Licence 1 Sciences & Technologies

Algèbre - Semestre 2

Université du Littoral - Côte d'Opale, La Citadelle

Laurent SMOCH

Janvier 2009

Laboratoire de Mathématiques Pures et Appliquées Joseph Liouville
Université du Littoral, zone universitaire de la Mi-Voix, bâtiment H. Poincarré
50, rue F. Buisson, BP 699, F-62228 Calais cedex

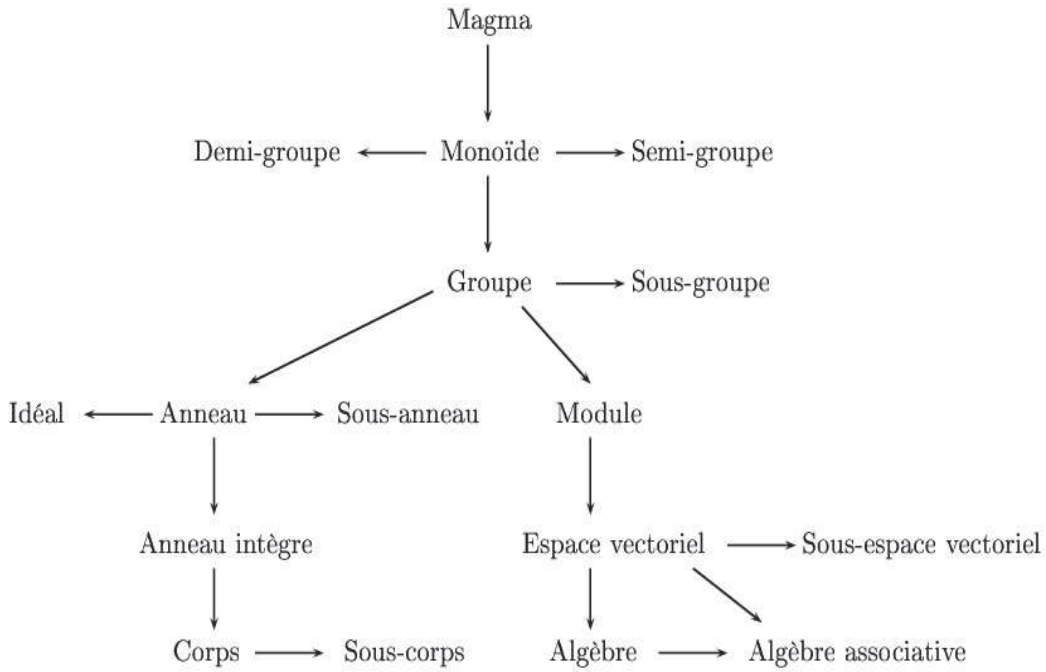
Table des matières

Chapitre 2

Les structures algébriques

2.1 Introduction

Dans la théorie des ensembles, l'objet principal est un ensemble qui se dissimule parfois sous d'autres noms tels que classe, collection ou famille. Cependant, dans d'autres disciplines des mathématiques, un ensemble est toujours muni d'une structure. En algèbre tout particulièrement, un ensemble est combiné avec une ou plusieurs lois de composition et s'appelle une structure algébrique. Voici une liste des structures algébriques importantes :



Tout en haut du diagramme, on trouve les structures algébriques impliquant un nombre minimal de contraintes et en bas, celles qui en impliquent un maximum. Plus on descend, plus la structure est en quelque sorte spécialisée.
Les structures les plus communes sont les groupes, les anneaux et les corps.

2.2 Magmas et monoïdes

2.2.1 Les magmas

Introduisons dans un premier temps une structure algébrique élémentaire : le magma.

Définition 2.2.1 *Un ensemble E muni d'une loi de composition interne T est appelé* ***magma*** *et est noté (E,T).*

Un magma est donc une structure algébrique élémentaire. Il existe des structures plus subtiles dans lesquelles un ensemble est muni de plusieurs lois et de différentes propriétés.

Définition 2.2.2 *Soit A une partie non vide d'un magma (E,T). On dira que A est* ***stable*** *pour la loi T ou que A est une* ***partie stable*** *de E (lorsqu'il n'y a pas d'ambigüité sur la loi en cause) si la restriction à A de la loi T est une loi de composition interne dans A. Autrement dit :*

$$A \subset E,\ A \text{ stable pour la loi } T \Leftrightarrow \forall (a,b) \in A \times A,\ aTb \in A$$

On peut donc remarquer que dire qu'une loi T est une loi de composition interne dans un ensemble E équivaut à dire que E est stable pour cette loi. En revanche, si A est un sous-ensemble de E, il n'est pas certain que A soit stable pour la loi T. Ainsi $\mathbb{N}$ n'est pas stable pour la soustraction, mais $\mathbb{Z}$ l'est. De même, $\mathbb{Z}^\star$ n'est pas stable pour l'inverse, mais $\mathbb{Q}^\star$ l'est.

Définition 2.2.3 *Si, pour tout couple (x,y) d'éléments de E, on a $xTy = yTx$, la loi T est dite* ***commutative****. (E,T) est dit* ***commutatif****.*

Remarque 2.2.1

- Les magmas $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{Z},\times)$ sont commutatifs. Ce n'est pas le cas de $(\mathbb{Z},-)$: $3-2=1$ alors que $2-3=-1$. De même, $(\mathbb{Q}-\{0\},/)$, ensemble des nombres rationnels non nuls muni de la division usuelle n'est pas commutatif : $3/2 \neq 2/3$.
- Lorsqu'une loi n'est pas commutative, certains éléments peuvent cependant "commuter" : on parle d'éléments **permutables**. Il suffit pour s'en convaincre de considérer la loi "o" de composition des applications et les fonctions $f : x \mapsto 3x+2$ et $g : x \mapsto 2x+1$.
- Dans un magma associatif (E,T), un élément x permutable avec deux éléments a et b est permutable avec le composé aTb.
  Si la loi T n'est pas associative, le résultat peut ne plus être vrai : dans $(\mathbb{Z},T)$ avec $aTb = a^2 - 2b$, 3 et -5 commutent donc 3 commute avec 3 et -5 mais 3 ne commute pas avec $19 = 3T(-5)$; en effet $3T19 = -29$ et $19T3 = 355$.

Définition 2.2.4 *Un élément e de E vérifiant $xTe = eTx = x$ est dit* ***neutre*** *pour la loi T. Le magma (E,T) muni de cet élément neutre est dit* ***unifère*** *(ou parfois* ***unitaire****).*

Exemple 2.2.1

- Dans les magmas $(\mathbb{N},+)$ et $(\mathbb{Z},+)$, "0" est neutre, c'est-à-dire que pour tout entier naturel ou tout entier relatif n, $n+0=0+n=n$.
- Dans $(\mathbb{Z},-)$, 0 n'est neutre qu'à droite : $x-0=x$ mais $0-x=-x$.
- Dans $\mathbb{N}$ et $\mathbb{Z}$, "1 " est neutre pour la multiplication.
- Dans $\mathcal{M}_2(\mathbb{R})$, ensemble des matrices carrées d'ordre 2 à termes réels, la matrice $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est neutre pour la multiplication.

Remarque 2.2.2 Un magma peut admettre plusieurs éléments neutres d'un "même" côté (à droite : $aTe = a$, ou à gauche : $eTa = a$). Par exemple, dans $(\mathbb{Z},T)$ où T désigne la loi définie par $aTb = a + E(b/3)$ les entiers 0, 1 et 2 sont neutres à droite et il n'y a pas d'élément neutre à gauche.

Proposition 2.2.1 *Un élément neutre à gauche et à droite est unique : c'est l'élément neutre du magma (E,T).*

Preuve : Supposons que (E,T) admette deux éléments neutres distincts e_1 et e_2 à gauche et à droite respectivement. On a d'une part $\forall x \in E$, $e_1 T x = x$, cette relation est donc vraie pour $x = e_2$ ce qui nous permet d'affirmer que $e_1 T e_2 = e_2$. D'autre part $\forall x \in E$, $x T e_2 = x$, cette relation étant vraie pour $x = e_1$, on a $e_1 T e_2 = e_1$. Par conséquent, $e_1 = e_2$ ■

Définition 2.2.5 *Si un élément b de E vérifie $aTb = bTa = b$, $\forall a \in E$, alors b est dit* ***élément absorbant*** *pour la loi T.*

2.2.2 Les monoïdes

Définition 2.2.6 *Si, pour tout triplet (x,y,z) d'éléments de E, on a $(xTy)Tz = xT(yTz)$, la loi T est dite* ***associative****. Le magma (E,T) est dit* ***associatif****.*

Un monoïde est un magma associatif et unifère

Remarque 2.2.3
- Si la loi interne est en plus commutative, nous disons alors que la structure forme un **monoïde commutatif**.
- Un **demi-groupe** est un magma associatif. Le monoïde est donc un demi-groupe muni d'un élément neutre.

Exercice 35 Montrer que l'ensemble des entiers naturels est un monoïde commutatif totalement ordonné par rapport aux lois d'addition et de multiplication.
Correction :

1. La loi d'addition $+$ est-elle une opération interne telle que $\forall a, b \in \mathbb{N}$ nous ayons $a + b = c \in \mathbb{N}$? Nous pouvons démontrer que c'est bien le cas en sachant que 1 appartient à $\mathbb{N}$ tel que $\sum_{i=1}^{a} 1 + \sum_{i=1}^{b} 1 = \sum_{i=1}^{a+b} 1$.
   Donc $c \in \mathbb{N}$ et l'addition est bien une loi interne (l'ensemble est stable par rapport à l'addition) et en même temps associative puisque 1 peut être additionné à lui-même par définition dans n'importe quel ordre sans que le résultat en soit altéré.
   La multiplication est une loi qui se construit sur l'addition donc la loi de multiplication $\times$ est aussi une loi interne et associative.
2. On admettra à partir d'ici qu'il est trivial que la loi d'addition est également commutative et que le "0" en est l'élément neutre e.
   La loi de multiplication est aussi commutative et il est trivial que "1" en est l'élément neutre e.
3. Pour conclure, on rappelle les résultats suivants :
   - $(\mathbb{N}, \leq, \geq)$ est totalement ordonné (attention cette notation est un peu abusive, il suffit qu'il y ait juste une des deux relations d'ordre $\mathcal{R}$ pour que l'ensemble soit totalement ordonné).
   - $(\mathbb{N}, +)$ et $(\mathbb{N}, \times)$ sont des monoïdes abéliens.

Conclusion, $\mathbb{N}$ est un monoïde abélien totalement ordonné par rapport aux lois d'addition et de multiplication.

Remarque 2.2.4 Il est rare d'utiliser les monoïdes car souvent, lorsque nous nous trouvons face à une structure trop pauvre pour pouvoir vraiment discuter, nous la prolongeons vers quelque chose de plus riche, comme un groupe, ou un anneau (voir plus loin).

Exemple 2.2.2
- Le magma $(\mathbb{Z}, +)$ est associatif et unifère (l'élément neutre étant dans ce cas 0) donc $(\mathbb{Z}, +)$ est un monoïde.

- Ce n'est pas le cas de $(\mathbb{Z}, -)$. En effet, $(\mathbb{Z}, -)$ est un magma non unifère et non associatif car, par exemple, $(3-2)-5=-4$ alors que $3-(2-5)=6$. Ce n'est pas le cas non plus de $(\mathbb{Q}-\{0\}, /)$, il suffit de considérer pour s'en convaincre l'exemple suivant : $(3/2)/5 = 3/10$ alors que $3/(2/5) = 15/2$.
- La loi de composition des applications est associative.
- Le produit vectoriel $\wedge$ (à ne pas confondre avec le "et " logique) n'est pas associatif : par exemple, si (i, j, k) est une base orthogonale $(i \wedge i) \wedge j = 0 \wedge k = 0$ alors que $i \wedge (i \wedge j) = i \wedge k = -j$.

Définition 2.2.7 *Dans un magma unifère (E, T) d'élément neutre e, un élément x est dit* ***symétrisable***
- *à droite : s'il existe x' dans E tel que $xTx' = e$,*
- *à gauche : s'il existe $x"$ dans E tel que $x"Tx = e$.*

Lorsque l'élément est symétrisable à gauche et à droite (bilatère) et si $x' = x"$, on a alors :

$$x'Tx = xTx' = e$$

Dans ce cas, x et x' sont dits ***symétriques*** *pour la loi T de E. On dit aussi que x' (respectivement x) est un symétrique de x (respectivement x'). Lorsque la loi T s'interprète comme une multiplication, on parle plutôt d'éléments* ***inversibles*** *et d'****inverses****.*

Remarque 2.2.5
- Dans $(\mathbb{Z}, -)$, 0 est neutre à droite et tout entier relatif est son propre et unique symétrique à droite.
- Dans $(\mathbb{Z}, +)$, tout entier relatif x possède un unique symétrique : son **opposé** $-x$.

Exercice 36 Montrer que les lois d'addition et de multiplication de l'ensemble des entiers naturels n'admettent pas de symétrique.

Correction : Existe-t-il pour la loi d'addition $+$ un symétrique $c \in \mathbb{N}$ tel que $\forall a \in \mathbb{N}$ nous ayons $a + c = \left(\sum_{i=1}^{a} 1\right) + c = e = 0$? Il est assez trivial que pour que cette égalité soit satisfaite on ait $\left(\sum_{i=1}^{a} 1\right) = -c \Leftrightarrow a = -c$ or les nombres négatifs n'existent pas dans $\mathbb{N}$. Ce qui nous amène aussi à la conclusion que la loi d'addition $+$ n'a pas de symétrique et que la loi de soustraction $-$ n'existe pas dans $\mathbb{N}$ (la soustraction étant rigoureusement l'addition d'un nombre négatif).

Existe t-il pour la loi de multiplication $\times$ un symétrique $a' \in \mathbb{N}$ tel que $\forall a \in \mathbb{N}$, on ait $a' \times a = e = 1$? D'abord il est évident que $a' = \dfrac{1}{a}$. Mais excepté pour $a = 1$, le quotient $1/a$ n'existe pas dans $\mathbb{N}$. Donc nous devons conclure qu'il n'existe pas pour tout élément de $\mathbb{N}$ de symétriques pour la loi de multiplication et ainsi que la loi de division n'existe pas dans $\mathbb{N}$.

Définition 2.2.8 *Dans un magma (E, T), un élément x est dit* ***régulier*** *(ou* ***simplifiable)*** ***à gauche*** *si pour tout couple (a, b) d'éléments de E tels que $xTa = xTb$, alors $a = b$. On définit de même un élément* ***régulier à droite****. Un élément est dit* ***régulier*** *s'il est régulier à droite et à gauche. Si T est commutative, les notions d'élément régulier à gauche et à droite coïncident.*

Exemple 2.2.3
- Dans $(\mathbb{N}, +)$, tout élément est régulier et dans $(\mathbb{N}, \times)$, tout élément non nul est régulier.
- Dans $(\mathbb{Z}, T)$, avec $aTb = |a| + b$, tout élément est régulier à gauche mais pas à droite.

Remarque 2.2.6
- Dans un magma associatif, le composé de deux éléments réguliers est régulier.
- Dans un magma associatif, tout élément symétrisable est régulier.
- Si le magma n'est pas associatif, rien n'est assuré.

Exercice 37 (*non corrigé*) On considère E l'ensemble des entiers naturels au plus égaux à 10 et la loi T définie dans E par $aTb = |a - b|$ (différence symétrique).

- Montrer que 0 est neutre et que tout élément est son propre symétrique.
- Montrer que seuls 0 et 10 sont réguliers.
- Montrer que T est non associative en considérant $(1T2)T3$ et $1T(2T3)$

Exercice 38 (*non corrigé*) On considère dans $\mathbb{Z}$ la loi T définie par $aTb = ab + 3$. Montrer que T n'est pas associative, que -1 et 3 sont réguliers mais que $-1T3 = 0$.

