permutations possibles comme suit

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

On peut constater que les permutations σ_i correspondent aux symétries axiales et ρ_i aux rotations. C'est ainsi qu'on retrouve le même nombre de transformations

montrés sur les dessins de la Figure 2.1. Bien que nous ayons réussi à simplifier les notations des éléments du groupe symétrique $\mathfrak{S}_n$ (généralisable à tout autre dimension finie), il existe une notation encore plus simple qui est plus utile d'un point de vu algébrique. Dorénavant $S_n := \{1, 2, 3, \dots, n\}$.

Définition 2.4.
*Soit $n \in \mathbb{N}^*$ et soit $\mathfrak{S}_n$ le groupe symétrique de degré n. Soient $\{a_1, a_2, \dots, a_m\} \subset S_n$. Soit la permutation σ de $\mathfrak{S}_n$ qui envoie a_1 vers a_2 et a_2 vers a_3 et ainsi de suite jusqu'à renvoyer a_m au point de départ a_1 tout en gardant les autres éléments fixés. Cet élément σ sera noté $(a_1\ a_2\ a_3\ \dots\ a_n)$, on l'appelle **cycle** de longueur m.*

Définition 2.5. *Soit $\sigma \in \mathfrak{S}_n$ et soit $a \in S_n$ fixé. On appelle **orbite** de a par σ l'ensemble*

$$\mathcal{O}_{a,\sigma} = \{\sigma^n(a), \quad n \in \mathbb{N}\}.$$

Exemple 2.3.
Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} \in \mathfrak{S}_5$.

— *L'orbite de 1 par σ est symboliquement*

$$1 \to 4 \to 1 \to 4 \dots$$

donc $\mathcal{O}_{1,\sigma} = \{1, 4\} = \mathcal{O}_{4,\sigma}$.

— *L'orbite de 3 par σ symboliquement est*

$$3 \to 2 \to 5 \to 3 \to 2 \to \dots$$

donc $\mathcal{O}_{3,\sigma} = \{2, 3, 5\} = \mathcal{O}_{5,\sigma} = \mathcal{O}_{2,\sigma}$.

Soit $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix} \in \mathfrak{S}_5$. On voit bien que $\mathcal{O}_{1,\mu} = \{1\}, \mathcal{O}_{3,\mu} = \{3\}$ et $\mathcal{O}_{2,\mu} = \mathcal{O}_{4,\mu} = \mathcal{O}_{5,\mu} = \{2, 4, 5\}$. Cet exemple que dans certains cas les permutations ont une seule orbite qui contient plus de deux éléments et toutes les autres en contiennent un seul.

Définition 2.6. *Une permutation de $\mathfrak{S}_n$ est un **cycle** si elle contient au plus une orbite avec plusieurs éléments. La **longueur** d'un cycle est le cardinal de sa plus grande orbite.*

Dans l'exemple 2.3 μ est un cycle. On notera μ plutôt (2 5 4). Cette notation est spécifique aux orbites de $\mathfrak{S}_n$. En effet, il y a le résultat suivant qui montre l'utilité des cycles et leur notation.

Théorème 2.2

Toute permutation de $\mathfrak{S}_n$ s'écrit comme composée de cycles disjoints.

Démonstration. Soit $\mathcal{O}_{1,\sigma}, \mathcal{O}_{2,\sigma}, \ldots, \mathcal{O}_{r,\sigma}$ les orbites de $\sigma \in \mathfrak{S}_n$ tels que $\mathcal{O}_{i,\sigma}$ sont deux à deux disjoints. Cette famille des $\mathcal{O}_i$ existe il suffit juste de considérer que toutes les orbites qui ont exactement les mêmes éléments sont en effet une unique orbite, par ce processus d'élimination on arrive à $r \leq n$ orbites disjointes. On construit le cycle μ_i tel que

$$\mu_i(x) = \begin{cases} \sigma(x), & \text{si } \ x \in \mathcal{O}_{i,\sigma} \\ x, & \text{sinon.} \end{cases}$$

