Université Mohamed El Bachir El Ibrahimi de Bordj Bou Arréridj
Faculté de Mathématiques et de l'Informatique
Département de Mathématiques

Mémoire

Présenté par

Chenahat Bouchra
Touahria Selma

Pour l'obtention du diplôme de

Master

Filière : Mathématiques

Spécialité :Analyse Mathématique et applications

Thème

Les espaces quotients

Soutenu publiquement Juillet 2019 devant le jury composé de

	Pr.	Université de Bordj Bou Arréridj	Président
Adimi Hadjer	*MAA.*	Université de Bordj Bou Arréridj	Encadreur
	MCA	Université de Bordj Bou Arréridj	Examinateur

Promotion 2018/2019

Remerciement

Le plus grand remerciement est au bon Dieu clément et miséricordieux qui m'a donné la force et la patience d'accomplir ce modeste travail.

Nous tenons à remercier très sincèrement tout d'abord mon encadreur Madame : «Adimi hadjer», pour sa confiance son orientation judicieuse, sa patience et diligence, ses précieux conseils ainsi que pour sa suggestion qui a grandement facilité ce travail.

En second lieu, Nous aimerions également remercier les membres du jury Mr. « ?» et Mr. « ? »
Pour l'intérêt qu'ils ont porté à cette recherche en acceptant d'examiner ce travail et de l'enrichir par leurs propositions.

Nous tenons aussi à remercier mes enseignantes Mme Benturki djamila , Mr Ramdhani et Mr Touati et tous les enseignants des années précédentes pour avoir œuvré à notre formation durant tous mes cinq ans, en signe d'un profond respect et d'un profond amour !

Dédicace

Je dédie ce modeste travail :
A mes parents pour leur soutien et leur Sacrificatrices, leurs encouragements pendant la durée de mes études : mon pére **Aissa** et ma mère **Horia**.
A mes frères.
A mes soeurs.
A toute la famille.
A toute mes amies sans exception .
Enfin je dédie ce mémoire à tous ceux qui me sont chers.
Ch. Bouchra

Dédicace

Je dédie ce travail
À cette source volonté, de patience et de générosité à **mon père Omar**
À la plus belle créature que Dieu a créée sur terre à **ma mère Ketfi tassadit**
À ma belle mère **Habiba** et le père de mon marie **Rabah**
Pour leur patience, leur amour, leur soutien, leurs encouragements et leurs sacrifices, pour que je puisse atteindre mes objectif
À mon marie Mohamed
À mes chèrs frères **Samir, Abdelwahabe , Abderahmane, Siffeddine, Rida et Mohamed**
À mes chères sœurs **Sabrina** et **Khadidja**
À mes chères **Lila, Warda, Hanane et Zahia**
À tout la famille de mon marie
À mes chères enfants
Malak, Maram, Aness, Elmouaiz, Abdelhak, Quosai, Rihame et Touta
À toute ma famille
À tous mes amis et mes collègues d'études spécialement **Bouchra, Randa**
À tous ceux qui ont contribué de près ou de loin pour que ce travail soit possible.

T.selma

Table des matières

Introduction

Le passage au quotient est une notion majeure en mathématiques. Sa vocation est de regrouper des éléments ayant la même propriété et de changer d'espace pour ne plus les distinguer

D'après Bourbaki, c'est chez Jordan que la notion de groupe quotient apparaît pour la première fois . L'expression « quotient des groupes G et H » a été introduite en 1889 par Otto Hölder, qui proposait la notation $G|H$.

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 de G, on peut définir une loi de groupe sur l'ensemble G/H des classes de G suivant H, à condition que H soit stable par les automorphismes intérieurs de G, c'est-à-dire que les classes latérales droites soient égales aux classes latérales gauches ($gH = Hg$). Un tel sous-groupe est appelé sous-groupe normal ou **sous- groupe distingué**. L'anneau quotient est un anneau qu'on construit sur l'ensemble quotient d'un anneau par un de ses idéaux bilatères.

Les utilisations de l'anneau Z/nZ en théorie des nombres illustrent l'efficacité de l'introduction d'anneaux quotients. Ainsi l'équation diophantienne $ax + by = 1$, qui peut être traitée par des méthodes d'arithmétique tout à fait élémentaire, peut aussi être interprétée comme recherche de l'inverse de a dans l'anneau quotient Z/bZ. Pour ce point de vue, il existe des solutions si et seulement si la classe de a est un élément inversible de l'anneau quotient, c.-à-d. si et seulement si a premier avec b. Les valeurs possibles de x sont alors les entiers qui se projettent dans Z/bZ sur cet inverse de la classe de a.

Le cas des quotients Z/pZ où p est premier est particulièrement fécond. L'anneau Z/pZ est alors un corps commutatif et on bénéficie de la richesse de cette structure. Le petit théorème de Fermat ou le théorème de Wilson sont deux exemples en arithmétique élémentaire qui peuvent bénéficier d'un tel traitement.

Dans le prolongement de cette idée, en algèbre commutative, l'anneau quotient par un idéal maximal est systématiquement un corps commutatif, appelé corps résiduel. Son utilisation peut renvoyer des informations sur l'anneau qu'on a quotienté ; elle peut aussi être une fin en soi, comme fournissant une méthode efficace de construction de nouveaux corps commutatifs.

Tout anneau commutatif A est le quotient de l'anneau de polynômes par l'idéal engendré par tous les éléments de la forme ou Cette remarque permet, pour démontrer n'importe quel énoncé universel d'algèbre commutative, de se contenter de le prouver pour les anneaux de polynômes à coefficients entiers.

Les anneaux quotients par des idéaux non nécessairement maximaux sont omniprésents en géométrie algébrique. l'espace vectoriel quotient E/F d'un espace vectoriel E par un sous-espace vectoriel F est la structure naturelle d'espace vectoriel sur l'ensemble quotient de E par la relation d'équivalence.

le théorème de factorisation est un principe général qui permet de construire un morphisme d'une structure quotient X/R dans un autre espace y à partir d'un morphisme de X vers Y, de façon à factoriser ce dernier par la surjection canonique de passage au quotient.

Le but de notre mémoire et de donner les notions des espaces quotients de différent structures algébriques, donner la méthode de constructions illustrées de quelques exemple, et de donner les théorèmes de factorisation pour chaque structure.

Notre mémoire est organisée de la manière suivante

Le premier chapitre contient les préliminaires et les notions de base sur les structures algébriques. Le deuxième chapitre est consacré aux théorèmes de construction des espaces quotients dont on donne les méthodes de construction et quelques exemples. Le troisième chapitre contient les théorèmes de factorisation des morphismes pour les structures étudier.

Chapitre 1

Notions de base

1.1 Relation d'équivalence

Définition 1.1.
Une relation d'équivalence est une relation binaire très particulière vérifiant les trois propriétés suivantes :
1. Réflexivité : tout élément est en relation avec lui même :

$$\forall x \in E \qquad x \Re x.$$

2. Symétrie : si un élément est en relation avec un autre, alors la réciproque est vrai :

$$\forall (x, y) \in E^2 \qquad (x \Re y \Rightarrow y \Re x).$$

3. Transitivité : si un élément est en relation avec un autre et que ce dernier est lui-même en relation avec un troisième, alors le premier est en relation avec le dernier :

$$\forall (x, y, z) \in E^3 \qquad (x \Re y \quad et \quad y \Re z) \Rightarrow x \Re z.$$

1.2 Classe d'équivalence

Définition 1.2.
Soit $\Re$ une relation équivalence sur un ensemble E. La classe d'équivalence d'un élément x, noté $Cl(x)$, est l'ensemble des éléments de E qui sont en relation avec x. Autrement dit

$$Cl(x) = \{y \in E : x \Re y\}.$$

Exemple 1.1.
Soit $\Re$ une relation d'équivalence :

$$x \Re y \Leftrightarrow \exists k \in \mathbb{Z} / x - y = kn$$

Proposition 1.1.
- Une classe d'équivalence n'est jamais vide.
- L'intersection de deux classes d'équivalence distinctes est vide

1.3 La congruence

Définition 1.3.
On dit que deux entiers relatifs a et b sont congru modulo n tel que $(n \in \mathbb{N}^*)$ et l'on écrit $a \equiv b\,[n]$ si et seulement si a et b ont le même reste dans la division par n.

Exemple 1.2.
$18 \equiv 23\,[5]$ *car 18 et 23 ont tous les deux 3 comme reste dans la division par 5.*

Propriétés.
• *$a \equiv b\,[n]$ si et seulement si n divise $a - b$ en particulier $a \equiv 0\,[n]$ si et seulement si n divise a.*
• *Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$ alors $a \equiv c\,[n]$.*
Soient quatre entiers relatifs a, b, c, d tels que $a \equiv b\,[n]$ et $c \equiv d\,[n]$ Alors :
• $a + c \equiv b + d\,[n]$ *et* $a - c \equiv b - d\,[n]$
• $ac \equiv bd\,[n]$
• $ka \equiv kb\,[n]$ *pour tout entier relatif* k
• $a^m \equiv b^m\,[n]$ *pour tout entier naturel* m

1.4 Les groupes

Définition 1.4.
On appelle groupe tout ensemble non-vide G muni d'une loi de composition interne $*$, vérifiant les trois propriétés suivantes (appelées axiomes de la structure de groupe) :
1. la loi $*$ est associative dans G , rappelons que cela signifie que :

$$x * (y * z) = (x * y) * z \ \forall\ x, y, z \in G$$

2. la loi $*$ admet un élément neutre dans G rappelons que cela signifie qu'il existe $e \in G$ tel que :

$$x * e = e * x = x \text{ pour tout } x \in G$$

3. tout élément de G admet un symétrique dans G pour la loi $*$
rappelons que cela signifie que, $\forall\ x \in G$, il existe $x' \in G$ tel que :

$$x * x' = x' * x = e$$

Remarque 1.1.
On appelle groupe commutatif, ou groupe abélien, tout groupe G dont la loi $*$ vérifie de plus la condition supplémentaire de commutativité :

$$x * y = y * x \ \forall\ x, y \in G$$

Exemple 1.3.
1. L'ensemble $\mathbb{C}$ des nombres complexes muni de l'addition est un groupe abélien. Le neutre est le nombre complexe nul 0, car :

$$z + 0 = 0 + z = z \qquad \forall\ z \in \mathbb{C}.$$

le symétrique de z pour l'addition est son opposé $-z$, car

$$z + (-z) = (-z) + z = 0$$

2. L'ensemble $\mathbb{C}$ des nombres complexes non-nuls muni de la multiplication est un groupe abélien. Le neutre est le nombre complexe 1, car $z.1 = 1.z = z$ pour tout $z \in \mathbb{C}^*$. $\forall\ z \in \mathbb{C}^*$, le symétrique de z pour la multiplication est son inverse z^{-1}, car $z.z^{-1} = z^{-1}.z = 1$.

Définition 1.5. *(Sous-groupe)*
Soit G un groupe muni d'une loi de composition interne. Et soit H un sous ensemble non-vide de G. On dit que H est un sous-groupe de G lorsque les deux conditions suivantes sont vérifiées :
1. H est stable pour la loi $\cdot$ (ce qui signifie $x \cdot y \in H \ \forall \ x, y \in H$).
2. H est stable par passage à l'inverse (ce qui signifie $x^{-1} \in H \ \forall \ x \in H$).
Dans ce cas, la restriction à H de la loi $\cdot$ de G définit une loi de composition interne dans H, pour laquelle H est lui-même un groupe.

Exemple 1.4.
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sont des sous-groupes du groupe $\mathbb{C}$ muni de l'addition , mais pas $\mathbb{N}$ (car l'opposé d'un l'élément de $\mathbb{N}$ n'est pas nécessairement un élément de $\mathbb{N}$).