2.3 Les groupes

2.3.1 Les groupes

Le terme est de Évariste GALOIS (1811-1832), la structure est de Augustin Louis CAUCHY (1789-1857), l'axiomatisation de Arthur CAYLEY (1821-1895).

Définition 2.3.1 *Un groupe G est un ensemble muni d'une loi de composition interne T pour laquelle les axiomes suivants sont vérifiés :*

- $\boxed{g_1}$ *la loi T est associative : $(xTy)Tz = xT(yTz)$ pour tout x, y et z de G,*
- $\boxed{g_2}$ *la loi T possède un élément neutre e : $xTe = eTx = x$ pour tout x de G,*
- $\boxed{g_3}$ *tout élément x de G possède un symétrique x' pour la loi T : $xTx' = x'Tx = e$.*

Le groupe G muni de sa loi T est souvent noté (G, T).

Un groupe est un magma unifère associatif dans lequel tout élément admet un symétrique

Un groupe est un monoïde dans lequel tout élément admet un symétrique

Exercice 39 Soit G un ensemble muni d'une loi de composition interne "T" associative, qui possède un élément neutre à droite e (i.e. pour tout x de G, $xTe = x$) et tel que tout élément x possède un symétrique à droite x' (i.e. $xTx' = e$). Montrer que G est un groupe.
Correction : Soit $x \in G$, de symétrique à droite x'. Par conséquent $x'Tx$ est un élément de G (lci), il possède donc un symétrique à droite que l'on note z. On a donc $xT((x'Tx)Tz) = x \Rightarrow (xTx')TxTz = x \Rightarrow eTxTz = xTz = x$, par associativité de la loi. On compose ensuite à gauche par x', pour trouver $x'T(xTz) = (x'Tx)Tz = e = x'Tx$, ce qui permet d'affirmer que x' est également un symétrique à gauche de x. On en déduit ensuite que e est aussi neutre à gauche, car si x est dans G, $eTx = (xTx')Tx = xT(x'Tx) = xTe = x$ (on a utilisé à nouveau l'associativité de la loi et le fait que e est un symétrique à droite).

Exercice 40

1. $(\mathbb{N}, +)$ et $(\mathbb{N}, \times)$ sont-ils des groupes ?
2. $(\mathbb{Z}, +)$ et $(\mathbb{Z}, \times)$ sont-ils des groupes ?
3. $(\mathbb{R}, +)$ et $(\mathbb{R}, \times)$ sont-ils des groupes ?

Correction : On vérifie pour chacun des couples les propriétés du groupe $\boxed{g_1}$, $\boxed{g_2}$ et $\boxed{g_3}$.

2.a. Pour $(\mathbb{Z}, +)$:
- $\forall (x, y) \in \mathbb{Z}^2$, $x + y \in \mathbb{Z}$, la loi est donc interne (*magma*),
- $\forall x \in \mathbb{Z}$, $x + 0 = 0 + x = x$. "0" est l'élément neutre (*unifère*),
- $\forall (x, y, z) \in \mathbb{Z}^3$, $(x + y) + z = x + (y + z)$, la loi $+$ est associative dans $\mathbb{Z}$ (*associatif*),
- $\forall x \in \mathbb{Z}$, $\exists x' = -x$, $x + x' = 0$, *tous les éléments ont un symétrique.*

$(\mathbb{Z}, +)$ est donc un groupe.

3.a. On démontre de même que $(\mathbb{R}, +)$ est un groupe.

Par contre :

1.a. les éléments de $\mathbb{N}$ n'ont pas d'opposé (sauf 0),

1.b. les éléments de $\mathbb{N}$ n'ont pas d'inverse (sauf 1),

2.b. les éléments de $\mathbb{Z}$ n'ont pas d'inverse (sauf 1 et -1),

3.b. 0 n'a pas d'inverse,

donc $(\mathbb{N},+)$, $(\mathbb{N},\times)$, $(\mathbb{Z},\times)$ et $(\mathbb{R},\times)$ n'ont pas de structure de groupe, ce sont néanmoins des monoïdes.

Définition 2.3.2 *Un groupe dont la loi de composition possède des caractéristiques semblables à celle de l'addition (respectivement la multiplication) dans $\mathbb{Z}$ (respectivement dans $\mathbb{R}^\star$) est dit* ***additif*** *(respectivement* ***multiplicatif****).*

Définition 2.3.3 *Un groupe G est dit* ***abélien*** *(du nom de Niels Henrick ABEL, 1802-1829) ou* ***commutatif*** *si sa loi de composition interne T est commutative c'est-à-dire si $xTy = yTx$, $\forall x, y \in G$.*

Exemple 2.3.1

- L'addition dans $\mathbb{Z}$ et dans $\mathbb{R}$ est commutative. Ce n'est pas le cas de la soustraction : $2-5 \neq 5-2$. Dans $(\mathbb{Z},-)$, 0 n'est neutre qu'à droite.
- $(\mathbb{Z},+)$ est un groupe abélien, de même $(\mathbb{R}-\{0\},\times)$. Par contre, $(\mathbb{R}-\{0\},/)$ ne l'est pas car la division n'est pas associative ($(2/3)/4 = 1/6$ et $2/(3/4) = 8/3$) ni commutative ($5/4 = 1,25$ et $4/5 = 0,8$).
- $(\mathbb{Z},-)$ n'est pas un groupe : la soustraction est une loi de composition interne dans $\mathbb{Z}$, mais elle n'est pas associative : $(2-3)-5 \neq 2-(3-5)$. C'est cependant un magma.
- Si $\mathcal{A}(\mathbb{R})$ désigne l'ensemble des fonctions affines bijectives de $\mathbb{R}$ sur $\mathbb{R}$ soit l'ensemble des fonctions de la forme $x \mapsto ax+b$ avec a non nul, $(\mathcal{A}(\mathbb{R}),\mathrm{o})$ est un groupe non abélien (o : loi de composition des applications). Si f désigne $x \mapsto 2x-1$ et si g désigne $x \mapsto 3x$, on a $f_o g : x \mapsto 6x-1$ et $g_o f : x \mapsto 6x-3$.
- Si $\mathcal{M}_2(\mathbb{R})$ désigne l'ensemble des matrices carrées réelles d'ordre 2 de déterminant non nul, $(\mathcal{M}_2(\mathbb{R}),\times)$ est un groupe multiplicatif non abélien.
- L'ensemble constitué des homothéties de rapport non nul et des translations dans un plan P, muni de la loi de composition des applications, est un groupe non commutatif. Son élément neutre est l'application identique assimilé à la translation de vecteur nul ou à l'homothétie de rapport 1.
- Dans un plan P, considérons un carré $ABCD$ de centre O. Notons S_0 la symétrie centrale par rapport à O, S_1 la symétrie d'axe d_1 passant par les milieux des côtés $[AD]$ et $[BC]$, S_2 la symétrie d'axe d_2 passant par les milieux des côtés $[AB]$ et $[CD]$ et i l'application identique de P. Muni de la loi de composition des applications, l'ensemble $E = \{i, S_0, S_1, S_2\}$ est un groupe commutatif.

Exercice 41 Décrire tous les groupes possibles à 1, 2, 3 ou 4 éléments.

Correction :

1. Un groupe à un élément est un ensemble E constitué d'un seul élément e, et la loi $\star$ est nécessairement définie par $e \star e = e$. On vérifie sans difficulté que $(E,\star)$ est bien un groupe.
2. Si E contient deux éléments, l'un doit être le neutre pour $\star$, notons le e et notons l'autre x. On a donc $e \star e = e$ et $e \star x = x \star e = x$. Si l'on veut de plus que x soit inversible, on doit nécessairement avoir $x \star x = e$, et on vérifie que $(E,\star)$ est alors un groupe.
3. Ajoutons un troisième élément y à notre ensemble, on a nécessairement $e \star e = e$, $e \star x = x \star e = x$ et $e \star y = y \star e = y$. On ne peut avoir $x \star y = y$ $(x \neq e)$ ni $x \star y = x$ $(y \neq e)$ donc $x \star y = e$ (lci). On montre de la même manière que $y \star x = e$. On ne peut pas avoir $x \star x = x$ $(x \neq e)$ ni $x \star x = e$ (car l'inverse de x est unique dans un groupe et on sait qu'il vaut y). Par conséquent, $x \star x = y$ (lci) et on montre de la même manière que $y \star y = x$. On a donc les résultats suivants :

$\star$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Cette loi est bien une loi de groupe.

4. Enfin, dans le cas de quatre éléments, on obtient en étudiant toutes les possibilités les quatre lois suivantes :

$\star$	e	x	y	z
e	e	x	y	z
x	x	y	z	e
y	y	z	e	x
z	z	e	x	y

$\star$	e	x	y	z
e	e	x	y	z
x	x	z	e	y
y	y	e	z	x
z	z	y	x	e

$\star$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

$\star$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	x	e
z	z	y	e	x

Théorème 2.3.1 *Tout élément d'un groupe (G,T) est régulier.*

Preuve : Vu que T est associative et que tout élément x admet un symétrique x', si e est l'élément neutre pour la loi T, $\forall (a,b) \in G^2$, $xTa = xTb \Rightarrow x'T(xTa) = x'T(xTb) \Rightarrow (x'Tx)Ta = (x'Tx)Tb \Rightarrow eTa = eTb \Rightarrow a = b$. (G,T) est régulier à gauche et on montre de la même façon que ce groupe est régulier à droite. ■

Théorème 2.3.2 *Dans un groupe (G,T), tout élément admet toujours un unique élément symétrique.*

Preuve : L'existence du symétrique est justifiée par la définition, il reste à prouver l'unicité. Supposons que $\forall x \in E$, $\exists x', x'' \in E,\ x' \neq x''$, $x'Tx = x''Tx (= e) \Leftrightarrow x' = x''$ pusique $x \in G$ est régulier (à droite). ■

Exercice 42 (*non corrigé*) Démontrer que si $(E,\star)$ est un groupe d'élément neutre e, dans lequel tout élément est **involutif** (c'est-à-dire $x \star x = e$), alors ce groupe est commutatif.
Généralement, l'unique élément symétrique de x est noté x^{-1}. On a

Propriété 2.3.1

- $e^{-1} = e$. *L'élément neutre est son propre symétrique, il est involutif.*
- $(x^{-1})^{-1} = x$.
- $(xTx')^{-1} = x'^{-1}Tx^{-1}$. *Le symétrique d'un produit est le produit inverse des symétriques.*
- *Plus généralement* $(x_1Tx_2T\dots Tx_n)^{-1} = x_n^{-1}Tx_{n-1}^{-1}T\dots Tx_1^{-1}$.

En particulier on a $(x^n)^{-1} = (x^{-1})^n$, $(n \in \mathbb{N}^\star)$. On note alors $x^{-n} := (x^n)^{-1}$ ce qui permet de définir x^m pour $m \in \mathbb{Z}$ en convenant $x^0 = e$. Dans ces conditions on a les relations.

$$(x^m)^{m'} = x^{mm'} \text{ et } x^mTx^{m'} = x^{m+m'},\ \forall m, m' \in \mathbb{Z}.$$

2.3.2 Les sous-groupes

Définition 2.3.4 *Un **sous-groupe** est une partie S d'un groupe (G,T) qui, munie de la loi T de G, est aussi un groupe.*

Proposition 2.3.1 *Un sous-ensemble H de (G,T) est un sous-groupe si et seulement si il contient e (élément neutre de (G,T)) et est stable par produit et passage à l'inverse.*

Preuve : Si un sous-ensemble de G vérifie ces trois propriétés, c'est bien un sous-groupe.
Réciproquement, si H est un sous-groupe, il possède un élément neutre e_0. Soit alors x un élément de H, on a $xTe_0 = x = xTe$ (la première loi est prise dans H, la deuxième dans G), donc $e_0 = e$ par simplification. De même, l'inverse de x dans H est nécessairement un inverse dans G également, donc il s'agit de l'unique inverse de x par T, et H est stable par inversion. Enfin, H doit clairement être stable par produit. ■

Proposition 2.3.2 *Une partie H non vide de G, contenant e, est un sous-groupe de (G,T) si et seulement si*

1. $\forall x, y \in H, xTy \in H$
2. $\forall x \in H, x^{-1} \in H$

Les deux conditions précédentes peuvent être remplacées par la suivante :

$$\forall x, y \in H, xTy^{-1} \in H$$

Remarque 2.3.1 La notation $H < G$ est employée pour dire H est sous-groupe de G. Lorsqu'on n'exclut pas la possibilité que H soit égal à G on écrit $H \leq G$.

Exercice 43 (*non corrigé*) Montrer que
- dans le groupe multiplicatif $(\mathbb{C}, \times)$ des nombres complexes, l'ensemble des nombres de module 1 est un sous-groupe de $\mathbb{C}$,
- dans le groupe additif $(F, +)$ des fonctions numériques, l'ensemble des fonctions linéaires $x \mapsto ax$ est un sous-groupe de F.

Exercice 44 Soit $n \in \mathbb{N}$. On note $n\mathbb{Z}$ l'ensemble des entiers relatifs de la forme nx, $x \in \mathbb{Z}$. Montrer que $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$.
Correction : Soit $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\} = \{\ldots, -2n, n, 0, n, 2n, \ldots\}$.
- Soit $(x_1, x_2) \in (n\mathbb{Z})^2$, $\exists (k_1, k_2) \in \mathbb{Z}^2$, $x_1 = nk_1$, $x_2 = nk_2 \Rightarrow x_1 + x_2 = n(k_1 + k_2) \Rightarrow x_1 + x_2 \in n\mathbb{Z}$ donc la loi est interne.

(- Soit $(x_1, x_2, x_3) \in (n\mathbb{Z})^3$, $\exists (k_1, k_2, k_3) \in \mathbb{Z}^3$, $x_1 = nk_1$, $x_2 = nk_2$, $x_3 = nk_3$. Or $(x_1 + x_2) + x_3 = (nk_1 + nk_2) + nk_3 = nk_1 + (nk_2 + nk_3) = x_1 + (x_2 + x_3)$ donc la loi est associative.)

(- $0_{\mathbb{Z}} = 0_{n\mathbb{Z}} = 0$. En effet, si $x \in n\mathbb{Z}$, $x + 0 = 0 + x = x$.)
- Soit $x \in n\mathbb{Z}$, $\exists k \in \mathbb{Z}$, $x = nk$. $\exists x' = n(-k) \in n\mathbb{Z}$, $x \times x' = n(k - k) = 0$ donc tout élément possède un symétrique.

Conclusion, $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$.

Exercice 45 Montrer que l'ensemble des racines n-ièmes de l'unité forment un sous-groupe de $(\mathbb{U}, \times)$.
Correction : On constate dans un premier temps que l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité est un sous-ensemble de $\mathbb{U}$. En effet, si $z^n = 1$, on a en particulier $|z|^n = 1$, donc $|z| = 1$ (dans $\mathbb{R}^+$, l'équation $x^n = 1$ a une seule solution). Ensuite, il reste à faire les vérifications élémentaires : $\mathbb{U}_n$ contient 1, $\mathbb{U}_n$ est stable par

produit (si $z^n = z'^n = 1$, alors $(zz')^n = z^n z'^n = 1$) et par inverse (si $z^n = 1$, $\frac{1}{z^n} = 1$), donc c'est bien un sous-groupe multiplicatif de $\mathbb{U}$.