On remarque que par construction les cycles μ_i sont disjoints car $\mathcal{O}_{i,\sigma}$ sont disjoints. Prenons un x_0 quelconque de S_n, il appartient forcément à une orbite $\mathcal{O}_{i_0,\sigma}$. Par conséquent, pour tout $i \neq i_0, \mu_i(x) = Id(x) = x$, ceci est vrai pour tout x dans $\mathcal{O}_{i_0,\sigma}$, en particulier pour $\sigma(x_0)$ car il appartient aussi à $\mathcal{O}_{i_0,\sigma}$. C'est pourquoi $\forall i \neq i_0, \mu_i(\sigma(x_0)) = Id(\sigma(x_0)) = \sigma(x_0)$. Donc

$$\mu_1 \circ \mu_2 \ldots \circ \mu_{i_0} \ldots \circ \mu_r(x_0) = Id \circ Id \circ \ldots \mu_{i_0} \circ \ldots \circ Id(x) = \mu_{i_0}(x) = \sigma(x).$$

En appliquant la même idée pour tous les éléments de $S_n = \{1, 2, \ldots, n\}$ on trouve que

$$\mu_1 \circ \mu_2 \circ \ldots \mu_r = \sigma.$$

C'est le résultat désiré. □

Le cardinal de $\mathfrak{S}_n$ est $n! = n \cdot (n-1) \cdot (n-2) \ldots 3 \cdot 2 \cdot 1$

2.1.2 Homomorphisme de groupes

Soit f une fonction de $(\mathbb{R}, +)$ vers $(\mathbb{R}, +)$ telle que $f(x) = 5x$. Par un calcul simple nous avons $f(x+y) = 5(x+y) = 5x + 5y = f(x) + f(y)$. Donc f est une appplication qui transfert la loi $+$ entre le groupe de départ et le groupe d'arrivée. Prenons un autre exemple, soit g une fonction de $(\mathbb{R}, +)$ vers $(\mathbb{R}^*, \cdot)$ telle que $g(x) = e^x$. On a pour tout x, y de $\mathbb{R}$, $g(x+y) = e^{x+y} = e^x \cdot e^y = g(x) \cdot g(y)$. C'est à dire que l'application g préserve la loi de composition interne dans les deux groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \cdot)$. Plus généralement ce type de fonctions représente des **morphismes**/**homomorphisme** entre groupes.

Définition 2.7. *Soit $(G,*)$ et $(G',\star)$ deux groupes. Soit $\phi : G \longrightarrow G'$ une application telle que*

$$\forall x, y \in G, \qquad \phi(x * y) = \phi(x) \star \phi(y).$$

Alors ϕ est un ***homomorphisme*****/*****morphisme****.*

Définition 2.8. *Soit $(G,*)$ et $(H,\star)$ deux groupes d'éléments neutres e_G et e_H consécutivement. On définit le* ***noyau***[3] *d'un morphisme $\phi : G \longrightarrow H$ tel que*

$$\ker \phi = \{x \in G, \qquad \phi(x) = e_H\}.$$

Lemme 2.1

Soit ϕ un morphisme de $(G,*)$ vers $(H,\star)$ alors

1. $\phi(e_G) = e_H$,
2. L'inverse de $\phi(y)$ dans H est $\phi(y^{-1})$ où y^{-1} est l'inverse de y dans G.

Démonstration.

1. On a pour tout x dans G,

$$\phi(x) = \phi(x * e_G) \underbrace{=}_{\phi \text{ morphisme}} \phi(x) \star \phi(e_G),$$

de même

$$\phi(x) = \phi(e_G * x) = \phi(e_G) \star \phi(x),$$

Donc $\phi(e_G) = e_H$ par unicité de l'élément neutre.

2. Soit y dans G et y^{-1} son inverse. On sait que $\phi(e_G) = e_H$. Donc $\phi\left(y * y^{-1}\right) = e_H$. En appliquant la propriété du morphisme on a $\phi(y) \star \phi(y^{-1}) = e_H$ donc $\phi(y^{-1})$ est l'inverse de $\phi(y)$.

□

Proposition 2.1

Soit $\phi : G \longrightarrow H$. Si $\ker \phi = \{e_G\}$ alors ϕ est injective.