Définition 1.6. *(Morphisme de groupe)*
Soit $(G, *)$ et $(H, \diamond)$ deux groupes .
Une application f de G dans H est un morphisme de groupes si :

$$\forall \ x,x^{'} \in G, \ f(x * x^{'}) = f(x) \diamond f(x^{'})$$

Remarque 1.2.
Si $G = H$, on dit que f est un endomorphisme de G.
On appelle automorphisme de G tout morphisme de groupes de G dans G qui est une bijection de G sur G.
On appelle isomorphisme de groupe de G sur G' tout morphisme de groupes $f : G \mapsto G'$ qui est de plus une bijection de G sur G'.

Définition 1.7. *(Produit direct de groupes)*
Si G et H sont deux groupes, on munit le produit cartésien $G \times H$ de la loi de composition :

$$(g_1, h_1) \times (g_2, h_2) = (g_1 \times g_2, h_1 \times h_2)$$

$(G \times H, \times)$ est alors un groupe, appelé le produit direct de G et H.

1.4.1 Quelques propriétés sur les groupes additif et les groupes multiplicatif

On se donne un groupe multiplicatif $(G, \cdot)$. L' Associativité du produit permet de définir les puissances entières, positives ou négatives, de $x \in G$ par :

$$\begin{cases} x^0 = 1 \\ \forall n \in \mathbb{N}, x^{n+1} = x^n x \\ \forall n \in \mathbb{N}^*, x^{-n} = (x^n)^{-1} \end{cases}$$

Remarque 1.3.
On peut remarque que pour $n \in \mathbb{N}^*$, on a aussi $x^{-n} = (x^{-1})^n$, ce qui résulte de :

$$(x^{-1})^n x^n = x^{-1}...x^{-1}x...x = 1$$

Dans le cas où $(G, +)$ est un groupe additif , x^n est noté nx pour $n \in \mathbb{Z}$

Théorème 1.1.
Pour x dans G et n, m dans $\mathbb{Z}$ on a :

$$x^n x^m = x^{n+m}$$

et pour $h \in G$ qui commute avec x, on a :

$$(xh)^n = x^n h^n = h^n x^n$$

Démonstration 1.1.
On montre tout d'abord le résultat pour n, m dans $\mathbb{N}$ par récurrences sur $m \geq 0$ à n fixé. Le résultat est évident pour $m = 0$ et le supposant acquis pour $m \geq 0$, on a :

$$x^n x^{m+1} = x^n x^m x = x^{n+m} x = x^{n+m+1}.$$

On en déduit que pour n', m' dans $\mathbb{N}$, on a :

$$x^{-n'} x^{-m'} = (x^{n'})^{-1}(x^{m'})^{-1} = (x^{m'} x^{n'})^{-1} = (x^{m'+n'})^{-1} = (x^{n'+m'})^{-1} = x^{-n'-m'}.$$

c'est-à-dire que le résultat est valable pour $n \leq 0$ et $m \leq 0$. Pour $n, m' \in \mathbb{N}$ tels que $n \geq m'$ on a :

$$x^{n-m'} x^{m'} = x^n \Rightarrow x^n (x^{m'})^{-1} = x^n x^{-m'} = x^{n-m'}.$$

et pour $n \leq m'$, on a :

$$x^{n-m'} = (x^{m'-n})^{-1} = (x^{m'} x^{-n})^{-1} = x^n x^{-m'}$$

donc le résultat est valable pour $n \geq 0$ et $m \leq 0$.
On voit de manière analogue qu'il est valable pour $n \leq 0$ et $m \geq 0$.
En définitive c'est valable pour tout n, m dans $\mathbb{Z}$.
En supposant que x et h commutent, on montre par récurrence sur $n \geq 0$ que :

$$(xh)^n = x^n h^n$$

et

$$xh^{n+1} = h^{n+1} x.$$

C'est clair pour $n = 0$ et supposant le résultat acquis pour $n \geq 0$, on a :

$$\begin{aligned} (xh)^{n+1} &= (xh)^n xh = x^n h^n xh = x^n h^n hx. \\ &= x^n h^{n+1} x = x^n x h^{n+1} = x^{n+1} h^{n+1} \end{aligned}$$

Et avec $xh = hx$, on déduit que

$$(xh)^n = (hx)^n = h^n x^n.$$

En suite, pour $n' \geq 0$, on a :

$$(xh)^{-n'} = ((xh)^{n'})^{-1} = (x^{n'} h^{n'})^{-1} = (h^{-n'} x^{n'})^{-1} = x^{-n'} h^{-n'} = h^{-n'} x^{-n'}.$$

et le résultat est valable pour $n \leq 0$.

Remarque 1.4.
La relation $(xh)^n = x^n h^n$ est fausse si x et h ne commutent pas, des exemples simples étant donnés dans $GL_n(\mathbb{R})$ avec $n \geq 2$, ou dans le groupe symétrique $\mathcal{S}_n$ avec $n \geq 3$

Exemple 1.5.

$$pour A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

et

$$pour B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

dans $GL_n(\mathbb{R})$, on a

$$(AB)^2 = \begin{pmatrix} 10 & 24 \\ 24 & 58 \end{pmatrix}$$

et

$$A^2B^2 = \begin{pmatrix} 7 & 24 \\ 15 & 52 \end{pmatrix}$$

Définition 1.8.
Le centre (ou commutateur)$Z(G)$ d'un groupe G est la partie de G formée des éléments de G qui commutent à tous les autres éléments de G, soit :

$$Z(G) = \{h \in G \setminus \forall x \in G, xh = hx\}$$

Un groupe G est commutatif si et seulement si $Z(G) = G$.
Pour tout $x \in G$, l'application $\Phi_x :\mapsto xhx^{-1}$ est un automorphisme de G (on dit que Φ_x est un automorphisme intérieur de G) et l'application $\Phi : x \mapsto \Phi_x$ est un morphisme de groupes de G dans $Aut(G)$.
Le noyau de Φ est formé des $x \in G$ tels que $\Phi_x = Id_G$, c'est-à-dire des $x \in G$ tels que $xhx^{-1} = h$ pour tout $h \in G$, ce qui équivaut à $xh = hx$ pour tout $h \in G$.
Le noyau est donc le centre de G et ce centre est un sous-groupe de G. De plus ce sous-groupe est commutatif.

Remarque 1.5.
Si on prend pour définition d'automorphismes intérieurs les applications

$$\Psi_x : h \mapsto x^{-1}hx$$

on a

$$\Psi_{xx'} = \Psi_{x'} \circ \Psi_x \neq \Psi_x \circ \Psi_{x'}$$

en général et l'application $\Psi : x \mapsto \Psi_x$ n'est pas un morphisme de groupes

Exemple 1.6.
Pour le groupe multiplicatif $G = GL_2(\mathbb{R})$,soient $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$
On a $A^{-1} = A, B^{-1} = \begin{pmatrix} 0 & \frac{1}{2} \\ 1 & 0 \end{pmatrix}$
et pour toute matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$, on a :

$$\Psi_A(M) = A^{-1}MA = AMA = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$$

$$\Psi_B(M) = B^{-1}MB = \begin{pmatrix} d & \frac{c}{2} \\ 2b & a \end{pmatrix}$$

Ce qui donne :

$$\Psi_A \circ \Psi_B(M) = \begin{pmatrix} a & 2b \\ \frac{c}{2} & d \end{pmatrix} \neq \Psi_B \circ \Psi_A(M) = \begin{pmatrix} a & \frac{b}{2} \\ 2c & d \end{pmatrix}$$

en général.

Définition 1.9. *(sous groupe distingué)*
Soient G un groupe et H un sous-groupe de G. On dit que H est normal dans G, ou encore distingué dans G, lorsque $xHx^{-1} = H$ pour tout $x \in G$. On note alors $H \triangleleft G$.
$(H \triangleleft G) \Leftrightarrow (xHx^{-1} = H \text{ pour tout } x \in G) \Leftrightarrow (xhx^{-1} \in H \quad \forall h \in H, x \in G)$

On peut encore définir les sous groupes distingués de la manière suivante :

Définition 1.10. *(sous-groupe distingué)*
Soit G un groupe et H un sous-groupe de G.
• *On dit que H est **distingué** (ou **normal**) dans G, et note $H \triangleleft G$, s'il est stable par tout automorphisme intérieur de G, i.e.*

$$\forall x \in G, \quad xHx^{-1} \subset H.$$

• *On dit que H est caractéristique dans G s'il est stable par tout automorphisme de G.*

Exemple 1.7.
• *Tout groupe caractéristique est distingué dans G.*
• *e et G sont caractéristiques.*
• *Si G est abélien, tout sous-groupe de G est distingué .*
• *L'image par un morphisme surjectif et l'image réciproque par un morphisme quelconque d'un sous-groupe distingué sont distingués.*
• *Soit G un groupe, $H \triangleleft G$ cyclique et K un sous-groupe de H. Alors $K \triangleleft G$.*
• *Int $G \triangleleft$ Aut G.*
• *$\{1\}$ et G sont toujours distingués dans G*

Théorème 1.2.
Pour tout sous-groupe H de G, la relation $\mathcal{R}_x$(ou de manière plus précise $(\mathcal{R}_H)_x$) définie sur G par :

$$x_1 \mathcal{R}_x x_2 \Leftrightarrow x_1^{-1}x_2 \in H$$

est une relation d'équivalence.

Démonstration 1.2.
Pour tout $x \in G$, on a $x^{-1}x = 1 \in H$, donc $\mathcal{R}_x$ est réflexive.
Si x_1, x_2 dans G sont tels que $x_1^{-1}x_2 \in H$, on a alors :

$$(x_1^{-1}x_2)^{-1} = x_2^{-1}x_1 \in H$$

ce qui signifie que $x_2 \mathcal{R}_x x_1$ Cette relation est donc symétrique.
Si x_1, x_2, x_3 dans G sont tels que :

$$x_1^{-1}x_2 \in H, x_2^{-1}x_3 \in H$$

on a alors :

$$x_1^{-1}x_3 = (x_1^{-1}x_2)(x_2^{-1}x_3) \in H$$

ce qui signifie que : $x_1\mathcal{R}_x x_3$ Cette relation est donc transitive.

Notation.
Pour tout $x \in G$, $\overline{x}$ la classe d'équivalence de x modulo $\mathcal{R}_x$ et on dit que $\overline{x}$ est la classe à gauche modulo H de x
On a donc, pour tout $x \in G$:

$$h \in \overline{x} \Leftrightarrow x\mathcal{R}_x h \Leftrightarrow x^{-1}h \in H \Leftrightarrow \exists k \in H \ h = xk \Leftrightarrow h \in xH.$$

c'est-à-dire que $\overline{x} = xH$
En particulier, $\overline{1} = H$ et $\overline{x} = H$ si, et seulement si, $x \in H$
L'ensemble de toutes ces classes d'équivalence est noté G/H et on l'appelle l'ensemble des classes à gauche modulo H
On a donc :

$$G/H = \{\overline{x} : x \in G\} = \{xH : x \in G\}.$$

Remarque 1.6.
On peut définir, de manière analogue l'ensemble :

$$H\backslash G = \{Hx : x \in G\}.$$

des classes à droites modulo H à partir de la relation d'équivalence :

$$x_1\mathcal{R}_d x_2 \Leftrightarrow x_1x_2^{-1} \in H$$

La relation d'équivalence $\mathcal{R}_x$ nous fourni une partition de G

Proposition 1.2.
l'intersection de deux sous-groupes distingués de G est un sous groupe distingué.

Démonstration 1.3.
Si H, K sont distingués dans G
pour tous $x \in G$ et $h \in H \cap k$ on a $xhx^{-1} \in H \cap K$.