Exercice 46 On considère l'ensemble constitué des six fonctions de $\mathbb{R} - \{0, 1\}$ dans lui-même suivantes :

$$f_1(x) = x, \quad f_2(x) = \frac{1}{1-x}, \quad f_3(x) = \frac{x}{x-1}, \quad f_4(x) = \frac{1}{x}, \quad f_5(x) = 1 - x, \quad f_6(x) = \frac{x-1}{x}.$$

Montrer qu'il s'agit d'un groupe pour la composition (écrire sa table). Déterminer tous ses sous-groupes.
Correction : Le plus simple est de faire un tableau de loi :

o	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_6	f_4	f_5	f_3	f_1
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_3	f_2	f_1	f_6	f_5
f_5	f_5	f_4	f_6	f_2	f_1	f_3
f_6	f_6	f_1	f_5	f_3	f_4	f_2

Pour obtenir tous les sous-groupes, le plus simple est de les construire petit à petit. On connaît les sous-groupes triviaux : le groupe G tout entier et le sous-groupe réduit à l'élément neutre. Par ailleurs, tout sous-groupe contient f_1 qui est le neutre. Si on cherche un sous-groupe contenant f_1 et f_2, on voit que pour être stable par "o" il doit aussi contenir $f_2 \circ f_2 = f_6$. On constate que $\{f_1, f_2, f_6\}$ est un troisième sous-groupe de G. Par contre si on ajoute f_3, f_4 ou f_5 à f_1 et f_2, on est obligé pour avoir stabilité d'ajouter toutes les autres fonctions. Remarquons ensuite que $\{f_1, f_3\}$ est un sous-groupe de G, mais que si on y ajoute une troisième fonction, on va à nouveau retomber sur le sous-groupe trivial G. De même, $\{f_1, f_4\}$ et $\{f_1, f_5\}$ sont des sous-groupes, et on n'en obtient pas d'autres. Le groupe G a donc un sous-groupe à un élément, trois sous-groupes à deux éléments et un à trois éléments, et lui-même est un sous-groupe à six éléments.

Proposition 2.3.3 *Si (G, T) est un groupe, si H et K sont deux sous-groupes de G, alors $H \cup K$ est un sous-groupe de G si et seulement si $H \subseteq K$ ou $K \subseteq H$.*

Preuve : Soient H et K deux sous-groupes de G tels que $H \cup K$ soit un sous-groupe de G. Nous devons prouver qu'un des deux sous-groupes H ou K est contenu dans l'autre. Supposons que H ne soit pas contenu dans K et prouvons que K est contenu dans H. Soit k un élément de K. Il s'agit de prouver que k appartient à H. Puisque H n'est pas contenu dans K, il existe $h \in H$ tel que $h \notin K$. Puisque $H \cup K$ est un sous-groupe de G, nous avons $hTk \in H \cup K$. D'autre part, puisque $h \notin K$ et $k \in K$, nous avons $hTk \notin K$, donc $hTk \in H$, d'où $k \in H$ ce qui prouve que $K \subseteq H$.
La réciproque est évidente : si par exemple, $H \subseteq K$, $H \cup K = K$ et $H \cup K$ est naturellement un sous-groupe.■

Remarque 2.3.2 $H \cup K$ n'est pas en général un sous-groupe de G. Par exemple, soient H la droite d'équation $y = 0$ et K la droite d'équation $x = 0$ dans $\mathbb{R}^2$, groupe additif. Alors H et K sont des sous-groupes de $(\mathbb{R}^2, +)$ mais pas $H \cup K$ car $(1, 0) + (0, 1) = (1, 1)$ n'appartient pas à $H \cup K$.

Proposition 2.3.4 *Soient (G, T) un groupe et F une famille non vide de sous-groupes de G (F peut contenir un nombre fini ou infini de sous-groupes). Si I est l'intersection de tous les éléments de F, autrement dit $I = \cap_{H \in F} H$ alors I est lui-même un sous-groupe de G.*

Preuve : Considérons sans perte de généralité l'intersection $I = H \cap K$ de deux sous-groupes H et K. $H \cap K$ n'est pas vide car e appartient à $H \cap K$. Soient x et y appartenant à $H \cap K$. Comme H et K sont des sous-groupes de G, xTy^{-1} appartient à H et à K donc à $H \cap K$. D'où, $H \cap K$ est un sous-groupe de G. La démonstration se généralise à un nombre fini ou infini de sous-groupes. ■

Définition 2.3.5 *Soit (G,T) un groupe et A un sous-ensemble non vide de G. On appelle* ***sous-groupe engendré*** *par A le sous-groupe $< A >= \cap_{H \in S} H$ où S est l'ensemble de tous les sous-groupes de G qui contiennent A. Si g appartient à G, on note $< g >$ à la place de G.*

Cet ensemble n'est pas vide car il contient A lui-même et la formule ci-dessus est par conséquent bien définie.

Exemple 2.3.2 $< m >= m\mathbb{Z}$, $< G >= G$, $< m, n >= pgcd(m,n)\mathbb{Z}$ sont des sous-groupes engendrés.

Théorème 2.3.3 *Le sous-groupe $< A >$ est le plus petit sous-groupe (au sens de l'inclusion) de G contenant A. Autrement dit, $< A >$ est caractérisé par les deux conditions suivantes :*

1. *$< A >$ est un sous-groupe de G contenant A.*
2. *Si K est un autre sous-groupe de G contenant A on a $< A > \subset K$.*

Preuve : Soit $< A >$ le sous-groupe engendré par A. $< A >= \cap H$ où l'intersection porte sur les sous-groupes H de G contenant A. $< A >$ est donc un sous-groupe de G contenant A d'après la proposition 2.3.4. Soit K un sous-groupe de G contenant A. Alors, K fait partie de l'ensemble des sous-groupes sur lequel porte l'intersection définissant $< A >$ donc, $< A >$ étant inclus dans tout sous-groupe de G contenant A, $< A >$ est inclus dans K. Par conséquent, $< A >$ est le plus petit sous-groupe de G contenant A. ■

Proposition 2.3.5 *Tout sous-groupe de $\mathbb{Z}$ est de la forme $< n >= n\mathbb{Z}$ où n est un entier positif.*

Preuve : Soit H un sous-groupe de $\mathbb{Z}$ distinct de $\mathbb{Z}$.

- Si $H = 0$ alors $H =< 0 >$.
- Si $H = \mathbb{Z}$, $H =< 1 >$.
- On suppose que H est un **sous-groupe propre** de $\mathbb{Z}$ (donc différent de $\mathbb{Z}$ et de $\{1\}$). Soit n le plus petit élément strictement positif de H, montrons alors que $< n >= H$.
  n appartient à H sous-groupe de $\mathbb{Z}$ donc $< n >$ est inclus dans H ($< n >$ plus petit sous-groupe de $\mathbb{Z}$ contenant n).
  Montrons que H est inclus dans $< n >$: soit x appartenant à H. D'après la division euclidienne, il existe un couple d'entiers (i,j) avec $0 \leq j < n$ tel que $x = in + j$.
  Si i est positif, $in = n + ... + n$ appartient à H car n appartient à H et H est un sous-groupe de $\mathbb{Z}$.
  Si i est négatif, $in = (-n) + ... + (-n)$ appartient à H car n appartient à H et H est un sous-groupe de $\mathbb{Z}$.
  Comme x appartient à H sous-groupe de $\mathbb{Z}$, $j = x - in$ appartient à H. Or j est positif et strictement inférieur à n et n est le plus petit entier strictement positif appartenant à H donc $j = 0$. D'où, $x = in$ et x appartient donc à $< n >$. H est inclus dans $< n >$. Conclusion, $H =< n >= n\mathbb{Z}$.

■

Exercice 47 (*non corrigé*)

1. Soient $m\mathbb{Z}$ et $n\mathbb{Z}$ deux sous-groupes de $\mathbb{Z}$. Montrer que

$$m\mathbb{Z} + n\mathbb{Z} = \{mu + nv \mid u, v \in \mathbb{Z}\}$$

   a) est un sous-groupe de $\mathbb{Z}$,

b) contient $m\mathbb{Z}$ et $n\mathbb{Z}$,

c) est contenu dans tout sous-groupe de $\mathbb{Z}$ qui contient $m\mathbb{Z}$ et $n\mathbb{Z}$.

d) Si $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, que peut-on dire de d ?

2. Déterminer les sous-groupes engendrés par : $14\mathbb{Z} \cup 35\mathbb{Z}$; $4\mathbb{Z} \cup 8\mathbb{Z} \cup 6\mathbb{Z} \cup 64\mathbb{Z}$; $2\mathbb{Z} \cup 3\mathbb{Z}$; $4\mathbb{Z} \cup 21\mathbb{Z}$; $5\mathbb{Z} \cup 25\mathbb{Z} \cup 7\mathbb{Z}$; $\{70, 4\}$.

On introduit ensuite la notion de sous-groupe distingué (utilisée initialement par Galois). Les sous-groupes distingués connaissent des applications en géométrie dans l'étude des actions de groupes, en topologie algébrique dans la classification des revêtements, en théorie de Galois dans la correspondance de Galois.

Définition 2.3.6 *Un sous-groupe H d'un groupe (G, T) est **distingué** (ou **normal** ou **invariant**) si pour tout x de G et pour tout h de H, le produit $xThTx^{-1}$ est élément de H. On note alors $H \triangleleft G$ et on lit "H est distingué dans G".*

Un sous-groupe distingué H d'un groupe G est un sous-groupe globalement stable par l'action de G sur lui-même par conjugaison. Les sous-groupes distingués interviennent naturellement dans la définition du quotient d'un groupe.

Définition 2.3.7 *Pour tout x de G on note :*
- *xH l'ensemble (**classe à gauche**) des éléments de G de la forme xTh avec h élément de H,*
- *Hx l'ensemble (**classe à droite**) des éléments de G de la forme hTx avec h élément de H,*
- *xHx^{-1} l'ensemble des éléments de G de la forme $xThTx^{-1}$ avec h élément de H.*

Une façon équivalente de définir un sous-groupe distingué est de dire que les classes à droite et à gauche de H dans G coïncident, c'est-à-dire :

Proposition 2.3.6

$$\boxed{H \triangleleft G \text{ si et seulement si } xHx^{-1} = H \Leftrightarrow xH = Hx}$$

Preuve : Par définition, $H \triangleleft G \Leftrightarrow xHx^{-1} \subset H$ pour tout x de G. Or, $H \subset xHx^{-1}$. En effet, si $h \in H$, on aura :

$$h \in xHx^{-1} \Leftrightarrow \exists h' \in H,\ h = xTh'Tx^{-1} \Leftrightarrow \exists h' \in H,\ h' = x^{-1}ThTx$$

Vu que $H \triangleleft G$, $h' = x^{-1}ThTx$ est effectivement élément de H. Ainsi, on peut également dire $H \triangleleft G$ si et seulement si $xHx^{-1} = H \Leftrightarrow xH = Hx$. ■

Exemple 2.3.3 Les déplacements du plan, constitués des translations et des rotations, constituent un groupe (non commutatif) pour la loi de composition des applications. Les translations en constituent un sous-groupe distingué.

Remarque 2.3.3
- $\{e\}$ et G sont toujours des sous-groupes distingués.
- Un sous-groupe de G de la forme xHx^{-1} avec $x \in G$ est appelé un **conjugué** de H. Par conséquent, un sous-groupe est distingué si et seulement s'il est son seul conjugué.

Exercice 48 Soit $(G, \times)$ un groupe et $\simeq$ une relation d'équivalence sur G. On suppose que cette relation est compatible avec la loi de groupe, c'est-à-dire que si $\forall x, y, x', y' \in G$, $x \simeq x'$ et $y \simeq y'$ alors $xy \simeq x'y'$.

Montrer que la classe H de l'élément neutre 1 est un sous-groupe distingué de G et que $\forall x, x' \in G$, $x \simeq x'$ est équivalent à $x'x^{-1} \in H$.
Correction : Étant donnés $y, z \in H$, on a $y \simeq 1$ et $z \simeq 1$. La compatibilité de la loi donne d'une part $yz \simeq 1$, soit $yz \in H$, et d'autre part $yy^{-1} \simeq y^{-1}$ soit $y^{-1} \in H$. Cela montre que H est un sous-groupe de G. Pour tout $x \in G$, on a aussi $xyx^{-1} \simeq x1x^{-1} = 1$ et donc $xyx^{-1} \in H$. Le sous-groupe H est donc distingué. De plus, pour $x, x' \in G$, si $x \simeq x'$, alors par compatibilité de la loi, on a $x'x^{-1} \simeq xx^{-1} = 1$, c'est-à-dire $x'x^{-1} \in H$.
Réciproquement, si $x'x^{-1} \in H$, alors $x'x^{-1} \simeq 1$, et donc, par compatibilité de la loi, $x \simeq x'$.

Proposition 2.3.7 *Si G est commutatif (groupe abélien), alors tout sous-groupe de G est distingué dans G.*

Preuve : Soit H un sous-groupe de G. (G, T) est commutatif donc tous les éléments de G commutent entre-eux y compris ceux qui sont dans H ((H, T) est donc commutatif). Par conséquent, $\forall x \in G$ et $\forall h \in H$, $xTh = hTx \Leftrightarrow xThTx^{-1} = h$ en composant à droite par x^{-1} (l'inverse de x, qui existe puisque (G, T) est un groupe). Comme $h \in H$, on conclut que tout sous-groupe H de G est distingué dans G. ■

Exemple 2.3.4 $(\mathbb{Z}, +)$ est commutatif et $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$ donc $n\mathbb{Z} \triangleleft \mathbb{Z}$.

2.3.3 Construction du quotient d'un groupe

Les sous-groupes distingués sont importants dans l'étude des groupes quotients à cause du résultat suivant : on peut construire un groupe quotient G/H de loi compatible avec celle de G si et seulement si H est un sous-groupe distingué de G. Plus précisément, dans l'étude des groupes, le quotient d'un groupe est une opération classique permettant la construction de nouveaux groupes à partir d'anciens. À partir d'un groupe G, et d'un sous-groupe H, on peut définir une loi de groupe sur l'ensemble G/H des classes de G suivant H, à condition que les classes latérales droites soient égales aux classes latérales gauches ($xH = Hx$).

Soient (G, T) et (H, T) désignant respectivement un groupe et un sous groupe de G.

Proposition 2.3.8 *Soient $x, y \in G$. La relation $\mathcal{R}$ définie par $x\mathcal{R}y \Leftrightarrow xTy^{-1} \in H$ est une relation d'équivalence(à droite) sur G.*

Preuve :
- $\mathcal{R}$ est réflexive : $\forall x \in G$, $xTx^{-1} = e \in H \Leftrightarrow x\mathcal{R}x$.
- Ensuite, comme H est un sous-groupe de G, tout élément dans H admet un inverse (dans H) donc $(xTy^{-1})^{-1} = yTx^{-1} \in H \Leftrightarrow y\mathcal{R}x$ (H étant stable par inversion). Par conséquent, $\mathcal{R}$ est symétrique.
- Montrons enfin que $\mathcal{R}$ est transitive : soit $(x, y, z) \in G^3$, ($x\mathcal{R}y$ et $y\mathcal{R}z$) $\Leftrightarrow$ ($xTy^{-1} \in H$ et $yTz^{-1} \in H$). $(xTy^{-1})T(yTz^{-1}) = xT(y^{-1}Ty)Tz^{-1} = xTeTz^{-1} = xTz^{-1} \in H \Leftrightarrow x\mathcal{R}z$ (car H est stable pour la loi de composition).

■

Par conséquent, ($\forall x, y \in H$, $x\mathcal{R}y$) $\Leftrightarrow$ (H est un sous-groupe de G) d'après la proposition 2.3.2 .