Démonstration. Soit x et y de G tels que $\phi(x) = \phi(y)$. Notons que $\phi(y) \in (H,\star)$ donc il existe l'inverse de $\phi(y)$ dans H qui est l'élément $\phi(y^{-1})$. C'est à dire qu'on peut écrire

$$\phi(x) \star \phi(y^{-1}) = \phi(y) \star \phi(y^{-1}) = e_H.$$

Et puisque ϕ est un morphisme alors $\phi(x) \star \phi(y^{-1}) = \phi(x * y^{-1}) = e_H$. Celà veut

dire que l'élément $x * y^{-1} \in \ker \phi$. Or $\ker \phi = \{e_G\}$, donc $x * y^{-1} = e_G$. En multipliant par y l'inverse de y^{-1} des deux côtés on obtient

$$x * y^{-1} * y = x * e = x = e * y = y.$$

Donc $x = y$ et l'application ϕ est injective. □

2.1.3 Sous-groupes

Chaque ensemble contient des sous-ensembles. On peut se poser la question suivante concernant les sous-ensembles d'un groupe : quelles sont les conditions suffisantes et nécessaires pour qu'un sous-ensemble d'un groupe soit aussi un groupe ? Une des réponses possibles est de dire que le sous-ensemble doit avoir toutes les propriétés du groupe et par conséquent il doit valider tous les axiomes donnés dans la Définition 2.2, mais ce serait pénible de vérifier tous ces axiomes à chaque fois ! C'est pourquoi la proposition suivante permet de donner un critère qui permet de réduire le nombre de conditions à vérifier.

Proposition 2.2

Soit $(G, *)$ un groupe et soit H une partie non-vide de G. H est un **sous-groupe** de G si

1. $*$ est une loi de composition interne pour H
2. Pour tout $h \in H$, son inverse est aussi dans H.

Dans ce cas $(H, *)$ est aussi un groupe.

Démonstration. La démonstration est évidente puisqu'il reste à montrer que $*$ est associative et qui est une propriété qui est vrai pour tous les éléments de G, en particulier ceux de H. Et il faut montrer que l'élément neutre de G est aussi celui de G. Soit h dans H. En utilisant le point 2 de la Prop 2.1.3 il existe h^{-1} aussi dans H tel que $h * h^{-1} = e$ où e est l'élément neutre de G. Puisque h et h^{-1} sont dans H et en utilisant le point 1 de la proposition 2.1.3 on en déduit que $h * h^{-1} \in H$, donc $e \in H$. C'est à dire que H admet un élément neutre. Donc $(H, *)$ est un groupe. □

Exemple 2.4.

1. *Les groupes* $(\mathbb{Z}, +)$ *et* $(\mathbb{Q}, +)$ *sont des sous-groupes de* $(\mathbb{R}, +)$.
2. $(\mathbb{Q}^*, \cdot)$ *est un sous-groupe de* $(\mathbb{R}, \cdot)$.

2.2 Anneaux

La richesse des groupes dépasse le contenu de ce cours, néanmoins nous allons élargir notre esprit afin de construire une structure plus complexe basée sur la structure du groupe.

Définition 2.9.

*Un **anneau** (aussi appelé anneau unitaire) est un triplet $(\mathbb{A}, +, \cdot)$ où $(A, +)$ est un groupe commutatif et $\cdot$ est une loi de composition interne qui vérifie*

1. $\forall x, y, z \in \mathbb{A}, \quad x \cdot (y + z) = x \cdot y + x \cdot z.$ *(distributivité)*
2. $\exists \mathbb{1}_{\mathbb{A}}, \forall x \in \mathbb{A}, \quad \mathbb{1}_{\mathbb{A}} \cdot x = x \cdot \mathbb{1}_{\mathbb{A}} = x.$ *(élément neutre pour $\cdot$)*

*Si de plus la loi $\cdot$ est commutative dans $\mathbb{A}$ alors l'**anneau est commutatif**.*

Sauf mention contraire, les anneaux considérés sont tous commutatifs et différents de l'anneau nul $(\{0_A\}, +, \cdot)$. L'anneau est le seul anneau oùn les éléments neutres de la loi $+$ et $\cdot$ sont le même.