Proposition 1.3.
Soit G un groupe et H un sous-groupe de G. Lpsse :
(i) H est distingué dans G
(ii) H est un point fixe de l'action par conjugaison sur les sous-groupes i.e.

$$\forall x \in G : xHx^{-1} = H.$$

(iii) H est le noyau d'un morphisme de groupes

Proposition 1.4.
Soit $f : G \to H$ un morphisme et $N \triangleleft H$, alors $f^{-1}(N) \triangleleft G$.

Remarque 1.7.
Un p-groupe (p-groupe sont des groupe d'un ordre p tell que p est un nombre premier) a des sous-groupes distingués de tous les ordres possibles.

Définition 1.11. *(Le cardinale et l'indice d'un groupe)*
Si H est un sous-groupe de G, le cardinal de l'ensemble G/H est noté $[G : H]$ et on l'appelle l'indice de H dans G

Définition 1.12.
On définit l'indice de H dans G, et on note $(G : H)$ comme le cardinal de G/H, i.e

$$(G : H) = |G/H|$$

Proposition 1.5.
Soient $(G, \cdot)$ un groupe fini d'ordre $n \geq 2$ et H un sous-groupe de G d'indice 2.Alors H distingué.

Démonstration 1.4.
Si H est d'indice 2, on a alors $G/H = H, x_1H$ avec $x_1 \notin H$ et la partition $G = H \cup x_1H$ Il s'agit alors de montrer que pour tous $x \in G$ et $h \in H$; on a forcément $xhx^{-1} \in H$. Si $x \in H$ c'est clair, sinon $x = x_1k$ avec $k \in H$ et $xhx^{-1} = x_1khk^{-1}x_1^{-1} = x_1x_1^{-1}$ avec $l \in H$ et $x_1lx_1^{-1} \in x_1H$ donne $x_1lx_1^{-1} = x_1k$ avec $m \in H$ et ce qui entraîne $x_1 = lm^{-1} \in H$ qui est faux, on a donc $xhx^{-1} = x_1lx_1^{-1} \in H$ et H est distingué dans G

Proposition 1.6.
Pour tout sous-groupe H de G on a :

$$card(G/H) = card(G \setminus H)$$

Démonstration 1.5.
En remarquant que l'application $x \mapsto x^{-1}$ réalise un isomorphisme de G, on en déduit que l'application :

$$\begin{cases} \varphi : G/H \longrightarrow G \setminus H \\ \quad xH \longrightarrow Hx^{-1} \end{cases}$$

est bijective. On vérifie d'abord qu'elle est bien définie : si $xH = x'H$; on a alors $(xH)^{-1} = Hx^{-1} = (x'H)^{-1} = H(x')^{-1}$. Puis qu'elle est injective : $Hx^{-1} = H(x)^{-1}$ entraîne $(Hx^{-1})^{-1} = xH = (H(x')^{-1})^{-1} = x'H$. Comme est surjective, c'est une bijection.L'application :

$$\pi : \begin{cases} G \longrightarrow G/H \\ x \longmapsto \overline{x} = xH \end{cases}$$

est surjective. On dit que c'est la surjection canonique de G sur G/H. Dans le cas des groupes finis, la partition en classes à gauche modulo H nous donne le résultat de démonstration élémentaire suivant qui a de nombreuses applications.

Corollaire 1.
Soient G, G' deux groupes et $\varphi : G \longrightarrow G'$ un morphisme de groupes. Si G est fini, on a alors :

$$card(G) = card(ker(\varphi))card(Im(\varphi))$$

Démonstration 1.6.
Comme $G/ker(\varphi)$ et $Im(\varphi)$ sont isomorphes, dans le cas où G est fini on a :

$$card(Im(\varphi)) = card(G/ker(\varphi)) = \frac{card(G)}{card(ker(\varphi))}$$

Définition 1.13.
Si G est un groupe fini, son cardinal est noté $(G : 1)$ et s'appelle l'ordre du groupe.

1.5 Anneaux

Définition 1.14. *(Anneau)*
Un anneau est un ensemble non vide muni de deux lois de composition internes, l'une note comme une addition et l'autre comme une multiplication, vérifiant les propriétés :
1. A est un groupe abélien pour l'addition, (on note 0 son élément neutre),
2. la multiplication est associative, c'est-à-dire :

$$x(yz) = (xy)z \quad \forall\ x, y, z \in A\ .$$

3. la multiplication est distributive sur l'addition à gauche et à droite c'est-à-dire :

$$x(y+z) = xy + xz \text{ et } (x+y)z = xz + yz \quad \forall\ x,\ y,\ z \in A.$$

Remarque 1.8.
On dit que l'anneau A est commutatif si de plus la multiplication est commutative, c'est-à-dire :

$$xy = yx \quad \forall\ x,\ y \in A.$$

On dit que A est unitaire si de plus la multiplication admet un élément neutre 1.

$$x \cdot 1 = 1 \cdot x = x \quad \forall\ x \in A.$$

Exemple 1.8.
(1)- L'ensemble $\mathbb{Z}$ des entiers est un anneau commutatif unitaire. Il en est de même de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
(2)- L'anneau nul est l'anneau 0 formé d'un unique élément.
(3)- Pour tout intervalle I de R, l'ensemble $F(I;R)$ des applications de I dans R est un anneau commutatif (la multiplication étant le produit des fonctions défini par $(fg)(x) = f(x)g(x)$ pour tout $x \in R$) unitaire (de neutre multiplicatif la fonction constante égale à 1). Il en est de même pour l'ensemble $\mathbb{R}^{\mathbb{N}}$ des suites de réels.

Définition 1.15. *(Sous-anneau)*
Soit A un anneau. On appelle sous-anneau de A toute partie non-vide B de A qui vérifie les deux conditions suivantes :
1. B est un sous-groupe du groupe additif A.
2. B est stable par la multiplication de A, c'est-à-dire que l'on a :

$$xy \in B \quad \forall\ x \in B \text{ et } y \in B$$

Exemple 1.9. *(Des entiers de Gauss)*
On appelle entier de Gauss tout nombre complexe dont la partie réelle et la partie imaginaire sont des entiers. On note $\mathbb{Z}[i]$ leur ensemble :

$$\mathbb{Z}[i] = \{a + ib; a, b \in \mathbb{Z}\}.$$

$\mathbb{Z}[i]$ est un anneau commutatif unitaire, contenant Z comme sous-anneau.
En effet, quels que soient $x = a + ib$ et $x' = c + id$ avec $a, b, c, d \in Z$, les complexes $x - x' = (a - c) + i(b - d)$ et $xx' = (ac - bd) + i(ad + bc)$ ont des parties réelles et imaginaires dans $\mathbb{Z}$, donc appartiennent à $\mathbb{Z}[i]$.
Ceci prouve que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ (donc en particulier un anneau commutatif). Il est clair que $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}$, d'où il résulte en particulier que $1 \in \mathbb{Z}[i]$.

Proposition 1.7.
(1) Si B est un sous-anneau de A, alors B est lui-même un anneau (pour les lois déduites de celles de A par restriction à B). De fait, dans la pratique, pour montrer qu'un ensemble donné

est un anneau, on cherche souvent à montrer que c'est un sous-anneau d'un anneau déjà connu.
(2) Si B est un sous-anneau unitaire d'un anneau unitaire A, alors B est lui-même un anneau unitaire, et l'on a $1_B = 1_A$.
(3) Si l'anneau A est commutatif, alors tout sous-anneau de A est commutatif.
(4) Dans la pratique, pour montrer qu'un sous-ensemble non-vide B d'un anneau A est un sous anneau de A, il suffit de vérifier que : pour tous $x \in B$ et $y \in B$, on a $x - y \in B$ et $xy \in B$.
Pour montrer qu'un sous-ensemble B d'un anneau unitaire A est un sous-anneau unitaire de A, il suffit de vérifier que :
$(1_A \in B)$ et (pour tous $x \in B$ et $y \in B$, on a $x - y \in B$ et $xy \in B$).

Définition 1.16. *(Morphisme d'anneaux)*
Soient A et B deux anneaux commutatifs unitaires.
On appelle morphisme d'anneaux unitaires de A dans B toute application $f : A \to B$ vérifiant les trois propriétés suivantes :
pour tous x,$y \in A$

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(xy) &= f(x)f(y) \\ f(1A) &= (1B) \end{aligned}$$

Proposition 1.8.
(1) Si $f : A \to B$ est un morphisme d'anneaux unitaires, alors l'image directe par f de tout sous-anneau unitaire de A est un sous-anneau unitaire de B, et l'image réciproque par f de tout sous-anneau unitaire de B est un sous-anneau unitaire de A.
(2) Si $f : A \to B$ et $g : B \to C$ sont des morphismes d'anneaux unitaires, alors $g \circ f : A \to C$ est un morphisme d'anneaux unitaires.
(3) Si $f : A \to B$ est un morphisme d'anneaux unitaires bijectif, alors sa bijection réciproque f^{-1} :$B \to A$ est un morphisme d'anneaux unitaires ;
on dit dans ce cas que f est un isomorphisme , et que les deux anneaux A et B sont isomorphes.

1.6 Intégrité

Définition 1.17. *(Intégrité)*
Un anneau A est dit intègre s'il ne contient pas de diviseur de 0.
(c'est-à-dire si pour tout couple (a, b), on a :

$$a * b = 0 \Rightarrow (a = 0 \ ou \ b = 0)$$

Démonstration 1.7.
Un élément x de A est appelé un diviseur de zéro dans A lorsque $x \neq 0$ et lorsque qu'il existe $y \neq 0$
dans A tel que $xy = 0$. En d'autres termes, A est intègre si et seulement s'il n'admet pas de diviseurs de zéro.

1.7 Idéaux

Définition 1.18. *(Idéal)*
Soit A un anneau commutatif unitaire. On appelle idéal de A toute partie non-vide I de A qui

vérifié les deux conditions suivantes :
1. I est un sous-groupe du groupe additif A,
2. pour tous $x \in I$ et $a \in A$, on a $xa \in I$.

Exemple 1.10.
$\{0\}$ *et A sont des idéaux de A.*

Proposition 1.9. *(stabilité par intersection et somme)*
• *Si $(I_\lambda)_{\lambda \in J}$ est une famille (non vide) d'idéaux de A, alors $\bigcap_{\lambda \in J} I_\lambda$ est encore un idéal de A.*
• *Si I_1 et I_2 sont deux idéaux de A, alors $I_1 + I_2$ est encore un idéal, ou :*

$$I_1 + I_2 = \{x \in A, \quad x = x_1 + x_2 \, avec \, x_1 \in I_1 \, et \, x_2 \in I_2\}$$

Démonstration 1.8. *Immédiate en revenant à la deuxième définition d'un idéal*
Soit A un anneau commutatif unitaire et I une partie de A.
Alors I est un idéal de A si et seulement si :

$$\begin{cases} I \neq \emptyset \\ I \text{ est stable pour la loi } + \\ \forall x \in I, \forall a \in A, a \times x \in I \end{cases}$$

Notons juste que l'ensemble $\bigcap_{\lambda \in J} I_\lambda$ est non vide car pour tout λ on a $0 \in I_\lambda$.

Définition 1.19. *Soit I un idéal de A. On dit que I est un idéal propre de A si $I \neq A$.*

Définition 1.20. *Soit A un anneau et soit I un idéal de A. On dit que I est un idéal premier si*
- l'idéal I est propre ;
- si $a, b \in A$ sont tels que $ab \in I$, alors $a \in I$ ou $b \in I$.
Cette notion généralise celle de nombre premier. En effet, si un produit d'entiers ab est multiple d'un nombre premier p, alors a ou b est multiple de p. La condition que I est propre, donc que $I \neq A$, est analogue à la convention qui dit que 1 n'est pas un nombre premier. Parfois on utilise la seconde assertion sous sa forme contra-posée : si a et b sont deux éléments de A n'appartenant pas à I, alors leur produit ab n'appartient pas à I.