Proposition 2.3.9 *Soit $x \in G$. La classe d'équivalence (à droite) de x pour la relation $\mathcal{R}$ est l'ensemble $Hx = \{hTx, h \in H\}$. Elle est notée $cl(x)$ ou $\overline{x}$.*

Preuve : Par définition, $cl(x) = \{y \in G, x\mathcal{R}y\}$. Soit $y \in G$ équivalent à x pour la relation $\mathcal{R}$. Alors il existe $k \in H$ (dont l'inverse $k^{-1} = h$ est aussi dans H) tel que $xTy^{-1} = k \Leftrightarrow y = hTx$. Et donc y est élément de Hx. Réciproquement, si y est élément de Hx, il est clair que $x\mathcal{R}y$. ■

Remarque 2.3.4 On aurait aussi pu définir la relation d'équivalence (à gauche) $\mathcal{R}$ par $x\mathcal{R}y \Leftrightarrow y^{-1}Tx \in H$. Dans ce cas, la classe d'équivalence d'un élément x de G aurait été donnée par l'ensemble xH (classe à gauche de x de H).

Supposons que H soit un sous-groupe distingué de G. On désire définir une loi $\boxed{\mathrm{T}}$ sur l'ensemble quotient $G/\mathcal{R}$ de la façon la plus naturelle possible c'est-à-dire en posant $cl(x)\boxed{\mathrm{T}}cl(y) = cl(xTy)$. La justification de ce choix est la suivante : si X et Y sont deux classes d'éléments de G suivant H, XY en est une aussi. Il existe des éléments x et y de G tels que X et Y soient repectivement les classes de x et y suivant H. Nous avons alors $XY = (xH)(yH) = (Hx)(yH) = H(xTy)H$; comme H est distingué, nous pouvons remplacer $H(xTy)$ par $(xTy)H$ et nous trouvons $XY = xTyHH$. Mais $HH = H$ (puisque H est un sous-groupe de G), donc la relation obtenue peut s'écrire $XY = xTyH$, ce qui montre bien que XY est une classe suivant H (et plus particulièrement, la classe de xTy). De ce qui précède, il résulte qu'en faisant correspondre à une classe X et une classe Y l'ensemble XY, nous définissons une loi de composition $\boxed{\mathrm{T}}$ dans l'ensemble des classes suivant H et que cette loi peut être caractérisée par la relation

$$xH\boxed{\mathrm{T}}yH = (xTy)H \Leftrightarrow cl(x)\boxed{\mathrm{T}}cl(y) = cl(xTy).$$

Cette définition a un sens si et seulement si la classe $cl(xTy)$ ne dépend pas du choix des représentants x et y des classes $cl(x)$ et $cl(y)$, autrement dit si : pour $x, y, x', y' \in G$,

$$\left.\begin{array}{l} x\mathcal{R}x' \\ y\mathcal{R}y' \end{array}\right\} \Rightarrow xTy\mathcal{R}x'Ty'. \tag{2.1}$$

Si l'implication (2.1) est vérifiée, on dit que la relation d'équivalence $\mathcal{R}$ est compatible avec la loi T (cf. chapitre 1). On ajoute la définition suivante :

Définition 2.3.8 *La relation $\mathcal{R}$ est dite* ***compatible à droite*** *(respectivement* ***à gauche****) avec la loi T si*

$$\forall x, y, z \in G,\ x\mathcal{R}y \Rightarrow xTz\mathcal{R}yTz \text{ (respectivement } x\mathcal{R}y \Rightarrow zTx\mathcal{R}zTy)$$

On a alors le

Théorème 2.3.4 *La relation $\mathcal{R}$ est compatible avec la loi de groupe si et seulement si elle est compatible à droite et à gauche.*

Preuve : Le sens non trivial se montre ainsi : $x\mathcal{R}x'$ et $y\mathcal{R}y' \Rightarrow xTy\mathcal{R}x'Ty$ et $x'Ty\mathcal{R}x'Ty' \Rightarrow xTy\mathcal{R}x'Ty'$. ■

On considère enfin le théorème intermédaire suivant :

Théorème 2.3.5 *Il y a équivalence entre*

1. *La relation d'équivalence $\mathcal{R}$ est compatible à droite.*
2. *Il existe un sous-groupe H tel que $x\mathcal{R}y \Leftrightarrow xTy^{-1} \in H \Leftrightarrow y \in Hx$*

Preuve : Si $\mathcal{R}$ est compatible à droite, $x\mathcal{R}y \Leftrightarrow xTy^{-1}\mathcal{R}e \Leftrightarrow xTy^{-1} \in cl(e)$ et on vérifie que $H = cl(e)$ est bien un sous-groupe de G. Réciproquement si on a 2., $xTy^{-1} \in H \Leftrightarrow (xTz)T(yTz)^{-1} \in H$, $\mathcal{R}$ est compatible à droite. ■

Des deux théorèmes précédents on déduit :

Théorème 2.3.6 *Soit (G, T) un groupe et $\mathcal{R}$ une relation d'équivalence dans G. Il y a équivalence entre :*

1. *$cl(x)\boxed{T}cl(y) = cl(xTy)$ définit une loi de groupe sur $G/\mathcal{R}$.*
2. *La relation $\mathcal{R}$ est compatible à droite et à gauche avec la loi de groupe.*
3. *Il existe un sous-groupe H tel que*
   (a) *$\forall x \in G,\ xH = Hx \Leftrightarrow H$ est distingué dans G.*
   (b) *$x\mathcal{R}y \Leftrightarrow xTy^{-1} \in H \Leftrightarrow x^{-1}Ty \in H$.*

Pour conclure on donne la

Définition 2.3.9 *Soit $H \triangleleft G$. La relation $\mathcal{R}$ définie par*

$$x\mathcal{R}y \Leftrightarrow xTy^{-1} \in H$$

est appelée ***relation d'équivalence*** *suivant le sous-groupe H. L'ensemble quotient $G/\mathcal{R}$ est alors un groupe pour la loi naturelle, appelé* ***groupe quotient****, et se note G/H.*

Exemple 2.3.5 Soit la relation $\mathcal{R}$ définie sur $\mathbb{Z}$ par $x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z}/x - y = kn$, $\mathcal{R}$ est une relation d'équivalence. Cette relation est appelée **relation de congruence modulo** n. Deux entiers x et y en relation sont dits congrus l'un à l'autre modulo n et on note alors $x \equiv y \mod n$ (ou $x \equiv y[n]$). On remarquera que $x \equiv 0 \mod n$ si et seulement si n divise x.
Soit x appartenant à $\mathbb{Z}$. On note par $\overline{x}$ la classe d'équivalence de x pour la relation de congruence modulo n. On note par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de la relation de congruence modulo n. On peut alors déduire des résultats précédents que $\mathbb{Z}/n\mathbb{Z}$ est un groupe (abélien) pour la loi $\overline{x} + \overline{y} = \overline{x+y}$.
Si on considère $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, cela nous permet d'affirmer par exemle que $\overline{9} = \overline{4+5} = \overline{4}+\overline{5} = \overline{4}+\overline{0} = \overline{4+0} = \overline{4}$.

Exercice 49 On définit sur $\mathbb{R}^2$ la relation ρ par

$$(x, y)\rho(x', y') \Leftrightarrow x + y = x' + y'$$

1. Montrer que ρ est une relation d'équivalence.
2. Trouver la classe d'équivalence du couple $(0, 0)$.
3. Soit f l'application de $\mathbb{R}^2$ dans $\mathbb{R}$ définie par :

   $$f : (x, y) \to x + y$$

   Montrer que deux éléments de $\mathbb{R}^2$ équivalents modulo ρ ont même image par f et que deux éléments non équivalents ont des images distinctes.
4. En déduire qu'entre l'ensemble quotient $\mathbb{R}^2/\rho$ et $\mathbb{R}$ il existe une bijection g que l'on précisera.

Correction :

1. On montre aisément que ρ est réflexive, symétrique et transitive donc ρ est bien une relation d'équivalence.
2. La classe d'équivalence du couple $(0, 0)$ est constituée par l'ensemble des couples $(x, y) \in \mathbb{R}^2$ vérifiant $x + y = 0$. C'est l'ensemble des points situés sur la deuxième bissectrice du plan $x0y$.
3. Soient $u, v \in \mathbb{R}^2$, alors $u\rho v \Leftrightarrow f(u) = f(v)$. On en déduit également que deux éléments non équivalents ont des images distinctes.
4. g est l'application qui à une classe fait correspondre la somme des composants d'un représentant quelconque de cette classe. g est injective d'après la question précédente. Par ailleurs, $\forall \alpha \in \mathbb{R}$, on peut considérer que α est l'image de $(\frac{\alpha}{2}, \frac{\alpha}{2}) \in \mathbb{R}^2$ donc g est surjective et par conséquent bijective.

2.3.4 Homomorphismes de groupes

On doit à Marie Ennemond Camille JORDAN (1838-1922) le concept d'**homomorphisme** entre deux structures :

Définition 2.3.10 *Un* ***morphisme de groupes*** *ou* ***homomorphisme de groupes*** *(du grec homoios = semblable et morphê = forme) est une application entre deux groupes qui respecte la structure des groupes.*

Plus précisément, si (G,T) et $(G',\star)$ sont deux groupes d'éléments neutres respectifs e et n, une application $f : G \to G'$ est un morphisme de groupes lorsque :

$$\boxed{\forall (a,b) \in G \times G,\ f(aTb) = f(a) \star f(b)}$$

Un morphisme de groupes transporte la loi de groupe, et va ainsi conserver toutes les propriétés liées à cette loi. Il est donc intéressant d'étudier comment se comportent les principaux objets de la théorie des groupes par les morphismes.

Définition 2.3.11 *Un **isomorphisme** f est un homomorphisme bijectif.*

Proposition 2.3.10 *Si (G,T) et $(G',\star)$ sont deux groupes quelconques, et si f est un isomorphisme de G sur G', alors f^{-1} est un isomorphisme de G' sur G.*

Preuve : Si f est un isomorphisme, alors f est une bijection, donc f^{-1} aussi. Il suffit de montrer que f^{-1} est un morphisme de groupes. Soient x et y deux éléments quelconques de G'. On a alors : $f(f^{-1}(x)Tf^{-1}(y)) = f(f^{-1}(x)) \star f(f^{-1}(y)) = x \star y$. D'où $f^{-1}(x)Tf^{-1}(y) = f^{-1}(x \star y)$ et f^{-1} est donc un isomorphisme de groupes de G' sur G. ■

Définition 2.3.12 *Lorsque $G = G'$, un homomorphisme est appelé **endomorphisme** et s'il est bijectif, on parlera d'**automorphisme**.*

Exemple 2.3.6

- L'application $f : (\mathbb{Q}^\star, \times) \to (\mathbb{Q}^+, \times)$ définie par $f(x) = \|x\|$ est un morphisme de groupes :
$$f(x \times y) = \|x \times y\| = \|x\| \times \|y\| = f(x) \times f(y),\ \forall x, y \in \mathbb{Q}^\star$$
- L'application $f : (\mathbb{R}^{+\star}, \times) \to (\mathbb{R}, +)$ définie par $f(x) = \ln x$ est un isomorphisme de groupes :
$$f(x \times y) = \ln(x \times y) = \ln x + \ln y = f(x) + f(y),\ \forall x, y \in \mathbb{R}^{+\star}.$$
- Soit $a \in \mathbb{R}$. L'application $f_a : (\mathbb{R}, +) \to (\mathbb{R}^{+\star}, \times)$ définie par $f_a(x) = a^x$ est un isomorphisme de groupes : on a
$$f_a(x+y) = a^{x+y} = a^x \times a^y = f_a(x) \times f_a(y),\ \forall x, y \in \mathbb{R}.$$
- L'application $f : (\mathbb{R}^\star, \times) \to (\mathbb{R}^\star, \times)$ définie par $f(x) = x^2$ pour tout $x \in \mathbb{R}^\star$ est un homomorphisme ; en effet
$$f(x \times y) = (x \times y)^2 = x^2 \times y^2 = f(x) \times f(y),\ \forall x, y \in \mathbb{R}^\star.$$
- L'application $f : (\mathbb{C}^\star, \times) \to (\mathbb{R}^\star, \times)$ définie par $f(z) = |z|$ pour tout $x \in \mathbb{C}^\star$ est un homomorphisme, car
$$f(z \times w) = |z \times w| = |z| \times |w| = f(z) \times f(w),\ \forall z, w \in \mathbb{C}^\star.$$
- L'application $f : (\mathbb{R}, +) \to (\mathbb{R}^{+\star}, \times)$ définie par $f(x) = e^x$ pour tout $x \in \mathbb{R}$ est un isomorphisme, car elle est bijective et
$$f(x+y) = e^{x+y} = e^x \times e^y = f(x) \times f(y),\ \forall x, y \in \mathbb{R}.$$
- L'application $f : (\mathbb{R}, +) \to (\mathbb{C}^\star, \times)$ définie par $f(x) = e^{2i\pi x}$ pour tout $x \in \mathbb{R}$ est un homomorphisme, car
$$f(x+y) = e^{2i\pi(x+y)} = e^{2i\pi x} \times e^{2i\pi y} = f(x) \times f(y),\ \forall x, y \in \mathbb{R}.$$

Proposition 2.3.11 *Lorsque G possède un élément neutre e, l'image homomorphe $f(e) = n$ est neutre dans $f(G)$. Si la loi T de G est associative, alors celle de $f(G)$ l'est aussi. Si G est un groupe, son image homomorphe $f(G)$ en est aussi un et $f(x^{-1}) = [f(x)]^{-1}$: l'inverse de $f(x)$ dans $f(G)$ est l'image de l'inverse de x dans G.*

Preuve : Si e est neutre dans G, $f(e) \star f(x) = f(eTx) = f(x)$ et $f(x) \star f(e) = f(xTe) = f(x)$, donc $f(e)$ est neutre dans $f(G)$. Si la loi T est associative, la loi $\star$ l'est aussi : $f[aT(bTc)] = f[(aTb)Tc]$, donc $f(a) \star f(bTc) = f(a) \star [f(b) \star f(c)]$ et c'est aussi $f(aTb) \star f(c) = [f(a) \star f(b)] \star f(c)$. Enfin si x admet un inverse x^{-1} dans G, $f(xTx^{-1}) = f(e) = f(x) \star f(x^{-1})$ et c'est aussi $f(x^{-1}) \star f(x)$: l'inverse dans $f(G)$ de $f(x)$ existe et c'est $f(x^{-1})$. En d'autres termes $[f(x)]^{-1} = f(x^{-1})$. ■

Exercice 50 On considère sur $]-1,1[$ la loi $xTy = \dfrac{x+y}{1+xy}$, montrer que $(]-1,1[,T)$ est un groupe commutatif. Montrer qu'il est isomorphe à $(\mathbb{R},+)$.
Correction : On montre sans grande difficulté que T est commutative (même si ce n'est pas indispensable), associative $\left(xT(yTz) = (xTy)Tz = \dfrac{x+y+z+xyz}{xy+xz+yz}\right)$, d'élément neutre 0, et tout élément x est inversible, d'inverse $-x$. Le plus difficile est en fait de prouver que la loi T est bien une lci (loi de composition interne), c'est-à-dire de prouver que $]-1,1[$ est stable par T. Si $x<1$ et $y<1$, $(x-1)(y-1) = xy-x-y-1 < 0$, donc $-(1+xy) < x+y$, et en divisant par $1+xy$ qui est positif, on obtient $-1 < \dfrac{x+y}{1+xy}$. De même, en partant de $-1<x$ et $-1<y$, on obtient $\dfrac{x+y}{1+xy} < 1$. Finalement, T est bien une loi de groupe. On peut également remarquer que $th : \mathbb{R} \to]-1,1[$ est une application bijective vérifiant $th(x+y) = th(x)Tth(y)$. On peut en déduire immédiatement qu'il s'agit d'un isomorphisme de groupes.