Exemple 2.5.

1. *Les triplets $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$sont des anneaux.*
2. *Soient f et g des fonctions numériques de $\mathbb{R}$ dans $\mathbb{R}$. On définit les lois $+$ et $\cdot$ pour l'ensemble des fonctions numériques de la manière suivante*

$$(f + g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x), \forall x \in \mathbb{R}.$$

Dans ce cas $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \cdot)$ est un anneau, l'élément neutre pour la loi $+$ est la fonction nulle $(\theta(x) = 0, \forall x \in \mathbb{R})$, est l'élément neutre pour $\cdot$ est la fonction constante $\mathbb{1}(x) = 1, \forall x \in \mathbb{R}$.

Définition 2.10.
On définit $\mathbb{A}^*$ comme l'ensemble des inversibles d'un anneau $(\mathbb{A}, +, \cdot)$ c'est à dire

$$\mathbb{A}^* = \left\{ y \in \mathbb{A}, \exists y^{-1} \in \mathbb{A} \qquad y \cdot y^{-1} = \mathbb{1}_{\mathbb{A}} \right\}.$$

Remarque 2.2. *On appelle $0_{\mathbb{A}}$ un élément **absorbateur** car pout tout $a \in (\mathbb{A}, +, \cdot)$* $0_{\mathbb{A}} \cdot a = a \cdot 0_{\mathbb{A}} = 0_{\mathbb{A}}$.

Définition 2.11. *On dit que $(\mathbb{A}, +, \cdot)$ est un anneau **intègre** si le seul élément absorbant est $0_{\mathbb{A}}$. Autrement dit*

$$x \cdot y = 0_{\mathbb{A}} \quad \Longrightarrow \quad x = 0_{\mathbb{A}} \quad \text{ou} \quad y = 0_{\mathbb{A}}.$$

Exemple 2.6.

1. *L'anneau $(\mathbb{Z}, +, \cdot)$ est intègre.*
2. *L'anneau de $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ n'est pas intègre car $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$.*

Nous avons déjà défini un homomorphisme entre groupes. On peut définir de la même façon un morphisme d'anneaux. Afin de ne pas trop embrouiller le lecteur par des symboles de lois compliqués on se contentera de noter $+$ pour la loi des groupes et $\cdot$ la deuxième loi de l'anneau même si les anneaux de départ et d'arrivée sont de natures différentes.

Définition 2.12.
Soit $(\mathbb{A}, +, \cdot)$ et $(\mathbb{B}, +, \cdot)$ deux anneaux. Un homomorphisme entre anneaux est une application $\psi : \mathbb{A} \longrightarrow \mathbb{B}$ telle que

1. $\psi(x + y) = \psi(x) + \psi(y), \quad \forall x, y \in \mathbb{A},$
2. $\psi(x \cdot y) = \psi(x) \cdot \psi(y), \quad \forall x, y \in \mathbb{A},$
3. $\psi(\mathbb{1}_{\mathbb{A}}) = \mathbb{1}_{\mathbb{B}}.$

Concernant le troisième point de la Définition 2.12, il n'est pas mentionné par redondance, en effet, on sait que ψ est un morphisme entre les groupes $(\mathbb{A}, +)$ et $(\mathbb{B}, +)$ ce qui permet d'assurer que $\psi(0_{\mathbb{A}}) = 0_{\mathbb{B}}$. Mais pour $(\mathbb{A}, \cdot)$ et $(\mathbb{B}, \cdot)$ ce ne sont pas forcément des groupes, ce qui oblige d'ajouter la troisième condition. La notion est très intéressante parce qu'elle permet des développements algébriques profonds mais aussi des constructions en arithmétique qui dépassent les objectifs de ce cours.

Définition 2.13. *Un **idéal** d'un anneau $\mathbb{A}$ est un sou-groupe I de $\mathbb{A}$ tel que :*

$$\forall x \in I, \forall x \in \mathbb{A}, \qquad a \cdot x \in I.$$

Proposition 2.3

L'intersection d'idéaux est un idéal.