Exemple 1.11. *:*
L'idéal (0) d'un anneau est premier si et seulement si A est intègre.

Exemple 1.12. *:*
Dans l'anneau Z, un idéal (n) est premier si et seulement si n est premier.

1.8 Espace vectoriel

Définition 1.21. *(Espace vectoriel)*
On appelle espace vectoriel sur K (ou K-espace vectoriel) un ensemble E muni de deux lois : une loi interne, notée $+$, telle que $(E, +)$ soit un groupe commutatif. L'élément nul est noté 0_E. une loi externe, notée $\cdot$ qui est une application de $K \times E$ dans E vérifiant :
• $\forall (\alpha, \beta) \in K^2, \forall x \in E, \ (\alpha + \beta).x = \alpha.x + \beta.x$
• $\forall \alpha \in K, \ \forall (x, y) \in E^2, \ \alpha.(x + y) = \alpha.x + \alpha.y$
• $(\alpha, \beta) \in K^2, \forall x \in E, \ \alpha.(\beta.x) = (\alpha\beta).x$
• $\forall x \in E, \ 1.x = x$

Exemple 1.13. *(Le R-espace vectoriel $\mathbb{R}_n$)*
Soit n un entier supérieur ou égal à 1. Posons $\mathbb{K} = \mathbb{R}$ et $E = \mathbb{R}_n$. Un élément $u \in E$ tell que $u(x_1, x_2, ..., x_n)$ avec $x_1, x_2, ..., x_n$ des éléments de $\mathbb{R}$.
• *Définition de la loi interne. Si $(x_1, x_2, ..., x_n)$ et $(x_1^{'}, x_2^{'}, ..., x_n^{'})$ sont deux éléments de $\mathbb{R}_n$, alors :*

$$(x_1, x_2, ..., x_n) + (x_1^{'}, x_2^{'}, ..., x_n^{'}) = (x_1 + x_2^{'}, ..., x_n + x_0^{'}).$$

• *Définition de la loi externe. Si λ est un réel et $(x_1, x_2, ..., x_n$ est un élément de $\mathbb{R}_n$, alors :*

$$\lambda \cdot (x_1, x_2, ..., x_n) = (\lambda x_1, \lambda x_2, ..., \lambda x_n).$$

L'élément neutre de la loi interne est le vecteur nul (0, 0, . . . , 0). Le symétrique de $(x_1, x_2, ..., x_n)$ est $(-x_1, -x_2, ..., -x_n)$, que l'on note $-(x_1, x_2, ..., x_n)$.
De manière analogue, on peut définir le $\mathbb{C}-$ espace vectoriel $\mathbb{C}^n$, et plus généralement le $\mathbb{K}-$ espace vectoriel $\mathbb{K}^n$.

Définition 1.22. *(Sous-espace vectoriel)*
Soit E un K-espace vectoriel. Une partie F de E est appelée un sous-espace vectoriel si :
• $0_E \in F$,
• $u + v \in F$ *pour tous* $u, v \in F$,
• $\lambda.u \in F$ *pour tout* $\lambda \in K$ *et tout* $u \in F$.

Définition 1.23. *(Application linéaire)*
Soient E et F deux K-espaces vectoriels. Une application $f : E \Rightarrow F$ est une application linéaire si elle satisfait aux deux conditions suivantes :
1. $f(u + v) = f(u) + f(v), \quad \forall u, v \in E$.
2. $f(\lambda \cdot u) = \lambda \cdot f(u), \quad \forall u \in E$ *et* $\lambda \in K$.

Exemple 1.14.
L'application f définie par
$f : \mathbb{R}^3 \to \mathbb{R}^2 \qquad (x, y, z) \to (-2x, y + 3z)$ *est une application linéaire. En effet, soient $u = (x, y, z)$ et $v = (x^{'}, y^{'}, z^{'})$ deux éléments de $\mathbb{R}^3$ et λ un réel.*

$$\begin{aligned} f(u+v) &= f(x + x^{'}, y + y^{'}, z + z^{'}) \\ &= (-2(x + x^{'}), (y + y^{'}) + 3(z + z^{'})) \\ &= (-2x, y + 3z) + (-2x^{'}, y^{'} + 3z^{'}) \\ &= f(u) + f(v) \end{aligned}$$

et

$$\begin{aligned} f(\lambda u) &= f(\lambda x, \lambda y, \lambda z) \\ &= (-2\lambda x, \lambda y + 3\lambda z) \\ &= \lambda(-2x, y + 3z) \\ &= \lambda f(u) \end{aligned}$$

Définition 1.24. *(Image et noyau)*
Soit f un morphisme de groupes de G sur H.

- *On appelle, image de f , l'ensemble noté Imf , défini par :*

$$Imf = f(G) = f(x), x \in G$$

- *On appelle noyau de F, l'ensemble noté $Kerf$, défini par :*

$$Kerf = f^{-1}(\{e_H\}) = \{x \in G, f(x) = e_H\}$$

Exemple 1.15.
Le morphisme $exp : \mathbb{R} \to \mathbb{R}_+^*$ est surjectif; son noyau est $Ker(exp) = x \in R; exp(x) = 1 = 0$, ce qui prouve qu'il est aussi injectif.

Chapitre 2

Structures quotients

Soit H est un sous-groupe d'un groupe G, on souhaiterait munir l'ensemble G/H d'une structure de groupe par " passage au quotient ". Cela n'est pas toujours possible, il faut que H possédé des propriétés particulières.

2.1 Quotient d'un groupe abélien par un sous-groupe

On considère dans cette partie un groupe abélien $(G,+)$ et H un sous-groupe de G.

Théorème 2.1.
La relation d'équivalence $\Re$ appelée relation de congruence modulo H définie par :

$$x \equiv y \Leftrightarrow y - x \in H.$$

Démonstration 2.1.
Vérifier que $\equiv$ est une relation d'équivalence est immédiat en effet :
- *H contient le neutre 0 (réflexivité),*
- *est stable par passage à l'opposé (symétrie),*
- *et par addition (transitivité).*

Notation.
On notera G/H l'ensemble $G/\Re$ des classes d'équivalences de la relation $\Re$ sur G.

Remarque 2.1.
On remarque que :

$$y \in \overline{x} \Leftrightarrow \overline{y} = \overline{x} \Leftrightarrow y - x \in H \Leftrightarrow y \in x + H.$$

où l'on note :

$$x + H := \{x + h; h \in H\}.$$

Ainsi, la classe d'un élément x de G peut d'écrire explicitement comme :

$$\overline{x} = x + H.$$

Définition 2.1.
Soient X et Y deux éléments de G/H, x un représentant de X et y un représentant de Y.
On peut essayer de définir une loi $+$ sur G/H qui découlerait de celle de G.
Par exemple :

$$X + Y := \overline{x + y}.$$

En cela que le membre de gauche $\overline{x+y}$ dépend a priori des représentants x et y choisis. Vérifions qu'il n'en est rien. Si $x^{'}$ est un autre représentant de X , on a

$$\overline{x} = X = \overline{x^{'}}.$$

Donc $x \equiv x^{'}$, et la différence $(x^{'} - x)$ est un élément h_x de H.
De même, si $y^{'}$ est un autre représentant de Y , on a $(y^{'} - y) = h_y$ élément de H.
On en déduit :

$$(x^{'} + y^{'}) - (x + y) = (x^{'} - x) + (y^{'} - y) = h_x + h_y \in H.$$

Car H stable par $+$, i.e. $x+y \equiv x^{'}+y^{'}$, ou encore $\overline{x^{'} + y^{'}} = \overline{x + y}$. On peut donc effectivement munir G/H d'une loi $+$ définie par

$$\overline{x} + \overline{y} = \overline{x + y}.$$

Remarque 2.2.
On utilise volontairement le même symbole $+$ pour désigner les lois de G et de G/H, car la seconde découle de la première au vu de la définition, mais il faut garder à l'esprit qu'elle n'agissent pas sur les mêmes objets − la première sur des éléments de G, la seconde sur des classes d'éléments de G.

Conclusion 2.1.
Il est alors immédiat que le magma $(G/_H, +)$ est un groupe :
observer que l'associativité dans (G/H) découle de l'associativité dans G, et que le neutre ainsi que l'inverse dans G/H sont donnés par :

$$0_{G/H} = \overline{0_G} \quad et - \overline{x} = \overline{-x}.$$

Le groupe $(G/_H, +)$ est alors appelé groupe quotient de G par H, ou plus simplement quotient de G par H

De façon plus générale

Définition 2.2.
Si $*$ est un loi quelconque sur un ensemble E non vide muni d'une relation d'équivalence $\Re$, on dit que la relation $\Re$ est compatible avec la loi $*$ si

$$\begin{cases} x \Re x^{'} \\ y \Re y^{'} \end{cases} entraine (x * y) \Re (x^{'} * y^{'}).$$

Définition 2.3.
On peut alors définir une loi quotient $*_\Re$ sur $E/\Re$ par

$$\overline{x} *_\Re \overline{y} = \overline{x * y}$$

et l'on voit que toutes les propriétés de la loi $*$ (associativité, commutativité...) sont transportées dans le quotient et sont vérifiées par $*_\Re$.

Remarque 2.3.
Lorsqu'une relation d'équivalence est compatible avec une loi, on parle plutôt de relation de congruence et on la note généralement $\equiv$.
On peut donc mener des calculs avec la loi considérer, la présence d'un troisième trait sur le signe $=$ *rappelant qu'on travaille dans le quotient.*

Réciproquement.
Si l'on se donne une relation d'équivalence $\Re$ *sur* G *compatible avec la loi* $+$*, cherchons un sous-groupe* H *tel que* $G/\Re = G/H$*,*
i.e. tel que $\Re$ *soit la relation de congruence modulo* H*.*
Par définition de celle-ci, un tel H *doit vérifier* $x\Re y$ *si et seulement si* $y - x \in H$*, donc la seule possibilité est*

$$H = \{y - x : x\Re y\}$$

Démonstration 2.2.
En effet H *est bien un sous-groupe de* G*, car :*
• *En prenant un* x *dans* G*, on a (par réflexivité de* $\Re$*)* $x\Re x$*, donc* $0 = x - x \in H$ *;*
• *Si* $h \in H$*, on a* $h = y - x$ *avec* $x\Re y$*, donc (par symétrie de la relation* $\Re$*)* $y\Re x$ *, d'où* $-h = x - y \in H$ *;*
• *Si* h_x *et* h_y *sont dans* H*, on a*

$$\begin{cases} h_x = x^{'} - x, \ x\Re x^{'} \\ h_y = y^{'} - y, \ ; y\Re y^{'} \end{cases} \text{ donc (par compatibilité de } \Re \text{ avec } + \text{) } (x+y)\Re(x^{'} + y^{'}),$$

i.e. $(x^{'} + y^{'}) - (x + y) \in H$*, on encore* $h_x + h_y \in H$*.*
De plus, on a bien $x\Re y$ *si et seulement si* $y - x \in H$ *comme on le souhaitait.*

Conclusion 2.2.
Un sous-groupe et une relation d'équivalence compatible avec la loi de groupe, c'est pareil.