Définition 2.3.13 *Si G' admet un élément neutre n, l'ensemble N des éléments de G dont l'image par f est n s'appelle le* ***noyau*** *de f, noté $Kerf$. L'****image*** *de f est définie par $Imf = f(G)$.*

Exemple 2.3.7 Soient $G = \{\phi_0, \phi_1, \phi_2, \phi_3, \phi_4, \phi_5\}$, $G' = \{\phi_0, \phi_1\}$ d'élément neutre ϕ_0, et $f : G \to G'$ définie par $f(\phi_0) = \phi_0$, $f(\phi_1) = \phi_1$, $f(\phi_2) = \phi_0$, $f(\phi_3) = \phi_0$, $f(\phi_4) = \phi_1$ et $f(\phi_5) = \phi_1$. Alors, $\mathrm{Ker}f = \{\phi_0, \phi_2, \phi_3\}$ et $\mathrm{Im}f = G'$.

Exercice 51 Montrer que $x \mapsto \dfrac{x}{|x|}$ est un endomorphisme de groupes de $(\mathbb{R}^\star, \times)$. Déterminer son noyau et son image. Même question pour l'application $\theta \mapsto e^{i\theta}$ (de $(\mathbb{R},+)$ dans $(\mathbb{C}^\star, \times)$).
Correction : Il suffit de vérifier que $\forall x, y \in \mathbb{R}^\star$, $\dfrac{x}{|x|} \times \dfrac{y}{|y|} = \dfrac{xy}{|xy|}$, ce qui est vrai. L'image de ce morphisme est $\{-1,1\}$, et son noyau $\mathbb{R}^{\star+}$.
L'application $\theta \mapsto e^{i\theta}$ est un morphisme car $e^{i(\theta+\theta')} = e^{i\theta}e^{i\theta'}$. Son image est $\mathbb{U}$ ($\mathbb{U}$ est l'ensemble des nombres dont le module est égal à 1) et son noyau $2\pi\mathbb{Z} = \{2k\pi | k \in \mathbb{Z}\}$.

Proposition 2.3.12 *Le morphisme de groupe f est injectif si et seulement si le noyau de f n'est constitué que de l'élément neutre de G.*

Preuve : Soient $x, y \in G$ tels que $f(x) = f(y)$; alors $f(x) \star f(y)^{-1} = f(xTy^{-1}) = n$ c'est-à-dire que $xTy^{-1} \in \ker(f)$. Par conséquent $\ker(f) = \{e\}$ si et seulement si $xTy^{-1} = e$ c'est-à-dire que $x = y$. ■

Exercice 52 Soit G un groupe et $a \in G$. Montrer que l'application $x \mapsto axa^{-1}$ est un automorphisme de groupes de $(G, \times)$.
Correction : Comme $a(xy)a^{-1} = axa^{-1}aya^{-1}$, l'application est un endomorphisme de groupes. De plus, si $axa^{-1} = e$, alors $ax = a$, donc $x = e$, autrement dit le noyau de ce morphisme est réduit à l'élément neutre, l'application est donc injective. Comme de plus un élément y a toujours un antécédent, en l'occurence $a^{-1}ya$, elle est également surjective, donc bijective. C'est donc un automorphisme de groupes, dont la réciproque est d'ailleurs $y \mapsto a^{-1}ya$.

Théorème 2.3.7 *Lorsque G est un groupe, le noyau N de f est un sous-groupe distingué de G.*

Preuve : Notons e l'élément neutre de G. $n = f(e)$ est neutre dans $f(G)$. Soit u un élément de N et x dans G :

$$f(xTuTx^{-1}) = f(x) \star f(u) \star f(x^{-1}) = f(x) \star n \star f(x^{-1}) = [f(x) \star n] \star f(x^{-1}) = f(x) \star f(x^{-1}) = f(xTx^{-1}) = f(e) = n.$$

Par conséquent $xTuTx^{-1} \in N$ et donc $N \triangleleft G$. ■
Cela implique d'après la section sur la construction du quotient d'un groupe qu'on peut construire un groupe quotient $G/N = G/\mathrm{Ker}f$ de loi compatible avec celle de G.

On a également le résultat important ci-desssous qui permet de compléter le théorème 2.3.6 :

Théorème 2.3.8 *Soit (G, T) un groupe et $H \triangleleft G$. L'application s définie par*

$$\begin{array}{rcl} s : (G,T) & \to & (G/H, \boxed{T}) \\ x & \mapsto & cl(x) \end{array}$$

est un morphisme de groupes. Il est surjectif. Son noyau est égal à H. Le morphisme s s'appelle la ***surjection (ou projection) canonique*** *de G sur G/H. On note parfois $s = s_H$.*

Preuve : s est une application puisque tout élément de G appartient à une et une seule classe d'équivalence ; pour tout $x, y \in G$ on a $s(xTy) = HxTy = Hx\boxed{\mathrm{T}}Hy = s(x)\boxed{\mathrm{T}}s(y)$ c'est-à-dire que s est un morphisme. s est surjective puisqu'aucune classe d'équivalence n'est vide. ■

Le théorème suivant et qui utlise les résultats précédents est dû à Emmy NOETHER (1882-1935)

Théorème 2.3.9 *(Premier théorème d'isomorphisme ou théorème de décomposition canonique)*
Soient (G, T) et $(G', \star)$ deux groupes et φ un homomorphisme de G dans G'. Il existe alors un isomorphisme ν de $G/Ker(\varphi)$ sur $\varphi(G)$ tel que $\varphi = \nu_o s$ où s est la surjection canonique de G sur $G/Ker(\varphi)$. On a donc $G/Ker(\varphi) \simeq \varphi(G)$.

Preuve : Montrons que l'application $\nu : G/Ker(\varphi) \mapsto \varphi(G) = Im(G)$ est un homorphisme bijectif.

1. ν est bien définie. En effet, $\forall Hx, Hy \in G/H$ tels que $Hx = Hy$, il vient que $xTy^{-1} \in H = Ker(\varphi)$ donc $\varphi(xTy^{-1}) = \varphi(x) \star \varphi(y)^{-1} = n$ d'où $\varphi(x) = \varphi(y)$ soit $\nu(Hx) = \nu(Hy)$.
2. ν est un morphisme, pour tout $Hx, Hy \in G/H$ on a
$$\nu(Hx\boxed{\mathrm{T}}Hy) = \nu(HxTy) = \varphi(xTy) = \varphi(x) \star \varphi(y) = \nu(Hx) \star \nu(Hy).$$
3. ν est surjective par définition, il reste à prouver que ν est injective. Pour tout $Hx, Hy \in G/H$ tels que $\nu(Hx) = \nu(Hy)$ on a $\varphi(x) = \varphi(y)$. On en déduit que $\varphi(xTy^{-1}) = n$ d'où $xTy^{-1} \in Ker(\varphi)$ et $Hx = Hy$. ■

Corollaire 2.3.1 *Si φ est un homorphisme surjectif alors $G/Ker(\varphi) \simeq G'$ du fait que $Im(\varphi) = G'$.*

Exercice 53 *(non corrigé)* Soit $(A, +, 0)$ un groupe abélien (commutatif) et soit $H \subset A$ un sous-groupe de A. Pour tout $a \in A$, la classe de a modulo H est définie par le sous-ensemble de A suivant

$$a + H = \{a + h, h \in H\} \subset A$$

1. Donner une condition nécessaire et suffisante pour que deux classes soient égales ($a + H = b + H$). On note A/H l'ensemble des classes modulo H :

$$A/H = \{a + H, a \in A\}$$

2. Montrer que l'ensemble des classes modulo H forme une partition de A. Si, en outre, A est fini, montrer que toutes les classes ont le même cardinal. Combien y a-t-il de classes différentes dans ce cas ?

On définit la loi de composition interne suivante entre deux classes :

$$(a + H) \oplus (b + H) = (a + b) + H = \{a + b + h, h \in H\}$$

3. Montrer que $(A/H, \oplus, 0 + H)$ est un groupe abélien. Ce groupe est appelé le groupe quotient de A par H.

Exercice 54 *(non corrigé)*

1. Soit $n \in \mathbb{Z}$, montrer que $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +, 0)$.
2. Montrer que tous les sous-groupes de $\mathbb{Z}$ sont de cette forme.

On note $(\mathbb{Z}/n\mathbb{Z}, \oplus, 0 + n\mathbb{Z})$ le groupe abélien des classes modulo n. Pour tout $k \in \mathbb{Z}$, on notera $\overline{k}$ la classe $k + n\mathbb{Z}$ de k modulo n.

3. Que vaut $\overline{137} \oplus \overline{212}$ dans $\mathbb{Z}/13\mathbb{Z}$?
4. "Arithmétique horlogère" [Gauss] : "Je dois partir demain pour San Francisco à 9 heures. Le train mettra 126 heures pour relier Nice à Vladivostok. Il faudra ensuite 358 heures au bateau pour franchir le Golden Gate Bridge. En arrivant vais-je pouvoir manger mes pancakes favoris dans un café du port dont les horaires d'ouverture sont 7 heures - 11 heures ?

2.3.5 Les groupes finis et l'exemple du groupe symétrique

Définition 2.3.14 *Un groupe (ou sous-groupe) est dit **fini** si le nombre de ses éléments, appelé alors **ordre** du groupe (ou sous-groupe), est fini. On notera $|G|$ l'ordre du groupe G.*

Définition 2.3.15 *L'**ordre d'un élément** (on dit parfois période) a d'un groupe est le plus petit nombre entier positif m tel que $a^m = e$ (où e désigne l'élément neutre ou identité du groupe, et a^m désigne le produit de m copies de a). Si aucun m de la sorte n'existe, on dit que a est d'ordre **infini**.*

Proposition 2.3.13 *Si H est un sous-groupe fini de G et si x et y sont deux éléments de G alors les classes d'équivalence (à gauche ou à droite) de x et y pour la relation $\mathcal{R}$ ont même nombre d'éléments et ce nombre est égal au cardinal de H.*

Preuve : Soit T la loi de composition interne de G et x un élément de G. Posons $f : H \to xH, h \mapsto f(h) = xTh$; l'application f est injective car si h et h' sont des éléments de H tels que $f(h) = f(h')$ alors on a l'égalité $xTh = xTh' \Leftrightarrow h = h'$ car x est régulier. f est aussi surjective car si y est un élément de xH, alors il existe $h \in H$ tel que $y = xTh$ et donc $y = f(h)$. f étant à la fois injective et surjective, est bijective. Ceci prouve que H et xH ont même nombre d'éléments. Mais si y est un élément de G, yH et H auront aussi même nombre d'éléments. Donc xH et yH ont même cardinal.
De même on montrerait que toutes les classes à droite pour une relation $\mathcal{R}$, issue d'un sous groupe H de cardinal fini dans G, ont même nombre d'éléments, ce nombre étant égal à $|H|$. ■

Le théorème qui vient maintenant et qui résulte en partie de la proposition précédente est fondamental en algèbre.

Théorème 2.3.10 *(Lagrange) Soit G un groupe fini. Si H est un sous-groupe de G, alors le cardinal de H divise celui de G. On notera $|G/H|$ où $[G : H]$ le nombre $|G|/|H|$. $[G : H]$ s'appelle l'**indice** de H dans G.*

Preuve : Soit donc H un sous-groupe de G. On considère la relation d'équivalence $\mathcal{R}$ associée à H. Elle nous permet de définir une partition de G par des sous-ensembles de la forme xH où $x \in G$. On peut donc trouver, G étant fini, un nombre $n \in \mathbb{N}$ et $x_1, \ldots, x_n \in G$ tels que $\{x_1H, \ldots, x_nH\}$ forme une partition de G. Mais les sous-ensembles x_iH ont tous, d'après la proposition précédente, le même nombre d'éléments. De plus, ce nombre est égal à $|H|$. Donc le cardinal de G s'écrit $|G| = n|H|$. ■

On donne maintenant un corollaire du théorème de Lagrange qui est absolument fondamental dans la théorie des groupes finis.

Corollaire 2.3.2 *Soit G un groupe. Soit g un élément de G d'ordre fini. Alors l'ordre de g divise l'ordre de G.*

Preuve : Soient G et g comme dans l'énoncé et soit n l'ordre de g. Alors $\{g, g^2, \ldots, g^n = e\}$ est un sous groupe de G. Cette affirmation est triviale à vérifier. De plus, par définition de l'ordre d'un élément dans un groupe, ce sous-groupe est de cardinal n. Par application du théorème de Lagrange, n est un diviseur du cardinal de G.■

Remarque 2.3.5 On peut se poser le problème réciproque, à savoir : Si p est un diviseur de l'ordre du groupe alors existe-t-il un élément d'ordre p dans G ou encore, existe-t-il un sous groupe d'ordre p dans G ? La réponse est donnée par le théorème de Cauchy pour les éléments d'ordre p et sous certaines conditions sur p, et par le théorème de Ludwig SYLOW (1832-1918), pour les sous-groupes d'ordre p, sous certaines conditions sur p et sur G.

Définition 2.3.16 *Un groupe, noté ici multiplicativement, est dit* ***monogène*** *s'il contient un élément g tel que tout élément de G s'écrive sous la forme g^n. On dit que le groupe est* ***engendré par*** *g. Un groupe monogène* ***fini*** *(possédant un nombre fini d'éléments) est dit* ***cyclique****.*

Exemple 2.3.8 Dans $\mathbb{C}$, ensemble des nombres complexes contenant le célèbre nombre i tel que $i^2 = -1$, considérons $G = \{1, i, -1, -i\}$ muni de la multiplication usuelle des nombres complexes : $(G, \times)$ est un groupe commutatif ; on peut établir sa table de Pythagore (ci-dessous).

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Un tel groupe est monogène (il est engendré par les puissances d'un de ses éléments : i (ou bien -i)). Ce groupe monogène de 4 éléments est fini et donc cyclique.

Plus généralement un groupe (G, T) d'élément neutre e, non réduit à $\{e\}$ sera monogène s'il existe un élément a de G distinct de e tel que $G = \{e, a, aTa, aTaTa, \ldots, a^{(n)}, \ldots\}$ en désignant par $a^{(n)}$ le composé de n éléments égaux à a (n non nul). Un tel groupe sera cyclique, s'il existe un entier n non nul pour lequel $a^{(n)} = e$. Le plus petit entier non nul vérifiant cette égalité est alors l'ordre du groupe.

Proposition 2.3.14 *Soit $|G| = p$ premier. Alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (en particulier, G est commutatif).*

Preuve : Soit $x \neq 1$ dans G, et soit $H =< x >$ le sous-groupe engendré par x. Alors $|H||G/H| = p$, et comme $|H| > 1$, $|H| = p$, et $H = G$. Or $< x >$ est toujours un groupe cyclique ; en fait, si $< x >$ est fini, comme c'est le cas ici, $< x >= \mathbb{Z}/d\mathbb{Z}$, où $d > 0$ est le cardinal de $< x >$. Donc on a bien $G =< x > \simeq \mathbb{Z}/p\mathbb{Z}$. ■

Exemple 2.3.9
- Le groupe additif $(\mathbb{Z}, +)$ des entiers relatifs est monogène (engendré par 1) mais il est infini donc non cyclique.
- Dans $(\mathbb{Q}, \times)$, l'ensemble des puissances entières d'un nombre non nul a est un groupe monogène infini, isomorphe à $(\mathbb{Z}, +)$ vu que $a^{m+n} = a^m \times a^n$. Il suffit pour s'en convaincre de considérer l'ensemble des puissances de 2.
- Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est monogène (engendré par la classe de 1) et fini : c'est un groupe cyclique.
- Dans $\mathbb{C}$, les racines n-ièmes de l'unité constituent un groupe cyclique multiplicatif (pour la multiplication).

Remarque 2.3.6 Par définition, un groupe cyclique est fini mais un groupe fini n'est pas nécessairement cyclique : on pourra considérer le cas du groupe symétrique ci-après ou encore le groupe de Klein.