Démonstration. Soit un (I_i) $(i = 1 \dots n)$ une famille d'idéaux d'un anneau $\mathbb{A}$. Posons $I = \cup_{i=1}^{n} I_i$ et soit $x \in I$. Donc x appartient à chacun des I_i. Pour un élément $a \in \mathbb{A}$, on remarque que $a \cdot x \in I_i$ car chaque I_i est un idéal. Par conséquent $a \cdot x \in \cup_{i=1}^{n} I_i = I$, c'est à dire que I est un idéal. □

Proposition 2.4

Si $\psi : \mathbb{A} \longrightarrow \mathbb{B}$ est un homomorphisme d'anneaux commutatifs alors $\ker \psi$ est un idéal de $\mathbb{A}$.

Démonstration. Soit $x \in \ker \psi = \{z \in \mathbb{A}, \quad \psi(z) = 0_{\mathbb{B}}\}$ et $a \in \mathbb{A}$. On a

$$\psi(a \cdot x) \underbrace{=}_{\text{morphisme d'anneaux}} \psi(a) \cdot \psi(x) \underbrace{=}_{x \in \ker \psi} \psi(a) \cdot 0_{\mathbb{B}} \underbrace{=}_{0_{\mathbb{B}} \text{ absorbant}} 0_{\mathbb{B}}.$$

Donc $a \cdot x \in \ker \psi$, alors $\ker \psi$ est un idéal. □

Définition 2.14.
Un sous-anneau d'un anneau commutatif $(\mathbb{A}, +, \cdot)$ est une partie de $\mathbb{A}$ stable par addition, par multiplication et contenant l'élément unité de $\mathbb{A}$; c'est un sous-groupe de $(A, +)$ et c'est un anneau.

Un idéal d'un anneau n'est pas un sous-anneau sauf s'il contient l'élément $1_{\mathbb{A}}$.

Exemple 2.7.

1. *Les idéaux de $\mathbb{Z}$ sont les ensembles de la forme $n\mathbb{Z}$ où*

$$n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, 3n, \dots\}.$$

2.

On est habitué à l'utilisation de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. En effet ce sont ces deux structures il y a quelque chose qui les distingue. C'est le fait que tous ces éléments non nuls admettent un inverse.

Définition 2.15. *Soit $(\mathbb{A}, +, \cdot)$ un anneau commutatif. Si $\mathbb{K}^* = \mathbb{K} \setminus \{0_{\mathbb{A}}\}$ alors $\mathbb{K}$ est **un corps**.*

Comme déjà expliqué, un corps est tout simplement un anneau où tous les éléments sont inversibles sauf l'élément neutre pour l'addition.

Exemple 2.8.

1. *On connaît les corps infinis comme* $\mathbb{Q}, \mathbb{R}$ *et* $\mathbb{C}$*.*
2. *Il existe aussi des corps finis. Par exemple, les anneaux* $\mathbb{Z}/p\mathbb{Z}$ *pour* p *premier.*

Les corps finis ayant un nombre d'éléments égal à une puissance de 2 sont très utilisés dans les problèmes d'informatique, de transport de l'information et de cryptographie.

Bibliographie

[1] M. Artin. *Algebra*. Pearson Modern Classics for Advanced Mathematics Series. Pearson, 2017.

[2] Thomas Scott Blyth, Thomas Scott Blyth, and EF Robertson. *Algebra Through Practice : Volume 5, Groups : A Collection of Problems in Algebra with Solutions*. CUP Archive, 1985.

[3] Thomas Scott Blyth, Thomas Scott Blyth, and EF Robertson. *Algebra Through Practice : Volume 6, Rings, fields and modules : A Collection of Problems in Algebra with Solutions*. CUP Archive, 1985.

[4] Shahriar Shahriar. *Algebra in Action : A Course in Groups, Rings, and Fields*, volume 27. American Mathematical Soc., 2017.

[5] John B Fraleigh. *A first course in abstract algebra*. Pearson Education India, 2003.

[6] Jean-Pierre Escofier. *Toute l'algèbre de la Licence-4e éd. : Cours et exercices corrigés*. Dunod, 2016.