2.2 Quotient d'un groupe par un sous-groupe

On considère cette fois un groupe multiplicatif $(G, \cdot)$ *non nécessairement abélien et* H *un sous-groupe de* G*.*
Par analogie avec le cas abélien, on définit une relation $\equiv$ *sur* G *par :*

$$x \equiv y \Leftrightarrow x^{-1}y \in H.$$

Théorème 2.2.
La relation $\Re$ *définie par* $x\Re y \Leftrightarrow x^{-1}y \in H$ *est une relation d'équivalence.*

Démonstration 2.3.
On vérifie immédiatement qu'il s'agit bien d'une relation d'équivalence.

Proposition 2.1.
Les équivalences suivent sont équivalent :
• $y \in \overline{x}$;
• $\overline{x} = \overline{y}$;
• $x^{-1}y \in H$:
• $y \in xH$.
Et assurent que la classe d'un élément x *de* G *est donnée par :*

$$\overline{x} = xH = \{xh : h \in H\}.$$

On peut dès à présent noter les :

$$\begin{cases} (xy)H = x(yH) \\ \forall h \in H; hH = H. \end{cases}$$

• *La première est triviale,*
• *En vérifiant les deux inclusions (et ne nécessite pas que H soit un sous-groupe de G, toute partie de G convient), la seconde résulte de ce que H est stable par la loi $\cdot$ (d'où $hH \subset H$) et par passage à l'inverse (tout h_0 de H peut s'écrire $h(h^{-1}h_0)$, d'où $H \subset hH$).*
On a également de façon immédiate que pour toutes parties A et B de G :

$$A \subset B \Longrightarrow \begin{cases} xA \subset xB \\ Ax \subset Bx \end{cases}$$

Notation.
On notera G/H l'ensemble $G/\Re$ des classes d'équivalences de la relation $\Re$ sur G.

Définition 2.4.
On peut également définir une relation $x \equiv y$ par $xy^{-1} \in H$, auquel cas les classes d'équivalence sont données par $\overline{x} = Hx$ et sont alors appelées classes à droite de H (Hx est également appelé translaté à droite de H par x), l'ensemble quotient se notant dans ce cas

$$H \backslash G := \{Hx; x \in G\}.$$

Proposition 2.2.
Soit $x \in G$. La classe d'équivalence de x pour la relation

$$x \Re y \Leftrightarrow x^{-1}y \in H$$

est l'ensemble $Hx = \{x \cdot h; y \in h\}$.

Démonstration 2.4.
Soit $y \in G$ équivalent à x pour la relation $\Re$. Alors il existe $h \in H$ tel que $x^{-1} \cdot y \in h$. Et donc y est élément de Hx.
Réciproquement, si y est élément de xH, il est clair que $y \Re x$. L'ensemble xH s'appelle classe à gauche de l'élément x de G.

Remarque 2.4.
Pour ne pas se mélanger les pinceaux, on pourra retenir que, dans les notations

$$\begin{cases} G/H = \{xH; x \in G\} \\ H \setminus G = \{Hx; x \in G\} \end{cases}$$

ce par quoi on translate (les éléments x de G) est du bon côté de H : pour les classes à gauche, le "x" de xH à est à gauche de H, et le "G" de G/H est aussi à gauche de H

Proposition 2.3.
Si H un sous groupe fini de G et si x et y sont deux éléments de G alors les classes d'équivalences (à gauche ou à droite) de x et y pour la relation $\Re$ ont même nombre d'éléments et ce nombre est égal au cardinal de H.

Démonstration 2.5.
Soit x un élément de G. Posons $f : H \to xH \to f(h) = x \cdot h$.
f est injective car si h et h' sont des éléments de H tels que $f(h) = f(h')$ alors on a l'égalité

$x \cdot h = x \cdot h'$ et x étant élément du groupe G, ceci implique, en multipliant à gauche chacun des membres de l'égalité précédente par x^{-1} que $h = h'$.
f est aussi surjective car si y est un élément de xH, alors il existe $h \in H$ tel que $y = x \cdot h$ et donc $y = f(h)$.
f étant à la fois injective et surjective, elle 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 $\Re$, 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 des propositions précédentes est fondamental en algèbre.

Remarque 2.5.
Dans le cas abélien, tout commute et il n'y a pas lieu de différencier classe à gauche de classe à droite.
En pratique, on utilise la plupart du temps les classes à gauche et le quotient G/H.

Définition 2.5.
Cherchons à présent à munir le quotient G/H d'une structure de groupe, toujours par analogie avec le cas abélien. cette serait la loi quotient définie par :

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}.$$

On a déjà vu que, pour que la définition ci-dessus en soit vraiment une, on effet que la classe $\overline{xy}$ ne dépende pas des représentants choisis, il faut que la relation $\equiv$ soit compatible avec la loi de G.
Soient g quelconque dans G, h quelconque dans H. On a :

$$\begin{cases} \overline{h} = hH = H = \overline{1} \\ \overline{gh} = (gh)H = g(hH) = gH = \overline{g} \end{cases}$$

donc, dans le cas où la relation $\equiv$ est compatible avec la loi $\cdot$
on doit avoir
$\begin{cases} 1 \equiv h \\ gh \equiv g \end{cases} \Rightarrow (1) \cdot (gh) \equiv (h) \cdot (g) \Rightarrow gh \equiv hg \Rightarrow (gh)^{-1}(hg) \in H \Rightarrow$

$$h^{-1}g^{-1}hg \in H \Rightarrow h(h^{-1}g^{-1}hg) \in hH \Rightarrow g^{-1}hg \in H.$$

Ceci tenant pour tout h dans H, on doit avoir

$$\forall g \in G, g^{-1}Hg \subset H.$$

Remarque 2.6.
Un tel sous-groupe stable par les applications $i_g : x \mapsto g^{-1}xg$ (appelées conjugaisons ou automorphismes intérieurs), est dit distingué dans G (ou tout simplement distingué), et on note alors $H \lhd G$. le symbole $\lhd$ qui fait penser à une relation d'ordre, en général la relation "être distingué dans" n'est pas transitive
Noter que dans le cas abélien, tous les sous-groupes de G sont distingués dans G.

Montrons tout de suite deux caractérisations des sous-groupes distingués.

Lemme 2.1.
Les trois propositions suivantes sont équivalentes :
$\bullet H \triangleleft G$.
$\bullet \forall g \in G, gH = Hg$.
$\bullet \forall g \in G, g^{-1}Hg = H$.

Démonstration 2.6.
• *Supposons* $H \triangleleft G$, *et soit* $g \in G$. *En appliquant la définition à* g *et à* g^{-1},
on obtient $\left\{ \begin{array}{l} g^{-1}Hg \subset H \\ gHg^{-1} \subset H \end{array} \right.$ *d'où* $\left\{ \begin{array}{l} g(g^{-1}Hg) \subset gH \\ (gHg^{-1})g \subset Hg \end{array} \right.$ *i.e.* $\left\{ \begin{array}{l} Hg \subset gH \\ gH \subset Hg \end{array} \right.$ *ou encore*

$$Hg = gH.$$

• *Supposons*

$$\forall g \in G, gH = Hg.$$

Pour g *dans* G, *on vérifie que*

$$g^{-1}Hg = (g^{-1}H)g = (Hg^{-1})g = H(g^{-1}g) = H.$$

• *Supposons* $\forall g \in G, g^{-1}Hg = H$.
on a

$$\forall g \in G, g^{-1}Hg \subset H,$$

d'où $H \triangleleft G$.
On a donc montré que si l'on peut munir le quotient G/H *d'une loi* $\cdot$ *vérifiant* $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$, *alors nécessairement le sous-groupe* H *est distingué dans* G *(i.e. que* H *est stable par conjugaison), ce qui revient à dire (d'après le lemme) que les classes à gauche coïncident avec les classes à droite.*

Réciproquement.
Vérifions que la condition $H \triangleleft G$ *suffit à montrer la compatibilité de la relation* $\equiv$ *avec la loi* $\cdot$
Pour $\left\{ \begin{array}{l} x \equiv x^{'} \\ y \equiv y^{'} \end{array} \right.$ *, on a*

$$\begin{array}{rcl} \overline{xy} & = & (xy)H = x(yH) = x(y^{'}H) = x(Hy^{'}) = (xH)y^{'} \\ & = & (x^{'}H)y^{'} = (Hx^{'})y^{'} = H(x^{'}y^{'}) = (x^{'}y')H = \overline{x'y'}. \end{array}$$

Il reste juste à vérifier l'associativité de la loi quotient, mais elle découle naturellement de l'associativité de la loi dans G :

$$\overline{x} \cdot (\overline{y} \cdot \overline{z}) = \overline{x} \cdot (\overline{yz}) = \overline{x(yz)} = \overline{(xy)z} = (\overline{x} \cdot \overline{y}) \cdot \overline{z}.$$

Conclusion 2.3.
Soit H *un sous-groupe de* G. *La loi quotient* $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$ *sur* G/H *est bien définie si et seulement si* H *est distingué dans* G, *et alors la projection canonique :*

$$\pi : \left\{ \begin{array}{c} (G, \cdot) \to (G/H, \cdot) \\ g \mapsto \overline{g} = gH \end{array} \right.$$

est un morphisme de groupes. ce qui fournit au passage le neutre $1_{G/H} = \overline{1_G}$ *et l'inverse* $\overline{x}^{-1} = \overline{x^{-1}}$.
Juste un point pour finir concernant le terme de projection canonique : si E *est un ensemble*

non vide muni d'une relation d'équivalence $\Re$ pour laquelle on note $\overline{x}$ la classe d'un élément x de E, l'application :

$$\pi : \begin{cases} E \to E/_{\Re} \\ x \mapsto \overline{x} \end{cases}$$

est usuellement appelée projection canonique. Le terme projection (qui signifie surjection) vient du caractère surjectif de π (tout $\overline{x}$ a un antécédent x), et l'adjectif canonique découle de la définition simplisme de π l'ensemble E considéré est notre groupe G, et on quotiente par la relation de congruence modulo H.

2.3 Quotient d'un anneau par un idéal

Définition 2.6.
Soit A un anneau et I un sous-groupe additif de A. Comme $(A, +)$ est abélien, le quotient A/I est un groupe abélien. Le morphisme de groupes $\pi : A \to A/I$, qu'on appellera souvent la surjection canonique, a I pour noyau.
Supposons A/I muni d'une structure d'anneau de manière à ce que π soit un morphisme d'anneaux. Alors le produit dans A/I est donné par :

$$(a + I).(b + I) = \pi(a).\pi(b) = \pi(ab) = ab + I.$$

Et le sous-groupe I, en tant que noyau du morphisme d'anneaux π, est nécessairement un idéal. On va donc définir une multiplication sur A/I par la formule ci dessus et montrer que si réciproquement I est un idéal, elle est bien définie, c'est-à-dire ne dépend pas des représentants choisis. Elle définira donc une structure d'anneaux sur A/I.
Vérifions que, pour tous a, b de A, la classe du produit $ab + I$ ne dépend que des classes $a + I$ et $b + I$. Or, si le sous-groupe additif I est un idéal :

$$(a + I)(b + I) = \{a'b' | a' - a \in I, b' - b \in I\} \subset ab + aI + Ib + II \subset ab + I.$$

Ainsi, si $a' + I = a + I$ et $b' + I = b + I$ alors $a'b' \in ab + I$ et $a'b' + I = ab + I$. L'élément 0 de A/I est défini par $0 + I = I$ et l'élément 1 par $1 + I$. Que A/I est ainsi muni d'une structure d'anneau découle ensuite directement du fait que A est un anneau. On a donc montré.