On peut énoncer que, à un isomorphisme près, $(\mathbb{Z}, +)$ est le seul groupe monogène infini. Et, à un isomorphisme près encore, $(\mathbb{Z}/n\mathbb{Z}, +)$ est le seul groupe monogène fini. Il suit que :

Proposition 2.3.15 *Tout groupe monogène (donc tout groupe cyclique) est abélien (commutatif)*

On introduit ensuite un théorème de Cauchy sur les groupes finis : ce théorème fut également énoncé auparavant par Euler et Lagrange dans une formulation équivalente sans le secours de la notion algébrique de groupe :

Théorème 2.3.11 *Dans un groupe fini E d'ordre n (c'est-à-dire ayant n éléments), si k est l'ordre d'un sous-groupe F de E, alors k divise n.*

Preuve : utilisons la notation additive pour simplifier les écritures. Soit $\mathcal{R}$ la relation définie dans E par : $a\mathcal{R}b \Rightarrow a - b \in F$. Il est clair que $\mathcal{R}$ est une relation d'équivalence dont les classes sont en nombre fini (puisque E est fini). Dans E, b est en relation avec a si et seulement si $b = a + u$, $u \in F$. Par suite, le cardinal de toute classe est le cardinal k de F. Et puisque les classes forment une partition de E, il s'ensuit que si p est le nombre de classes, alors $n = pk$. ■

On a en corollaire l'important résultat suivant :

Corollaire 2.3.3 *Si G est un groupe fini d'ordre n d'élément neutre e, alors pour tout élément a de G : $a^{(n)} = e$.*

Intéressons nous maintenant au **groupe symétrique** c'est-à-dire le groupe des permutations d'un ensemble fini. Muni de la loi de composition des applications (loi "o"), l'ensemble des bijections d'un ensemble E dans lui-même, est un groupe, non commutatif si E possède plus de 2 éléments. L'application identique i est l'élément neutre du groupe. Lorsque E est fini et possède n éléments, ces bijections s'appellent des permutations (autrefois appelées substitutions) et leur groupe en possède $n!$ (factorielle n) : c'est un groupe fini, appelé groupe symétrique de E souvent noté S_n (S comme substitution). Il n'est pas cyclique.

Exemple 2.3.10 Lorsque $E = \{a, b, c\}$, le groupe symétrique de E, soit S_3, possède donc 6 éléments. Désignons par xyz la permutation $a \to x$, $b \to y$, $c \to z$, on peut alors les écrire : $i = abc$, acb, bac, bca, cab, cba. Par exemple, par composition, on voit que bca est la permutation inverse de cab (symétrique de cab pour la loi o) :
. cab : $a \to c$, $b \to a$, $c \to b$
. bca : $a \to b$, $b \to c$, $c \to a$
. $bca_o cab$: $a \to a$, $b \to b$, $c \to c$
C'est dire que $bca_o cab = i$, soit $bca^{-1} = cab$. On a la table suivante

o	abc	cab	bca	cba	acb	bac
abc	abc	cab	bca	cba	acb	bac
cab	cab	bca	abc	bac	cba	acb
bca	bca	abc	cab	acb	bac	cba
cba	cba	acb	bac	abc	cab	bca
acb	acb	bac	cba	bca	abc	cab
bac	bac	cba	acb	cab	bca	abc

acb, bac et cba étant leur propre symétrique, ils ne peuvent engendrer le groupe. On vérifiera que $bca^{(3)} = cab^{(3)} = i$: le groupe n'est donc pas cyclique. Mais on peut noter que $H = \{abc, cab, bca\}$ est un sous-groupe cyclique de S_3. A un isomorphisme près, H est le seul groupe fini d'ordre 3 ; on peut l'identifier à $\mathbb{Z}/3\mathbb{Z}$.

Théorème 2.3.12 *(Arthur CAYLEY (1821-1895)) Tout groupe fini d'ordre n est isomorphe à un sous-groupe du groupe symétrique S_n (lequel possède $n! = 1 \times 2 \ldots (n-1) \times n$ éléments).*

Définition 2.3.17 *Une permutation opérant sur $(x, y, z, \ldots, t, u)$ est dite* ***circulaire*** *pour signifier que $(x, y, z, \ldots, t, u)$ est transformé en $(y, z, \ldots, u, x)$: tout est décalé d'un rang et le dernier terme prend la place du premier.*

2.4 Les anneaux

Le terme est de David HILBERT (1862-1943).

2.4.1 Les anneaux

L'étude des anneaux trouve sa source dans la théorie des polynômes et la théorie des entiers algébriques. Richard Dedekind fut le premier à introduire le concept d'anneau mais le terme "anneau" (ou plus précisément le terme allemand Zahlring) a été utilisé en premier par David Hilbert en 1897. La première définition axiomatique d'un anneau fut donnée par Abraham Adolf FRAENKEL (1891-1965) en 1914 et Emmy Noether donna quant-à elle la première fondation axiomatique de la théorie des anneaux commutatifs dans son remarquable article "Ideal Theory in Rings" en 1921.

Définition 2.4.1 *On appelle ainsi un groupe abélien $(A, +)$ muni d'une seconde loi, souvent appelée multiplication, notée ici "$\times$", associative et distributive sur ou par rapport à la loi de groupe (addition), c'est-à-dire que pour tout triplet (a, b, c) d'éléments de A :*

- $(a \times b) \times c = a \times (b \times c)$ *(associativité)*
- $a \times (b + c) = a \times b + a \times c$ *et* $(a + b) \times c = a \times c + b \times c$ *(distributivité)*

Par conséquent, un anneau est un triplet $(A, +, \times)$ tel que :

- A est un ensemble ;
- $+$ est une loi de composition interne telle que $(A, +)$ soit un groupe commutatif ; ce qui implique que
  - la loi $+$ est associative ;
  - A contient au moins un élément : l'élément neutre pour la loi $+$, noté 0 ;
  - tout élément a de A a un opposé, noté $-a$;
  - la loi $+$ est commutative $(a + b = b + a)$;
- $\times$ est une loi de composition interne associative et distributive par rapport à $+$;

Remarque 2.4.1 Si seule est vérifiée l'égalité $a \times (b+c) = a \times b + a \times c$, on parle de distributivité à gauche. Si seule est vérifiée l'égalité $(a+b) \times c = a \times c + b \times c$, on parle de distributivité à droite. Mais pour un anneau, on doit avoir la distributivité à gauche et à droite : on parle d'ailleurs parfois de double distributivité.

Définition 2.4.2 *L'anneau est dit* ***unifère*** *(ou unitaire) si sa multiplication admet un élément neutre. Cet élément est dit* ***unité****. Il est dit* ***commutatif*** *si sa multiplication est commutative. L'élément neutre du groupe est dit* ***nul*** *et souvent appelé zéro par analogie avec l'anneau* $(\mathbb{Z}, +, \times)$.

Exemple 2.4.1

- L'ensemble des entiers relatifs, $\mathbb{Z}$, muni de l'addition (la loi $+$) et de la multiplication (la loi $\times$) est un anneau.
- L'ensemble des entiers congruents modulo un nombre entier donné n est un anneau pour la loi provenant de la congruence ; il est noté $\mathbb{Z}/n\mathbb{Z}$.
  Ainsi $\mathbb{Z}/2\mathbb{Z}$ pour les lois $+$ et $\times$ est un anneau. 0 correspond aux nombres pairs et 1 aux nombres impairs. On retrouve alors les résultats suivants :
  - Un pair plus un pair est pair $(0 + 0 = 0)$.
  - Un impair plus un pair est impair $(0 + 1 = 1 + 0 = 1)$.
  - Un impair plus un impair est pair $(1 + 1 = 0)$.
  - Un pair fois un entier quelconque est pair $(0 \times x = 0)$.
  - Un impair fois un impair est impair $(1 \times 1 = 1)$.
- Un corps (voir plus loin) est un cas particulier d'anneau. En particulier, l'ensemble des nombres rationnels muni de l'addition et de la multiplication usuelles est un anneau.
- L'ensemble des réels s'écrivant $a + b\sqrt{2}$, où a et b sont des entiers relatifs, muni de l'addition et de la multiplication usuelles est un anneau.
- Les endomorphismes d'un espace vectoriel (applications linéaires de l'espace vers lui-même) forment un anneau, avec l'addition de fonction pour la loi $+$, et la composition pour la loi $\times$. L'identité est un élément neutre pour $\times$, donc c'est un anneau unifère. Il n'est pas commutatif en général. C'est une grande source de contre-exemples à des affirmations fausses sur les anneaux.
- Plus généralement les endomorphismes d'un groupe abélien forment un anneau.
- En particulier, l'ensemble des matrices 2×2 muni de l'addition et de la multiplication est aussi un anneau non commutatif unifère.
- L'ensemble des polynômes à coefficients dans un anneau est aussi un anneau.
- L'ensemble des fonctions d'un ensemble dans un anneau muni des lois héritées de l'anneau (c'est-à-dire $(f+g)(x) = f(x) + g(x)$ et $(f \times g)(x) = f(x) \times g(x)$) forme un anneau.

Exercice 55 (*non corrigé*) Soit $(A, +, \times)$ un anneau et h un homomorphisme de A vers un ensemble muni de deux lois de composition internes $(E, \oplus, \otimes)$. Prouver que l'image homomorphe $(h(A), \oplus, \otimes)$ est un anneau.

Exercice 56 Un élément x d'un anneau A est dit **nilpotent** s'il existe un entier $n \geq 1$ tel que $x^n = 0$. On suppose que A est commutatif, et on fixe x, y deux éléments nilpotents.

1. Montrer que xy est nilpotent.
2. Montrer que $x + y$ est nilpotent.
3. Montrer que $1_A - x$ est inversible.
4. Soient u, $v \in A$ tels que uv est nilpotent. Montrer que vu est nilpotent.

Correction : Soient n, m tels que $x^n = 0$ et $y^m = 0$.

1. Puisque x et y commutent, on a $(xy)^n = x^n y^n = 0 \times y^n = 0$.

2. Remarquons d'abord que pour $p \geq n$, on a $x^p = x^{p-n}x^n = 0$. D'après la formule du binôme, $(x+y)^{n+m} = \sum_{k=0}^{n+m} \begin{pmatrix} n+m \\ k \end{pmatrix} x^k y^{n+m-k}$. Mais, pour $k \geq n$, $x^k = 0 \Rightarrow x^k y^{n+m-k} = 0$. D'autre part, pour $k < n$, on a $n+m-k \geq m$ et donc $y^{n+m-k} = 0 \Rightarrow x^k y^{n+m-k} = 0$. Ainsi, $(x+y)^{n+m} = 0$. On pourrait même se contenter de prendre la puissance $n+m-1$.
3. L'idée est d'utiliser l'identité remarquable (toujours valable dans un anneau)
$$1 - x^p = (1-x)(1+x+\ldots+x^{p-1}).$$
Si on l'applique pour $p = n$, alors on obtient $1 - x^n = 1 = (1-x)(1+x+\ldots+x^{n-1})$ ce qui implique que $1-x$ est inversible d'inverse $1+x+\ldots+x^{n-1}$.
4. Soit $n \geq 1$ tel que $(uv)^n = 0$. Alors $(vu)^{n+1} = v(uv)^n u = v \times 0 \times u = 0$. Ainsi, vu est nilpotent.

Exercice 57 Soit A un anneau non nécessairement commutatif et soient $a, b \in A$ tels que $1-ab$ soit inversible. Montrer qu'alors $1-ba$ est également inversible.
Correction : Soit c l'inverse de $1-ab$. On a
$$(1+bca)(1-ba) = 1 - ba + bca - bcaba = 1 - ba + bc(1-ab)a = 1 - ba + ba = 1$$
$$(1-ba)(1+bca) = 1 - ba + bca - babca = 1 - ba + b(1-ab)ca = 1 - ba + ba = 1$$
Ainsi $1-ba$ est inversible d'inverse $1+bca$.

Exercice 58 Soit A un anneau commutatif. On appelle **élément idempotent** tout élément $x \in A$ vérifiant $x^2 = x$.

1. Si A est le produit de deux anneaux B et C, montrer qu'il existe des éléments idempotents de A distincts de 0 et de 1.
2. Supposons qu'il existe un élément $b \in A$ idempotent distinct de 0 et de 1. On pose $c = 1-b$, $B = bA$ et $C = cA$.
   (a) Montrer que c est idempotent et que $bc = 0$.
   (b) Montrer que B et C sont stables pour l'addition et la multiplication de A. En déduire que B et C sont des anneaux non nuls.
   (c) Montrer que l'application
   $$\begin{array}{rcl} \varphi : A & \to & B \times C \\ x & \mapsto & (bx, cx) \end{array}$$
   est un isomorphisme d'anneaux (qui permet d'identifier A avec $B \times C$).
   (d) Les anneaux B et C sont-ils des sous-anneaux de A ?

Correction :

1. Les éléments $0_A = (0_B, 0_C)$ et $1_A = (1_B, 1_C)$ sont des éléments idempotents, mais il en est de même des éléments $(0_B, 1_C)$ et $(1_B, 0_C)$.
2. (a) On a
   $$c^2 = (1-b)^2 = 1 - 2b + b^2 = 1 - 2b + b = 1 - b = c$$
   $$bc = b(1-b) = b - b^2 = b - b = 0$$
   ainsi c est un élément idempotent de A et $bc = 0$.
   (b) Soient $x, y \in B$, il existe $x', y' \in A$ tels que $x = bx'$ et $y = by'$. Alors $x+y = bx' + by' = b(x'+y') \in B$ et $xy = bx'by' = b(x'by') \in B$. Ainsi B est stable pour l'addition et la multiplication et donc leurs restrictions sont des lois de composition interne dans B. Comme ces lois sont commutatives, associatives et l'une distributive sur l'autre dans A, il en est de même de leurs restrictions à B. Et

0 étant l'élément neutre pour l'addition dans A et appartenant à B, c'est l'élément neutre pour l'addition dans B. Soit $x \in B$, il existe $b' \in A$ tel que $x = bx'$ et $bx = bbx' = bx' = x$ donc b est l'élément neutre pour la multiplication dans B. Ainsi B est un anneau commutatif non nul. De même C est un anneau commutatif non nul.

(c) Soient $x, y \in A$. On a

$$\varphi(x+y) = (b(x+y), c(x+y)) = (bx+by, cx+cy) = (bx, cx) + (by, cy) = \varphi(x) + \varphi(y)$$
$$\varphi(xy) = (bxy, cxy) = (bxby, cxcy) = (bx, cx)(by, cy) = \varphi(x)\varphi(y)$$

Et $\varphi(1) = (b, c)$, qui est l'élément neutre de $B \times C$. Ainsi φ est un morphisme d'anneaux.
Soit $x \in A$, on a

$$\varphi(x) = 0 \Rightarrow (bx, cx) = 0 \Rightarrow bx = cx = 0 \Rightarrow x = (b+c)x = 0$$

Donc φ est injective.
Soit $(x, y) \in B \times C$, il existe $x', y' \in A$ tels que $x = bx'$ et $y = cy'$. Alors

$$\varphi(x+y) = (b(bx'+cy'), c(bx'+cy')) = (b^2x' + bcy', cbx' + c^2y') = (bx', cy') = (x, y)$$

Donc φ est surjective. Ainsi φ est un isomorphisme d'anneaux de A sur $B \times C$.

(d) Les anneaux B et C ne sont pas des sous-anneaux de A car ils n'ont pas les mêmes éléments unités (voir section suivante).

2.4.2 Sous-anneau

Définition 2.4.3 *Une partie B de A est un **sous-anneau** de A si, muni des opérations de A, B est lui-même un anneau. Pour qu'il en soit ainsi il faut et il suffit que :*

- *B soit un sous-groupe de A,*
- *pour tout couple (u, v) d'éléments de B, $u \times v$ soit élément de B.*

Exemple 2.4.2

- $(\mathbb{Z}, +, \times)$, anneau des entiers relatifs, est un sous-anneau de $(\mathbb{Q}, +, \times)$, anneau des nombres rationnels.
- Tout sous-groupe de $\mathbb{Z}$ contenant 1 est $\mathbb{Z}$ lui-même. On en déduit que le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même.