Proposition 2.4.
Soit A un anneau et I un sous-groupe additif de A. Les lois de A munissent le quotient A/I d'une structure d'anneau si, et seulement si, le sous-groupe I est un idéal de A.
Si $I \subset A$ est un idéal, A/I est en tant que ensemble le quotient de A par la relation d'équivalence $a \Re b \Leftrightarrow a - b \in I$. Si l'on note une classe d'équivalence de A/I par $[a]$, la structure d'anneau est donné par :

$$[a] + [b] := [a + b]$$

et

$$[a][b] = [ab].$$

Cette notation a l'avantage d'être plus courte que $a + I$, mais est moins précise dans le sens qu'elle ne mentionne pas l'idéal I. Quand il n'y a pas de risque de confusion, on utilisera souvent la notation $[a]$ pour désigner une classe. Mais le plus souvent, on voit l'anneau A/I comme un anneau tout court, et on notera ses éléments donc par $x, y, z, \ldots$

Remarque 2.7.
On ajoute une loi multiplicative $\times$ de façon a ce que $(A/I, +, \times)$ devienne un anneau, et poser

$$\overline{a} + \overline{b} = \overline{a \times b}.$$

Se pose a nouveau le problème de l'indépendance de $\overline{a \times b}$ par rapport aux représentants a et b. Cherchons les conditions que cela implique sur le sous-groupe I considéré. Soit a quelconque dans A, i quelconque dans I. Puisque :

$$\begin{cases} \overline{a+i} = \overline{a} \\ \overline{0} = \overline{i} \end{cases}$$

On devrait avoir $\overline{a + i \times 0} = \overline{a \times i}$,i.e. $\overline{ai} = \overline{0} = I$, ou encore $ai \in I$, et de même $ia \in I$. Ceci tenant pour tout i dans I, on doit donc avoir :

$$\forall a \in A \begin{cases} aI \subset I \\ Ia \subset I \end{cases}$$

que l'on écrira de manière plus concise :

$$\begin{cases} AI \subset I \\ IA \subset I \end{cases}$$

Remarque 2.8.
Un tel sous-groupe stable par multiplication scalaire à droite et à gauche est appelé idéal bilatère de A. On parle également d'idéal à gauche si $AI \subset I$, et d'idéal à droite si $IA \subset I$, i.e un idéal des deux côtés, d'où son nom. Évidemment, si l'anneau A est commutatif, les trois notions coïncident, et on parle alors d'idéal tout court. Donnons immédiatement une caractérisation "vectorielle" (ou "linéaire") des idéaux dans le cas où A est commutatif (le plus fréquent).

Lemme 2.2.
Soit A un anneau commutatif et I une partie de A. Les deux propositions suivantes sont équivalentes :
• *I est un idéal de A ;*
• *I contient 0_A et est stable par combinaisons linéaires à coefficients dans A.*

Démonstration 2.7.
• *Supposons que I soit un idéal de A. $(I, +)$ est donc un sous-groupe de $(A, +)$, donc il contient 0_A. De plus,pour i, j dans I et a, b dans A, par définition d'un idéal, ai et bj sont dans I, donc leur somme aussi (puisque I est stable par $+$), donc I est stable par combinaisons linéaires.*
• *Supposons que I contienne 0_A et soit stable par combinaisons linéaires. Pour tout i, j de I, les combinaisons linéaires $i + j$ et $-i$ restent donc dans I, donc I est stable par $+$ et par passage à l'opposé, donc $(I, +)$ est un groupe. De plus, pour tout a dans A, la combinaison linéaire ai reste dans I. Il en résulte que I est un idéal.*

Remarquer que cette caractérisation vectorielle des idéaux reste valable si A n'est plus supposé commutatif, à condition de remplacer "idéal" par "idéal à droite" et "combinaisons linéaires" par "combinaisons linéaires à droite" (idem à gauche, bien sûr).
Attention à ne surtout pas dire qu'un idéal (bilatère, à gauche, ou à droite) contient le neutre multiplicatif 1_A. D'une part il faudrait déjà que l'anneau A soit unitaire pour avoir l'existence de 1_A, d'autre part un idéal contenant 1_A contient tous les combinaisons linéaires $a1_A$ ou 1_Aa pour a dans A et donc vaut A tout entier. En résumé, si I est un idéal (bilatère, à gauche, ou à droite) de A unitaire :

$$1_A \in I \Longleftrightarrow I = A.$$

Vérifions maintenant que la condition I idéal bilatère de A suffit à définir une loi multiplicative $\times$ sur A/I
vérifiant

$$\overline{a} \times \overline{b} = \overline{a \times b}.$$

Pour $\left\{ \begin{array}{l} a \equiv a' \\ b \equiv b' \end{array} \right.$ *,i.e* $\left\{ \begin{array}{l} a' - a = i_a \in I \\ b' - b = i_b \in I \end{array} \right.$ *, on a :*

$$\overline{a'b'} = a'b' + I = (a + i_a)(b + i_b) + I = ab + \underbrace{ai_b}_{\in I} + \underbrace{i_a b}_{\in I} + \underbrace{i_a i_b}_{\in I} + I = ab + I = \overline{ab}.$$

Il reste enfin à montrer la distributivité de $\times$ sur $+$ dans le quotient, mais ceci est immédiat en passant tout sous la barre et en utilisant les propriétés de $\times$ de l'anneau de départ :

$$\overline{a} \times (\overline{b} \times \overline{c}) = \overline{a} \times (\overline{b + c}) = \overline{a \times (b + c)} = \overline{a \times b + a \times c} = \overline{a} \times \overline{b} + \overline{a} \times \overline{c}.$$

Exemple 2.1.
$\mathbb{Z}/n\mathbb{Z}$. Fixons un entier $n \geq 2$ Considérerons le groupe additif $\mathbb{Z}/n\mathbb{Z} = \overline{0}, \overline{1}, ..., \overline{n-1}$.
Rappelons que l'addition est définie par :

$$\overline{x} + \overline{y} = \overline{x + y}$$

pour tous

$$\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}.$$

On a vu que cette définition est indépendante des représentants choisis, et que le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est abélien. On définit une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ à partir de celle de $\mathbb{Z}$ en posant :

$$\overline{x}\,\overline{y} = \overline{xy}.$$

pour tous

$$\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}.$$

Cette multiplication est bien définie, indépendamment des représentants choisis.

En effet, si $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, alors $x' = x + nu$ et $y' = y + nv$ pour deux entiers $u, v \in \mathbb{Z}$, de sorte que

$$x'y' = xy + n(uy + vx + nuv), \quad d'\text{où} \quad \overline{x'y'} = \overline{xy}.$$

Il est immédiat de vérifier que $\mathbb{Z}/n\mathbb{Z}$ satisfait les conditions suivant :
(1)- la multiplication est associative, c'est-à-dire :

$$x(yz) = (xy)z$$

pour tous

$$x, y, z \in A.$$

(2)- la multiplication est distributive sur l'addition à gauche et à droite, c'est-à-dire :

$$x(y + z) = xy + xz$$

et

$$(x + y)z = xz + yz.$$

pour tous $x, y, z \in A$. que $\overline{1}$ est neutre pour la multiplication, et que la multiplication est commutative. On conclut que :

$$\mathbb{Z}/n\mathbb{Z}.$$

est un anneau commutatif unitaire.

2.4 Quotient d'un espace vectoriel par un sous-espace vectoriel

2.4.1 Aspects algébriques :

Soit E un espace vectoriel et soit F un sous-espace vectoriel de E. On définit la relation suivante entre vecteurs de E

$$x\Re y \Leftrightarrow x - y \in F$$

La relation précédente est une relation d'équivalence car :
(1) elle est réflexive : $x\Re x$ puisque $0 \in F$,
(2) elle est symétrique : $x\Re y$ implique $y\Re x$ puisque $x - y \in F$ implique

$$y - x = -(x - y) \in F$$

(3) elle est transitive : $x\Re y$ et $y\Re z$ impliquent $x\Re z$ puisque $x - y \in F$ et $y - z \in F$ impliquent

$$x - z = (x - y) + (y - z) \in F.$$

on peut considérer le groupe quotient

$$E/F = \{\overline{x} = x + F; x \in E\}$$

muni de la loi

$$\overline{x} + \overline{y} = \overline{x + y}.$$

Comme pour les anneaux, on aimerait rajouter une loi externe $\cdot$ de façon à ce que $(E/_F, +, \cdot)$ devienne un espace vectoriel.
On pose $\lambda \cdot \overline{x} = \overline{\lambda \cdot x}$. et pose à nouveau le problème de l'indépendance de $\overline{\lambda \cdot x}$ par rapport au représentant x de $\overline{x}$. Si la définition est correcte, on doit avoir pour tout f de F, pour tout scalaire λ :

$$\overline{f} = f + F = F = \overline{0} \Rightarrow \lambda\overline{f} = \lambda\overline{0} \Rightarrow \overline{\lambda f} = \overline{\lambda 0} = \overline{0} \Rightarrow \lambda f \in F,$$

donc F doit être stable par multiplication scalaire ,
comme F est déjà par hypothèse stable par somme, il en résulte que F doit être un sous-espace vectoriel de E.
Réciproquement, on a bien que, pour F sous-espace vectoriel de E,

$$\overline{x} = \overline{y} \Rightarrow x - y \in F \Rightarrow \lambda(x - y) \in F \Rightarrow \lambda x - \lambda y \in F \Rightarrow \overline{\lambda x} = \overline{\lambda y}$$

et donc la loi

$$\lambda \cdot \overline{x} = \overline{\lambda \cdot x}$$

est bien définie sur E/F .
Les vérifications d'usage que $(E/_F, +, \cdot)$ est bien un espace vectoriel se font en passant tout sous la barre et en utilisant la structure d'espace vectoriel de E , par exemple :

$$\lambda \cdot (\overline{x} + \overline{y}) = \lambda \cdot (\overline{x + y}) = \overline{\lambda \cdot (x + y)} = \overline{\lambda \cdot x + \lambda \cdot y} = \lambda \cdot \overline{x} + \lambda \cdot \overline{y}$$

En dimension finie, on peut dire des choses concernant la dimension du quotient.
On rappelle que si E est de dimension finie n, la codimension de F est définie par

$$codim F = n - dim F.$$

Proposition 2.5.
Soit E un espace vectoriel de dimension finie, F un sous-espace vectoriel de E. On a alors :

$$dim(E/F) = codimF.$$

Démonstration 2.8.
Soit $(e_1, ..., e_p)$ une base de F, que l'on complète en $(e_1, ..., e_p, e_{p+1}, ..., e_n)$ base de E. Alors $(\overline{e_{p+1}}, ..., \overline{e_n})$ est une base de E/F .
En effet, elle est libre car :

$$\sum_{i=p+1}^{n} \lambda_i \overline{e_i} = \overline{0} \Rightarrow \overline{\sum_{i=p+1}^{n} \lambda_i e_i} = \overline{0} \Rightarrow \sum_{i=p+1}^{n} \lambda_i e_i \in F \Rightarrow (\lambda_i) = (0)$$

par liberté de la base $(e_1, ..., e_n)$ et elle est génératrice car, pour $\overline{x} \in E/F$, x se décompose sur la base $(e_1, ..., e_n)$ en $x = \sum_{i=1}^{n} \lambda_i e_i$ d'où

$$\overline{x} = \overline{\sum_{i=1}^{n} \lambda_i e_i} = \overline{\underbrace{\sum_{i=1}^{p} \lambda_i e_i}_{\in F}} + \overline{\sum_{i=p+1}^{n} \lambda_i e_i} = \overline{0} + \sum_{i=p+1}^{n} \lambda_i \overline{e_i} \in Vect(\overline{e_{p+1}}, ..., \overline{e_n}).$$

Remarque 2.9.
Dans le cas où E est normé, on peut transporter la structure d'espace vectoriel normé dans le quotient E/F , sous réserve que le sous-espace vectoriel F par lequel on quotiente soit fermé. Le caractère complet passe alors également au quotient au sens de la proposition suivante.

Théorème 2.3.
Dans le cas particulier où E est de dimension finie, on a :

$$dimE/F = dimE - dimF.$$

Démonstration 2.9.
En effet, si l'on considère un supplémentairement G de F et $(g_1, ..., g_k)$ une base de G alors $(\overline{g_1}, ..., \overline{g_k})$ est une base de E/F. Le fait que cette famille soit libre découle du fait que

$$\lambda \overline{g_1} + ... + \lambda_k \overline{g_k} = \overline{0}$$

implique que $\lambda_1 g_1 + ... + \lambda_k g_k \in G \cap F = 0$, ce qui implique que tous les coefficients λ_i sont nuls puisque la famille $(g_1, ..., g_k)$ est libre. Le fait que cela soit une famille génératrice vient du fait que l'on peut compléter la famille $(g_1, ..., g_k)$ par des vecteurs $(f_1, ..., f_m)$ de F pour former une base de E. Il suffit alors de décomposer n'importe quel vecteur x de E selon cette base et passer cette égalité au quotient

$$x = \sum_{j=1}^{k} \lambda_j g_j + \sum_{j=1}^{m} u_j f_j.$$

implique

$$\overline{x} = \sum_{j=1}^{k} \lambda_j \overline{g_j} + \overline{0}.$$

2.4.2 Aspects analytiques :

Proposition 2.6.
On suppose désormais que E est un espace normé et que F est un sous- espace fermé de E. On veut définir une norme sur l'espace quotient ; on pose pour cela

$$\|\overline{x}\| = d(x, F).$$

Démonstration 2.10.
Il faut montrer que cette quantité ne dépend pas du choix du représentant x de $\overline{x}$. Si $x\Re x^{'}$ alors $x - x^{'} \in F$ et par conséquent :

$$d(x,F) = \inf_{f\in F} \|x - f\| = \inf_{f\in F} \|x^{'} - \underbrace{(f + x^{'} - x)}_{=f^{'}\in F}\| = \inf_{f^{'}\in F} \|x^{'} - f^{'}\| = d(x^{'},F).$$

On peut à présent vérifier que la fonction (à valeurs positives) que l'on a définie sur E/F est bien une norme.
(1) Si $\|\overline{x}\| = 0$ alors $d(x;F) = 0$, ce qui implique que $x \in F$ car F est un sous-espace fermé de E, donc que

$$\overline{x} = \overline{0}.$$

(2) On a $\|\overline{0}\| = d(0;F) = 0$ et si $\lambda \neq 0$ alors on a

$$\|\lambda\overline{x}\| = \inf_{f\in F} \|\lambda x - f\| = |\lambda| \inf_{f\in F} \|x - \underbrace{\lambda^{-1}f}_{\in F}\| = |\lambda| d(x,F) = |\lambda| \|\overline{x}\|.$$

(3) Il reste à vérifier l'inégalité triangulaire, soit

$$d(x+y,F) \leqslant d(x,F) + d(y,F).$$

Or pour tout $s,t \in F$ on a $s+t \in F$ et donc

$$d(x+y,F) \leqslant \|x+y-s-t\| \leqslant \|x-s\| + \|y-t\|.$$

En passant à la borne inférieure dans l'inégalité précédente successivement dans la variable s puis t, on obtient l'inégalité désirée. On considère alors l'application suivante

$$\pi : \left\{ \begin{array}{c} E \longrightarrow E/F \\ x \mapsto \overline{x} \end{array} \right.$$

C'est une application linéaire continue. En effet, on a :

$$\|\pi(x)\| = \|\overline{x}\| = d(x,F) = \inf_{f\in F} \|x - f\| \leq \|x\|$$

ce qui implique

$$\|\pi\|_{L(E,E/F)} \leq 1.$$

En outre π est une application ouverte. Comme π est linéaire, il suffit de vérifier que $\pi(B_E(0,1))$ est un voisinage de l'origine. Ce dernier point découle de l'égalité

$$\pi(B_E(0,1)) = B_{E/F}(0,1)$$

qui se vérifie aisément :

$$si \;\; \overline{x} \in B_{E/F}(0,1) \;\; alors \;\; d(x,F) < 1$$

et il existe donc $f \in F$ tel que $\|x - f\| < 1$ par conséquent

$$\overline{x} = \pi(x - f) \in \pi(B_E(0,1).$$

Inversement,

$$si \;\; \overline{x} = \pi(x) \in \pi(B_E(0,1)) \;\; alors \;\; \|\overline{x}\| \leq \|\pi\|_{L(E,F)} \|x\| < 1,$$

donc

$$\overline{x} \in B_{E/F}(0,1).$$

Conclusion 2.4.
Soit F un sous-groupe de $(E,+)$. La loi quotient $\lambda \cdot \overline{x} = \overline{\lambda \cdot x}$ sur E/F est bien définie si et seulement si F est un sous-espace vectoriel de E et alors la projection canonique

$$\pi : \begin{cases} (E,+,.) \longrightarrow (E/F,+,.) \\ x \longmapsto \overline{x} = x + F \end{cases}$$

est une application linéaire. Si de plus E est de dimension finie, alors

$$dim(E/F) = codimF.$$

2.5 Quotient d'une algèbre unitaire par un idéal

Définition 2.7.
Considérons une algèbre $(A,+,\times,\cdot)$ unitaire et I un sous-groupe de $(A,+)$. On peut considérer le quotient

$$A/I = \{\overline{a} = a + I : a \in A\}$$

muni de la loi $\overline{a} + \overline{b} = \overline{a+b}$
On aimerait rajouter une loi $\times$ et une loi $\cdot$ de sorte que A/I soit une algèbre avec les lois agréables

$$\begin{cases} \lambda \cdot \overline{a} = \overline{\lambda.a} \\ \overline{a} \times \overline{b} = \overline{ab} \end{cases}$$

A/I devra en particulier être un anneau pour la loi quotient $\times$, donc I devra être un idéal bilatère de A. L'algèbre A étant unitaire, tout idéal est stable par multiplication scalaire en vertu de l'identité :

$$\lambda.i = (\lambda.1) \times i.$$

Chapitre 3

Factorisation canonique des morphismes,théorèmes d'isomorphismes

3.1 Factorisation canonique d'une application quelconque

Soit f une application d'un ensemble E non vide dans un ensemble F non vide, ce que l'on note usuellement :

$$f : \begin{cases} E \longrightarrow F \\ x \longmapsto f(x) \end{cases}$$

f n'a aucune raison d'être injective, surjective, a fortiori bijective.

Définition 3.1.
On peut toujours la "rendre" surjective en considérant l'application

$$f' : \begin{cases} E \longrightarrow Imf \\ x \longmapsto f(x) \end{cases}$$

On a juste changé l'ensemble d'arrivé

Définition 3.2.
Il est plus difficile de rendre une application injective. L'ennui est qu'à une image $f(x)$ on pourrait trouver deux antécédents x et y (ou même plus) distincts.
Pour une image $f(x)$ donnée, on regroupe tous ses antécédents, on les met dans un sac étiqueté $\overline{x}$, on note $\overline{E}$ l'ensemble des sacs d'antécédents, et on considère l'application

$$\tilde{f} : \begin{cases} \overline{E} \longrightarrow F \\ \overline{x} \longmapsto f(x) \end{cases}$$

Avant, pour une image $f(x)$ donnée, on avait plusieurs antécédents par f maintenant, on en toujours autant (par f), mais en les regroupant et en les ficelant, il n'en reste qu'un seul par $\tilde{f}$, qui est son sac d'antécédents par f. Il en résulte que $\tilde{f}$ est injective.

Proposition 3.1.
Si l'on souhaite formaliser ce qui précède, on considère la relation d'équivalence $\Re$ sur E définie par $x\Re y \Leftrightarrow f(x) = f(y)$, on note $\overline{x}$ la classe d'un élément x de E, $\overline{E}$ l'ensemble quotient $E/\Re$

et on a alors

$$\tilde{f}(\overline{x}) = \tilde{f}(\overline{y}) \Rightarrow f(x) = f(y) \Rightarrow \overline{x} = \overline{y}$$

d'où l'injectivité de $\tilde{f}$

Si l'on résume les deux transformations que l'on a effectuées, on peut "injectiviser" f *en ligottant les éléments ayant même image, on obtient alors une application*

$$\tilde{f} : \begin{cases} \overline{E} \longrightarrow F \\ \overline{x} \longmapsto f(x) \end{cases}$$

Puis on peut "surjectiviser" $\tilde{f}$ *en changeant l'ensemble d'arrivée, ce qui donne au final une application bijective*

$$\overline{f} : \begin{cases} \overline{E} \longrightarrow Imf \\ \overline{x} \longmapsto f(x) \end{cases}$$

Pour faire le lien avec l'application $f : \begin{cases} E \longrightarrow F \\ x \longmapsto f(x) \end{cases}$ *de départ, la première transformation consiste envoyer un élément* x *de* E *sur sa classe* $\overline{x}$ *dans* $\overline{E}$*, ce qui se fait au moyen de la projection canonique*

$$\pi : \begin{cases} E \longrightarrow \overline{E} \\ x \longmapsto \overline{x} \end{cases}$$

Puis on envoie le paquet $\overline{x}$ *d'antécédents sur son unique image* $f(x)$*, ce qui se fait via l'application bijective*

$$\overline{f} : \begin{cases} \overline{E} \longrightarrow Imf \\ \overline{x} \longmapsto f(x) \end{cases}$$

Notre élément x *de départ est rendu dans* Imf*, on voudrait l'envoyer dans* F *, c'est pourquoi on considère l'injection canonique*

$$\iota : \begin{cases} Imf \longrightarrow F \\ x \longmapsto x \end{cases}$$

Finalement, on a le parcours suivant :

$$E \xrightarrow{\pi} \overline{E} \xrightarrow{\overline{f}} Imf \xrightarrow{\iota} F$$

$$f = \iota \circ \overline{f} \circ \pi$$

C'est ce qu'on appelle la factorisation canonique de f *(factorisation pour la loi* $\circ$*, bien sûr) En général,on représenter ces deux dernières relations sur un schéma, appelé diagramme (c'est juste des ensembles avec des flèches représentant des applications entre ces ensembles) commutatif (ça veut dire que, quand on suit les flèches le long de deux chemins différents qui mènent de* A *à* B*, les composées d'applications que l'on considère sont égales) :*

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ \overline{E} & \xrightarrow{\overline{f}} & Imf \end{array}$$

Remarque 3.1.
On dispose d'une bijection $\overline{f}$ *reliant le quotient* E *à l'image* Imf*. On verra bientôt la factorisation canonique des morphismes où cette bijection devient un isomorphisme qu'il est très souvent opportun de considérer.*

3.2 Factorisation canonique d'un morphisme de groupes

Définition 3.3.
Considérons G et H deux groupes f un morphisme de groupes de G dans H, c'est-à-dire que pour tout x,y dans G on a :

$$f(xy) = f(x)f(y).$$

Proposition 3.2.
La relation "x et y ont même image par f" est la relation de congruence modulo $Kerf$.

Démonstration 3.1.
La relation "x et y ont même image par f" définissait une relation d'équivalence sur G, déterminée par :
$f(y) = f(x) \Leftrightarrow f(x)^{-1}f(y) = 1_H \Leftrightarrow f(x^{-1})f(y) = 1_H \Leftrightarrow f(x^{-1}y) = 1_H \Leftrightarrow x^{-1}y \in Kerf \Leftrightarrow y \in xKerf \Leftrightarrow y = x(modKerf)$,
alors la relation "x et y ont même image par f" est la relation de congruence modulo $Kerf$.

Proposition 3.3.
On a l'ensemble quotient G est égal à $G/Kerf$. Pour munir ce dernier d'une structure de groupe pour la loi quotient, il convient de vérifier que $Kerf$ est distingué dans G.