Exercice 59 Montrer que l'ensemble $\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2}/(a, b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$.
Correction : Tout est très simple, il ne faut juste oublier aucune vérification : $\mathbb{Z}[i\sqrt{2}]$ contient 0 et 1, est stable par somme et par produit, et par opposé, c'est un sous-anneau de $\mathbb{C}$.

Exercice 60 On considère $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau.
2. On note $N(a + b\sqrt{2}) = a^2 - 2b^2$. Montrer que, pour tous x, y de $\mathbb{Z}[\sqrt{2}]$, on a $N(xy) = N(x)N(y)$.
3. En déduire que les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont ceux s'écrivant $a + b\sqrt{2}$ avec $a^2 - 2b^2 = \pm 1$.

Correction :

1. Il suffit de prouver que $\mathbb{Z}[\sqrt{2}]$ un sous-anneau de $(\mathbb{R}, +, \times)$. $\mathbb{Z}[\sqrt{2}]$ est
   - stable par la loi + : $(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2}$.
   - stable par la loi × : $(a + b\sqrt{2}) \times (a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2}$.
   - stable par passage à l'opposé $-(a + b\sqrt{2}) = -a + (-b)\sqrt{2}$.

   De plus, 0 et $1 \in \mathbb{Z}[\sqrt{2}]$, ce qui achève la preuve.
2. Posons $x = a + b\sqrt{2}$ et $y = a' + b'\sqrt{2}$. En tenant compte de la formule pour le produit obtenue à la question précédente, on a $N(xy) = (aa' + 2bb')^2 - 2(ab' + a'b)^2 = (aa')^2 - 2(ab')^2 - 2(a'b)^2 + (4bb')^2$. D'autre part, $N(x) \times N(y) = (a^2 - 2b^2)(a'2 - 2b'^2) = (aa')^2 - 2(ab')^2 - 2(a'b)^2 + (4bb')^2$.

3. Soit $x = a + b\sqrt{2}$. Supposons d'abord que x est inversible, d'inverse y. Alors $N(xy) = N(1) = 1$, et donc $N(x)N(y) = 1$. Puisque $N(x)$ et $N(y)$ sont tous les deux des entiers, on a nécessairement $N(x) = \pm 1$. Réciproquement, si $N(x) = \pm 1$, alors, en utilisant la quantité conjuguée : $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \pm(a - b\sqrt{2})$ ce qui montre que $a + b\sqrt{2}$ est inversible, d'inverse $\pm(a - b\sqrt{2})$.

Exercice 61 Montrer que l'ensemble des suites réelles, muni de la somme et du produit terme par terme, est un anneau. Quels sont ses éléments inversibles (pour le produit) ? Parmi les ensembles suivants, lesquels en sont des sous-groupes ou des sous-anneaux :

1. suites bornées
2. suites monotones
3. suites convergentes
4. suites périodiques
5. suites divergeant vers $+\infty$

Correction : Le fait que l'ensemble des suites soit un anneau ne pose aucun problème. L'associativité et la commutativité des deux lois découlent de celles des opérations similaires sur les réels, puisqu'on fait les sommes et produits terme à terme. L'élément neutre pour la somme est la suite nulle, et celui pour le produit est la suite constante égale à 1. Enfin, l'opposé d'une suite (u_n) est la suite $(-u_n)$. Les suites inversibles sont celles qui ne s'annulent jamais, on peut alors inverser terme à terme.

1. Les suites bornées forment un sous-anneau de cet anneau : le sous-anneau contient les neutres, il est stable par opposition (si $m \leq u_n \leq M$) pour tout n, on a $(-M \leq u_n \leq -m)$, par somme (il suffit de prendre la somme des bornes) et même par produit (c'est un peu plus compliqué à cause des changements de signes, mais en prenant le plus gros produit parmi les valeurs absolues des quatre possibles, c'est un majorant du produit des deux suites).
2. Les suites monotones ne forment pas un sous-anneau, ce n'est pas stable par somme (une croissante plus une décroissante, cela peut donner n'importe quoi).
3. Pour les suites convergentes, aucun problème, les stabilités découlent des propriétés sur les limites de suites.
4. Les suites périodiques forment aussi un sous-anneau : il contient les neutres (une suite constante est périodique de période 1), stable par opposition (même période) et par somme et produit (le produit des deux périodes, par exemple, est alors une période).
5. Les suites divergeant vers $+\infty$ ne forment pas un sous-anneau, ce n'est pas stable par passage à l'opposé.

2.4.3 Anneau intègre, diviseur de zéro

Définition 2.4.4 *Un anneau est dit* ***intègre*** *si un produit nul nécessite que l'un des facteurs soit nul (égal à l'élément neutre pour l'addition). Lorsqu'un produit a.b est nul alors que ni a, ni b le sont, on dit que a et b sont des* ***diviseurs de zéro****.*

Justifions cette appellation par un exemple fondamental :

Exemple 2.4.3 L'ensemble des matrices carrées d'ordre 2 à termes réels muni de l'addition et de la multiplication usuelles $(\mathcal{M}_2(\mathbb{R}), +, \times)$ est un anneau unitaire non commutatif et non intègre.
On a ce résultat étonnant puisqu'on est habitué à rencontrer un produit nul si et seulement si l'un des facteurs est nul :

$$\begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix} \times \begin{pmatrix} 2 & -1 \\ -4 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Le produit de deux matrices non nulles peut être nul !

Exemple 2.4.4
- L'ensemble $\mathbb{Z}$ des entiers relatifs est un anneau intègre.
- L'anneau des congruences modulo 6 noté $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre car on peut y écrire $\overline{3} \times \overline{2} = \overline{6} = \overline{0}$.
- L'anneau $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ n'est pas intègre, $(\overline{1}, \overline{0})$ et $(\overline{0}, \overline{1})$ sont deux éléments non nuls dont le produit est nul.

Ce dernier exemple découle de la proposition suivante :

Proposition 2.4.1 *L'anneau des congruences modulo n noté $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.*

Preuve : Cette proposition est une conséquence directe de l'identité de Bézout (Étienne BÉZOUT 1730-1783). Supposons n premier, alors si a est un entier premier avec n, c'est-à-dire non multiple de n, il existe deux entiers b et c tels que $ab + nc = 1$, ce qui signifie que la classe de a est inversible d'inverse la classe de b. Réciproquement si n n'est pas premier, il existe deux entiers a et b différents de n et de 1 tels que leur produit est égal à n. La classe de a ainsi que la classe de b sont donc des diviseurs de zéro. ■

Exercice 62 Soit E un ensemble. Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau. En préciser les éléments neutres, les éléments inversibles (et leur inverse) pour chacune des deux lois. Cet anneau est-il intègre ? Si $F \subset E$, $(\mathcal{P}(F), \Delta, \cap)$ est-il un sous-anneau de $\mathcal{P}(E)$?
Correction : Les deux lois Δ et $\cap$ sont internes, commutatives, associatives et distributives l'une par rapport à l'autre. De plus, Δ possède un élément neutre qui est $\emptyset$, $\cap$ possède pour élément neutre E, et tout élément A de $\mathcal{P}(E)$ est inversible pour Δ, son inverse étant lui-même puisque $A\Delta A = (A \backslash A) \cup (A \backslash A) = \emptyset$. On est donc bien en présence d'un anneau.
Les éléments inversibles pour $\cap$ sont les parties A de E telles qu'il existe $B \subset E$ pour laquelle $A \cap B = E$. Ceci ne peut se produire que si $A = B = E$, donc le neutre est le seul élément inversible pour $\cap$. Pour que l'anneau soit intègre, il faudrait avoir $A \cap B = \emptyset \Rightarrow A = \emptyset$ ou $B = \emptyset$, ce qui n'est pas le cas (il suffit de prendre A non vide tel que A est non vide, ce qu'on peut toujours trouver dans un ensemble comportant au moins deux éléments). Enfin, $(\mathcal{P}(F), \Delta, \cap)$ n'est pas un sous-anneau de E car il ne contient pas l'élément neutre pour l'intersection, bien qu'il soit lui-même un anneau.

2.4.4 Idéal d'anneau

En mathématiques, un idéal est une structure algébrique définie dans un anneau. Les idéaux généralisent de façon féconde l'étude de la divisibilité pour les entiers. Il est ainsi possible d'énoncer des versions très générales de théorèmes d'arithmétique tels que le théorème des restes chinois ou le théorème fondamental de l'arithmétique, valables pour les idéaux. On peut aussi comparer cette notion à celle de sous-groupe distingué pour la structure algébrique de groupe en ce sens qu'elle permet de définir la notion d'anneau quotient.

Définition 2.4.5 *Un **idéal d'anneau** est un sous-groupe additif J d'un anneau A stable pour le produit par un élément de A (seconde loi).*

Par stabilité, on entend ici que pour tout a de A et tout x de J, les produits $a \times x$ et $x \times a$ sont éléments de J. Une telle partie est souvent qualifiée de bilatère. Un idéal à gauche (respectivement à droite) se limite à la condition $a \times x$ (respectivement $x \times a$) est élément de J.

Exemple 2.4.5 Un exemple élémentaire est donné par les sous-groupes additifs de $\mathbb{Z}$ de la forme $n\mathbb{Z}$, ensemble des multiples de l'entier relatif n.

Remarque 2.4.2 Un idéal joue, pour les anneaux, le même rôle que les sous-groupes distingués pour les groupes.

- Soient A et B deux anneaux et f un morphisme de A dans B, alors le noyau de f est un idéal bilatère.
- Soient A un anneau et I un idéal bilatère de A, alors le groupe quotient A/I peut être muni d'une unique structure d'anneau telle que la surjection canonique de A dans A/I soit un morphisme d'anneaux.
- Soient A et B deux anneaux, φ un morphisme d'anneau de A dans B. Notons s l'application canonique de A dans l'anneau quotient A/I et i le morphisme de $f(A)$ dans B qui à b associe b. Alors, i est une injection, s une surjection et il existe une bijection b telle que $\varphi = i_o b_o s$ (on a utilisé le théorème de décomposition canonique avec $\nu = i_o b$ où ν est un isomorphisme de A/I sur $\varphi(A)$).

Définition 2.4.6 *Soient A un anneau commutatif unitaire, a un élément de A et I un idéal de A. Un idéal I de A est dit* ***premier*** *si et seulement si le quotient de A par I est intègre et qu'il est différent de l'anneau réduit à l'élément nul.*

On peut exprimer cette définition à l'aide de la condition suivante :

Proposition 2.4.2 *Un idéal I de A est premier si et seulement si c'est un idéal propre (différent de A) et si :*

$$\forall x, y \in A,\ xy \in I \Rightarrow x \in I \text{ ou } y \in I$$

Cette proposition est l'équivalent du lemme d'Euclide : "si un nombre premier divise le produit ab alors il divise soit a soit b".

Exemple 2.4.6 Si n est un nombre premier, $I = n\mathbb{Z}$ est un idéal premier. En effet, d'après la proposition 2.4.1, $\mathbb{Z}/n\mathbb{Z}$ est intègre ssi n est premier.

Définition 2.4.7 *Soit A un anneau. Soit I un idéal de A.*

- *I est dit* ***principal à gauche*** *s'il existe un élément $a \in I$ tel que, pour tout $x \in I$, il existe un élément $y \in A$ tel que $x = y \times a$: $I = \{x \times a / x \in A\}$. On note $I = Aa$.*
- *I est dit* ***principal à droite*** *s'il existe un élément $a \in I$ tel que, pour tout $x \in I$, il existe un élément $y \in I$ tel que $x = a \times y$: $I = \{a \times x / x \in A\}$. On note $I = aA$.*
- *I est dit* ***principal*** *s'il est principal à la fois à gauche et à droite (ce qui est toujours le cas si A est commutatif). Dans ce cas, on peut noter $I = aA$ et I est forcément le plus petit idéal contenant a.*

Exemple 2.4.7

- Pour tout entier relatif k, $k\mathbb{Z} = \{kx / x \in \mathbb{Z}\}$ est un idéal principal de $\mathbb{Z}$.
- Un idéal n'est pas forcément principal. Par exemple, si $A = \mathbb{C}[X, Y]$, l'anneau commutatif des polynômes à deux indéterminées à coefficients complexes, l'ensemble des polynômes ayant un terme constant nul, noté (X, Y) car engendré par ces deux variables, est un idéal de $\mathbb{C}[X, Y]$, mais il n'est pas principal : si P engendrait (X, Y), X et Y seraient divisibles par P, ce qui est impossible, sauf si P est un polynôme constant non nul, ce qui est contradictoire.

Définition 2.4.8 *Un anneau intègre dont tous les idéaux sont principaux est dit* ***anneau principal****.*

Les anneaux principaux forment un type d'anneaux important dans la théorie mathématique de la divisibilité. Ce sont les anneaux intègres (commutatifs unitaires non nuls) auxquels on peut étendre deux théorèmes qui, au sens strict, concernent l'anneau des entiers relatifs : le théorème de Bachet-Bézout et le théorème fondamental de l'arithmétique qu'on rappelle :

Théorème de Bachet-Bézout : Si a et b sont deux éléments de A n'ayant pas d'autres diviseurs communs que les éléments du groupe des unités de l'anneau, alors il existe u et v éléments du groupe tel que $a \times u + b \times v = 1$.

Théorème fondamental de l'arithmétique : Un anneau principal est un anneau factoriel, c'est-à-dire que tout élément de l'anneau se décompose de manière unique en un produit de facteurs irréductibles et d'une unité (à un facteur inversible près).

Exemple 2.4.8 $\mathbb{Z}$ ou l'anneau $\mathbb{K}[X]$ des polynômes sur un corps $\mathbb{K}$ sont des anneaux principaux.

Définition 2.4.9 *Un* ***anneau euclidien*** *est un anneau disposant d'une division euclidienne. Un tel anneau est toujours principal.*

Exemple 2.4.9 Des exemples de cette nature sont donnés par
- l'ensemble des entiers relatifs $\mathbb{Z}$,
- l'ensemble des polynômes à coefficients dans un corps, par exemple celui des rationnels, réels ou complexes.

Remarque 2.4.3 Tous les anneaux principaux ne sont pas euclidiens

2.4.5 Intersection, somme et produit d'idéaux

Proposition 2.4.3 *Dans un anneau A, l'****intersection*** *de deux idéaux est un idéal. Et toute intersection d'idéaux de A est un idéal de A. Un idéal est dit* ***irréductible*** *s'il ne peut s'écrire comme intersection de deux idéaux de A.*

Définition 2.4.10 *Comme pour un sous-espace vectoriel, on définit la somme $K = I + J$ de deux idéaux I et J d'un anneau commutatif A comme étant l'ensemble des éléments z de A s'écrivant $x + y$ où x est élément de I et y élément de J.*

Définition 2.4.11 *Dans un anneau A, le* ***produit*** *de deux idéaux I et J est l'ensemble des sommes finies d'éléments de la forme $x_i y_i$ où x_i est dans I et y_i dans J.*

On vérifie facilement que l'ensemble IJ ainsi défini est un idéal de A.

Exercice 63 (*non corrigé*) Vérifier la chaîne d'inclusion : $IJ \subset (I \cap J) \subset (I \cup J) \subset I + J$.

Exercice 64 (*non corrigé*)

1. Justifier que l'intersection de deux idéaux est un idéal.
2. Montrer par un exemple que la réunion de deux idéaux n'en est pas toujours un !
3. Montrer que la somme de deux idéaux contient leur intersection. Étudier l'inclusion inverse.
4. Dans $\mathbb{Z}$, quel est l'idéal défini par $18\mathbb{Z} + 24\mathbb{Z}, 2\mathbb{Z} + 4\mathbb{Z}, 2\mathbb{Z} + 3\mathbb{Z}$? (mot clé : pgcd)

Exercice 65 *Le théorème chinois dans un anneau commutatif*

Soient I et J deux idéaux d'un anneau commutatif A tels que $I + J = A$.

1. Établir que $I \cap J = IJ$.
2. On considère l'application $\varphi : A \to A/I \times A/J$ qui à $x \in A$ associe le couple de ses classes modulo I et J. Montrer que φ est un morphisme d'anneaux et déterminer son noyau.
3. Montrer que les anneaux A/IJ et $A/I \times A/J$ sont isomorphes.

Correction :

1. Soient $x \in I$ et $y \in J$. Puisque I et J sont des idéaux, on a $xy \in I$ et $xy \in J$, d'où $xy \in I \cap J$. Puisque IJ est l'idéal engendré par les produits xy, $x \in I$ et $y \in J$, et puisque $I \cap J$ est un idéal, on a $IJ \subset (I \cap J)$.
   Réciproquement, puisque $I + J = A$, il existe $u \in I$ et $v \in J$ tels que $u + v = 1$ (élément neutre de A pour la seconde loi). Soit $x \in I \cap J$, on a alors $x = xu + xv \in IJ$ car $x \in J$, $u \in I$ et $x \in I$, $v \in J$. Donc $(I \cap J) \subset IJ$. Ainsi $I \cap J = IJ$.

2. Soient π_I et π_J les surjections canoniques de A sur A/I et A/J respectivement. Ce sont des morphismes d'anneaux et $\forall x \in A$,

$$\varphi(x) = (\pi_I(x), \pi_J(x)).$$

On a $\varphi(1_A) = (\pi_I(1_A), \pi_J(1_A)) = (1_{A/I}, 1_{A/J}) = 1_{A/I \times A/J}$.
Soient $x, y \in A$, on a

$$\varphi(x+y) = (\pi_I(x+y), \pi_J(x+y)) = (\pi_I(x) + \pi_I(y), \pi_J(x) + \pi_J(y)) = (\pi_I(x), \pi_J(x)) + (\pi_I(y), \pi_J(y)) = \varphi(x) + \varphi(y)$$
$$\varphi(xy) = (\pi_I(xy), \pi_J(xy)) = (\pi_I(x)\pi_I(y), \pi_J(x)\pi_J(y)) = (\pi_I(x), \pi_J(x))(\pi_I(y), \pi_J(y)) = \varphi(x)\varphi(y)$$

Donc φ est un morphisme d'anneaux.
Soit $x \in A$, on a

$$x \in Ker(\varphi) \Leftrightarrow \varphi(x) = 0 \Leftrightarrow (\pi_I(x), \pi_J(x)) = 0 \Leftrightarrow \left\{ \begin{array}{l} \pi_I(x) = 0 \\ \pi_J(x) = 0 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} x \in I \\ x \in J \end{array} \right. \Leftrightarrow x \in I \cap J \Leftrightarrow x \in IJ.$$

Ainsi le noyau de φ est l'idéal IJ.

3. Puisque $Ker(\varphi) = IJ$, φ induit par passage au quotient un morphisme injectif d'anneaux $\overline{\varphi} : A/IJ \to A/I \times A/J$ qui à $x \in A/IJ$ associe $(\pi_I(x'), \pi_J(x'))$ où x' est un représentant de x dans A. De plus $Im(\overline{\varphi}) = Im(\varphi)$, donc pour montrer que $\overline{\varphi}$ est surjectif, il suffit de montrer que φ est surjectif. Soit $(x, y) \in A/I \times A/J$. Soient x', $y' \in A$ tels que $x = \pi_I(x')$ et $y = \pi_J(y')$. Soient $u \in I$ et $v \in J$, on a

$$\varphi(x'v + y'u) = (\pi_I(x'v + y'u), \pi_J(x'v + y'u)) = (\pi_I(x')\pi_I(v) + \pi_I(y')\pi_I(u), \pi_J(x')\pi_J(v) + \pi_J(y')\pi_J(u)) = (\pi_I(x'), \pi_J(y')) = (x, y)$$

car $\pi_I(u) = 0$ ($u \in I$), $\pi_J(v) = 0$ ($v \in J$), $\pi_I(v) = 1$ et $\pi_J(v) = 1$ ($u + v = 1$). Ainsi φ est surjectif.
En conclusion φ est un isomorphisme d'anneaux et les anneaux A/IJ et $A/I \times A/J$ sont isomorphes.

Exercice 66 (*Théoème des restes chinois)* Soient deux nombres entiers p et q premiers entre eux.

1. Montrer que $\mathbb{Z}/pq\mathbb{Z}$ est isomorphe au produit $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.
2. Un général chinois est parti pour une bataille avec 386 soldats. À la fin du combat, il souhaite compter ses troupes. Il leur ordonne de se mettre en rang de p soldats et il note le nombre de soldats formant la dernière rangée incomplète. Puis il procède de même mais en les faisant se mettre en rang de q soldats. Quelles valeurs de p et q doit-il prendre ?
Expliquer comment il s'y prend finalement pour compter précisement ses soldats.
3. Que peut-on dire si p n'est pas premier avec q ?

Correction : On rappelle que si p et q sont premiers entre-eux, $ppcm(p, q) = pq = n$ et $pgcd(p, q) = 1$.

1. On considère l'application

$$\begin{array}{rcl} \varphi : \mathbb{Z}/pq\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ \alpha & \mapsto & (\alpha[p], \alpha[q]) \end{array}$$

où $\alpha[r]$ est le reste de la division euclidienne de α par r. Par exemple, si $p = 2$ et $q = 3$, $\varphi(15) = (1, 0)$. Cette application est un isomorphisme de groupes (voir exercice précédent). On remarquera que les deux ensembles $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ ont le même nombre d'éléments. On le constate en considérant par exemple $p = 2$ et $q = 3$: $\mathbb{Z}/(2 \times 3)\mathbb{Z} = \mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{5}\}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}\} \times \{\overline{0}, \overline{1}, \overline{2}\}$.

2. D'après les données, si x désigne le nombre de soldats vivants à la fin du combat, on a :
   - $x \equiv p_1[p] \Leftrightarrow \exists k \in \mathbb{Z}, x = kp + p_1$ où k et p_1 désignent respectivement le nombre de rangées de p soldats et le nombre de soldats formant la dernière rangée incomplète,
   - $x \equiv q_1[q] \Leftrightarrow \exists k' \in \mathbb{Z}, x = k'q + q_1$ où k' et q_1 désignent respectivement le nombre de rangées de q soldats et le nombre de soldats formant la dernière rangée incomplète.

On a alors $\varphi(x) = (p_1, q_1)$. φ étant un isomorphisme, on est assuré de l'existence et de l'unicité de la solution recherchée pour p et q donnés. p et q sont premiers entre-eux donc d'après le théorème de Bézout, on peut trouver $u, v \in \mathbb{Z}$ tels que $up+vq = 1$. Ainsi, $x = upx+vqx = up(q_1+k'q)+vq(p_1+kp) = upq_1 + vqp_1 + (upk'q + vqkp) = upq_1 + vqp_1 + Kn$ avec $K = uk' + vk \in \mathbb{Z}$. Modulo $n = pq$, une solution du problème est donnée par $x = upq_1 + vqp_1$.

3. Si p et q ne sont pas premiers entre-eux, le morphisme φ n'est qu'injectif. Il existe une solution au problème initial si et seulement si les données sont dans l'image, c'est-à-dire si et seulement si $p_1 \equiv q_1[pgcd(p, q)]$ (ou ssi $pgcd(p, q)$ divise $p_1 - q_1$).

2.5 Les Corps

C'est Richard Dedekind qui définit pour la première fois la structure de corps (Körper en allemand) et c'est la raison pour laquelle un corps quelconque est souvent nommé K ou $\mathbb{K}$. La structure de corps s'insère dans une hiérarchie comprenant le monoïde, le groupe, l'anneau, et donne lieu à la définition de l'espace vectoriel, et de l'algèbre.

De manière informelle, un corps est un ensemble dans lequel il est possible d'effectuer des additions, des soustractions, des multiplications et des divisions.

Définition 2.5.1 *Un anneau dans lequel tout élément non nul admet un symétrique pour la multiplication (souvent appelé inverse) est un* ***corps****. En particulier, un corps est un anneau intègre. Si la multiplication (seconde loi) est commutative, le corps est dit commutatif.*

Un corps est donc un ensemble $\mathbb{K}$ muni de deux lois internes notées en général $+$ et $\times$ vérifiant
- $(\mathbb{K}, +)$ forme un groupe commutatif dont l'élément neutre est noté 0,
- $(\mathbb{K}\backslash\{0\}, \times)$ forme un groupe multiplicatif,
- la multiplication est distributive pour l'addition (à gauche comme à droite) c'est-à-dire que
$$\forall a, b, c \in \mathbb{K},\ a \times (b + c) = a \times b + a \times c \text{ et } (b + c) \times a = b \times a + c \times a$$

On parle alors du corps $(\mathbb{K}, +, \times)$.

Définition 2.5.2 *Un* ***sous-corps*** *d'un corps $\mathbb{K}$ est un sous-anneau $\mathbb{K}'$ de $\mathbb{K}$ tel que pour tout x de $\mathbb{K}'$, son inverse soit élément de $\mathbb{K}'$. On dit inversement que $\mathbb{K}$ est un* ***sur-corps*** *de $\mathbb{K}'$.*

Exemple 2.5.1
- $\mathbb{R}$ et $\mathbb{C}$ munis de leurs opérations usuelles sont des corps commutatifs.
- $\mathbb{C}$ est un sur-corps de $\mathbb{R}$.
- $(\mathbb{Q}, +, x)$ est un corps commutatif, sous-corps de $(\mathbb{R}, +, x)$
- Le corps H de quaternions n'est pas commutatif (corps gauche).
- Les nombres constructibles constituent un sous-corps de $\mathbb{R}$.
- Si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo p est un corps fini (ayant un nombre fini d'éléments).
- $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre mais ce n'est pas un corps : les seuls éléments inversibles (ayant un inverse) sont 1 et - 1.
- $(\mathcal{M}_2(\mathbb{R}), +, \times)$ n'est pas un corps (voir ci-dessus). La division, on le sait dans le calcul élémentaire, n'est autre que la multiplication par l'inverse : dans le cas des matrices, on ne parle pas de diviseur mais d'inverse. L'inverse (s'il existe) d'une matrice carrée A est une matrice notée A^{-1} vérifiant $A^{-1} \times A = A \times A^{-1} = I$, où I est la matrice unité.
- Soit D l'ensemble des nombres décimaux (l'ensemble des nombres admettant un représentant de la forme $a \times 10^n$ avec $(a, n) \in \mathbb{Z}^2$. Par exemple $3/5$, $-7/4$ et $1,237$ sont décimaux. $(D, +, \times)$ est un anneau intègre, sous-anneau de $(\mathbb{Q}, +, \times)$. Ce n'est pas un corps, 3 par exemple est décimal mais pas son inverse $1/3$.

Remarque 2.5.1 L'ensemble $(\mathbb{Z}, +\times)$ n'est pas un corps car la plupart des éléments de $\mathbb{Z}^\star$ ne sont pas inversibles : par exemple, il n'existe pas d'entier relatif n tel que $2n = 1$ donc 2 n'est pas inversible.

Proposition 2.5.1 *Les seuls idéaux d'un corps sont l'idéal nul et le corps tout entier. Réciproquement si A est un anneau n'ayant comme seuls idéaux que l'idéal nul et lui même alors A est un corps.*

Preuve :

- Supposons que $\mathbb{K}$ est un corps. Soit I un idéal non nul de A. Soit donc x un élément non nul de I. x est, par définition d'un corps, inversible dans $\mathbb{K}$. Soit x^{-1} l'inverse de x dans $\mathbb{K}$. $x^{-1}x$ est, par définition d'un idéal, élément de I. Mais $x^{-1}x$ est égal à l'élément unité de $\mathbb{K}$. Donc $1 \in I$ et $I = \mathbb{K}$.
- Réciproquement, supposons maintenant que les seuls idéaux de l'anneau A sont l'idéal nul et A tout entier. Il nous suffit de montrer que tout les éléments non nuls de A sont inversibles. Soit $x \neq 0$ un élément de A. Soit (x) l'idéal engendré par x. Comme x n'est pas nul, cet idéal n'est pas nul non plus. Il est alors égal à A tout entier. L'unité de A est donc élément de (x). Ceci signifie qu'il existe y dans A tel que $xy = 1$. x est donc inversible d'inverse y. ■

Définition 2.5.3 *Un **corps fini** est un corps (commutatif) dont le cardinal est fini. À un isomorphisme près, un corps fini est entièrement déterminé par son cardinal qui est toujours de la forme p^n, une puissance d'un nombre premier. Ce nombre premier n'est autre que sa **caractéristique** et le corps se présente comme l'unique extension simple du corps premier $\mathbb{Z}/p\mathbb{Z}$ de dimension n.*

Théorème 2.5.1 *Théorème de Wedderburn (Joseph WEDDERBURN 1882-1948) Tout corps fini est commutatif.*

Preuve : http ://www.math.mcgill.ca/chenever/PDF/Wedderburn.pdf ■

Exercice 67 Soit A un anneau intègre de cardinal fini. Montrer que A est un corps.
Correction : Soit $a \in A$ non nul. L'application

$$\begin{array}{rccc} \mu_a : & A & \to & A \\ & x & \mapsto & ax \end{array}$$

est injective. En effet, puisque A est un anneau intègre et a est non nul, pour tous $x, y \in A$, on a $\mu_a(x) = \mu_a(y) \Rightarrow ax = ay \Rightarrow ax - ay = 0 \Rightarrow a(x-y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$.
Et comme A est un ensemble fini, toute injection de A dans A est une bijection. Ainsi μ_a est bijective. Soit $b \in A$ l'antécédent de 1 par μ_a. Alors $ab = \mu_a(b) = 1$. Et puisque A est un anneau commutatif, on a $ba = 1$ et b est l'inverse de a. Ainsi A est un corps.

Exercice 68 Soit $S\mathbb{K}$ un sous-corps d'un corps commutatif $\mathbb{K}$. Soient $P, Q \in S\mathbb{K}[X]$, P irréductible. On suppose que P et Q, considérés comme éléments de $\mathbb{K}[X]$, ont une racine commune. Montrer que P divise Q.
Correction : Soit D un *pgcd* de P et Q dans $S\mathbb{K}[X]$. L'algorithme d'Euclide est identique que l'on considère les polynômes P et Q dans $S\mathbb{K}[X]$ ou dans $\mathbb{K}[X]$, donc D est un *pgcd* de P et Q dans $\mathbb{K}[X]$. Puisque P et Q ont une racine commune dans $\mathbb{K}$, ils ne sont pas premiers entre eux et ainsi D est distinct de 1. Or P est irréductible dans $S\mathbb{K}[X]$, donc il existe $\lambda \in S\mathbb{K}\backslash\{0\}$ tel que $D = \lambda P$. Ainsi P divise Q.
Autre méthode : puisque P et Q ont une racine commune dans $\mathbb{K}$, il existe un idéal I de $\mathbb{K}[X]$ distinct de $\mathbb{K}[X]$ contenant P et Q. On pose $J = I/S\mathbb{K}[X]$, c'est un idéal de $S\mathbb{K}[X]$, distinct de $S\mathbb{K}[X]$ (sinon 1 appartiendrait à J, donc à I et alors I serait égal à $\mathbb{K}[X]$) et contenant P et Q. Puisque $S\mathbb{K}[X]$ est principal et P est irréductible, J est l'idéal engendré par P, donc P divise Q.