Démonstration 3.2.
Pour $k \in Kerf$ et $g \in G$ on a :

$$f(x^{-1}kx) = f(x^{-1})f(k)f(x) = f(x)^{-1}1_H f(x) = f(x)^{-1}f(x) = 1_H,$$

d'où $x^{-1}kx \in Kerf$; donc $x^{-1}(Kerf)x \subset Kerf$
i.e. $Kerf \triangleleft G$ comme voulu.

Proposition 3.4.
Supposons que $H \triangleleft G$ Notons $\pi : G \to G/H$ l'application qui à $x \in G$ associe sa classe d'équivalence $\overline{x}$ dans G/H. Alors π est un homomorphisme de groupe. De plus $H = Ker\pi$ et π est surjectif.

Démonstration 3.3.
Soient x et y des éléments de G alors

$$\pi(x \cdot y) = \overline{x \cdot y} = \overline{x} \cdot \overline{y} = \pi(x) \cdot \pi(y).$$

Cette propriété n'est que l'expression de la définition de la loi de groupe sur G/H. Pour l'égalité entre le noyau de π et H, il suffit de remarquer que tout élément de H est équivalent dans G/H au neutre de G/H. De plus si $\overline{x}$ est un élément de G/H, x est un antécédent de cet élément par π. Donc π est bien surjectif.

Proposition 3.5.
La bijection

$$\overline{f} : \begin{cases} G/Kerf \to Imf \\ \overline{x} \mapsto f(x) \end{cases}$$

est un morphisme de groupes.

Démonstration 3.4.
$\overline{f}$ est un morphisme de groupes car :

$$\overline{f}(\overline{x} \cdot \overline{y}) = \overline{f}(\overline{x \cdot y}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y}).$$

Remarque 3.2.
(Remarquer que ceci découle de ce que f est un morphisme ainsi que des lois quotients), la projection canonique π est également un morphisme de groupes (par construction de la loi quotient), et de même trivialement pour l'injection canonique ι.

On a donc la décomposition canonique de f en morphismes de groupes $f = \iota \circ \overline{f} \circ \pi$, ce que l'on peut représenter par le diagramme commutatif :

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ G/ker f & \xrightarrow[\overline{f}]{} & imf \end{array}$$

On dispose également de l'isomorphisme de groupes

$$G/Ker f \simeq Imf.$$

Le caractère bijectif a déjà été expliqué dans le cas général (à une image correspond son unique paquet d'antécédents), et le caractère de morphisme vient juste de celui de f ainsi que de la structure de groupe qui passe de G à $G/Ker f$ via la loi quotient.

Corollaire 2.
On retiendra de tout ceci que, si $f : G \longrightarrow H$ est un morphisme de groupes, alors le noyau $Ker f$ est distingué dans G et on a l'isomorphisme de groupes

$$\begin{cases} G/Ker f \simeq Imf \\ \overline{x} \longmapsto f(x) \end{cases}$$

3.2.1 Théorèmes d'isomorphismes

Premier théorème d'isomorphisme :

On va maintenant pouvoir énoncer un théorème de première importance en algèbre, appelé propriété universelle des groupes quotients, ou premier théorème d'isomorphisme.

Théorème 3.1. *(Premier théorème d'isomorphisme)*
Soit G un groupe, $H \triangleleft G$ et $\pi : G \to G/H$ la surjection canonique. Soit $f : G \to G'$ un morphisme de groupes tel que $H \subseteq ker(f)$,
alors il existe un unique morphisme $\varphi : G/H \to G'$ tel que $f = \varphi \circ \pi$. De plus
(i) si $H = ker(f)$ alors φ est injective ;
(ii) si f est surjective, alors φ est surjective.
Plus spécifiquement, si f est surjective et $H = ker(f)$ alors φ est un isomorphisme.

Remarque 3.3.
On peut mémoriser ce résultat en le résumant dans le diagramme (On dit que le diagramme est commutatif, puisque $f = (\varphi \circ \pi)$) suivant :

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists!\varphi} & \\ G/H & & \end{array}$$

Démonstration 3.5.
Unicité : *Soit φ et φ' tel que*

$$f = \varphi \circ \pi = \varphi' \circ \pi.$$

Soit $x \in G$ alors

$$f(x) = \varphi \circ \pi(x) = \varphi' \circ \pi(x),$$

donc

$$\varphi(\pi(x)) = \varphi'(\pi(x)).$$

Donc pour tout $xH \in G/H$ on a :

$$\varphi(xH) = \varphi'(xH).$$

D'où

$$\varphi = \varphi'$$

car deux fonctions sont égales si et seulement si leurs valeurs sur tous les éléments de l'ensemble de départ sont égales.
Existence : *Commençons par montrer que la fonction $\varphi : G/H \to G'$ définie par $\varphi(xH) = f(x)$, $x \in G$, est bien définie. Pour cela, il faut montrer que :*

$$si \quad xH = yH \quad alors \quad f(x) = f(y).$$

Ainsi, soit $x, y \in G$ tel que $xH = yH$. Donc

$$x^{-1}yH = H$$

et donc

$$x^{-1}y \in H \subseteq ker(f).$$

D'où

$$f(x^{-1}y) = e_{G'}.$$

Comme f est un morphisme de groupes, on obtient que

$$f(x)f(y)^{-1} = e_{G'}$$

et donc que

$$f(x) = f(y).$$

La fonction φ est bien définie.
Il reste à montrer que φ est un morphisme de groupes, que si $ker(f) = H$ alors φ est injective. Et que si f est surjective, alors φ l'est aussi.
• *φ est un morphisme de groupe car :*

$$si\ xH, x'H \in G/H$$

alors puisque f est un morphisme de groupes on obtient

$$\varphi(xH \cdot x'H) = \varphi(xx'H) = \varphi \circ \pi(xx') = f(xx') = f(x)f(x') = \varphi \circ \pi(x)\varphi \circ \pi(x') = \varphi(xH)\varphi(x'H).$$

• *φ est surjective si f l'est :*
soit $y \in G'$, alors il existe $x \in G$ tel que $f(x) = y$.
D'où

$$\varphi(xH) = \varphi \circ \pi(x) = f(x) = y.$$

• *φ est injective si $H = ker(f)$:*

$$soit\ xH, x'H \in G/H$$

tel que

$$\varphi(xH) = \varphi(x'H),$$

alors

$$f(x) = f(x').$$

Autrement dit, et en utilisant le fait que f est un morphisme de groupes, on a

$$f(x^{-1}x') = e_{G'}$$

Donc

$$x^{-1}x' \in ker(f) = H.$$

On en déduit que

$$x^{-1}x'H = H$$

et donc que

$$x'H = xH.$$

En d'autres termes, φ est bien injective.

Deuxième théorème d'isomorphisme :

Lemme 3.1. *(fondamental de factorisation)*
Soient G un groupe, H un sous-groupe normal dans G, et p la surjection canonique $G \longrightarrow G/H$.
Soient G' un groupe, H' un sous-groupe normal dans G', et p' la surjection canonique $G' \longrightarrow G'/H'$.
Alors, pour tout morphisme de groupes $f : G \longrightarrow G'$ vérifiant la condition $f(H) \subset H'$, il existe un unique morphisme $\varphi : G/H \to G'/H'$ tel que $\varphi \circ p = p' \circ f$.

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ G/H & \xrightarrow{\varphi} & G'/H' \end{array}$$

Démonstration 3.6.
Posons $g = p' \circ f$,qui est un morphisme de groupes $G \to G'/H'$, comme composé de deux morphismes.
Afin d'appliquer le premier théorème d'isomorphisme, montrons que $H \subseteq Kerg$.
Soit $x \in H$. On a

$$f(x) \in f(H).$$

L'hypothèse $f(H) \subseteq H'$ implique donc :

$$f(x) \in H'.$$

D'où

$$p'(f(x)) = \overline{e}'.$$

On déduit que :

$$g(x) = \overline{e}',$$

c'est-à-dire

$$x \in Kerg.$$

Ainsi $g : G \to G'/H'$ *est un morphisme vérifiant*

$$H \subseteq Kerg.$$

le premier théorème d'isomorphisme assure l'existence d'un unique morphisme

$$\varphi : G/H \to G'/H'$$

tel que

$$\varphi \circ p = g,$$

d'où le résultat.

Remarque 3.4.
Avec les données et notations ci-dessus, on a :
($p' \circ f$ *surjectif)* $\Rightarrow$ *(* φ *surjectif)* *et (* $H = Ker(p' \circ f) \Leftrightarrow f^{-1}(H') = H \Rightarrow$ *(* φ *injectif).*

Théorème 3.2. *(Deuxième théorème d'isomorphisme)*
Soient G *un groupe et* H *un sous-groupe normal dans* G*. Pour tout sous-groupe* K *de* G*, le sous-ensemble* HK *est un sous groupe de* G*, et l'on a :*

$$H \cap K \lhd K, \quad H \lhd HK, \quad K/(H \cap K) \simeq HK/H.$$

Démonstration 3.7.
Rappelons que

$$HK = \{hk; h \in H; k \in K\}.$$

Vérifions que HK *est un sous-groupe de* G*.*
On a clairement $e \in HK$*.*
Soient

$$x, y \in HK.$$

Il existe

$$h, h' \in H \quad et \quad k, k' \in K$$

tels que

$$x = hk \quad et \quad y = h'k'.$$

Donc

$$x^{-1}y = k^{-1}h^{-1}h'k' = k^{-1}(h^{-1}h')k(k^{-1}k').$$

Puisque

$$h^{-1}h' \in H \quad et \quad H \lhd G,$$

on a

$$k^{-1}(h^{-1}h')k \in H.$$

Comme par ailleurs

$$k^{-1}k' \in K$$

on a bien

$$x^{-1}y \in HK.$$

On conclut que HK *est un sous-groupe de* G*. Vérifions que*

$$H \cap K \lhd K.$$

Soit

$$h \in H \cap K \quad et \quad x \in K.$$

On a

$$xhx^{-1} \in H$$

puisque

$$H \lhd G.$$

On a aussi

$$xhx^{-1} \in K$$

puisque x et h appartiennent au sous-groupe K. On conclut que

$$xhx^{-1} \in H \cap K.$$

Ce qui prouve que

$$H \cap K \lhd K.$$

On peut donc considérer le groupe quotient $K/H \cap K$.
Notons $p : K \to K/H \cap K$ la surjection canonique.
Vérifions que

$$H \lhd HK.$$

Soit

$$\ell \in H \quad et \quad x = hk \in HK$$

avec

$$h \in H, k \in K.$$

On a

$$x\ell x^{-1} = hk\ell k^{-1}h^{-1}.$$

Puisque

$$H \lhd G \quad et \quad \ell \in H$$

on a

$$k\ell k^{-1} \in H.$$

Donc $x\ell x^{-1} = h(k\ell k^{-1})h^{-1} \in H$ comme produit de trois éléments de H.
Ce qui prouve que

$$H \lhd HK.$$

On peut donc considérer le groupe quotient HK/H.
Notons $p' : HK \to HK/H$ la surjection canonique.
Notons j l'injection canonique $K \to HK$. Rappelons que j est le morphisme défini par

$$j(k) = ke = k$$

pour tout $k \in K$. On a bien sûr

$$j(H \cap K) \subseteq H$$

donc il existe un morphisme de groupes

$$\varphi : K/H \cap K \to HK/H$$

tel que

$$\varphi \circ p = p' \circ j$$

$$\begin{array}{ccc} K & \xrightarrow{\quad j \quad} & HK \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ K/H\cap K & \xrightarrow{\varphi} & HK/H \end{array}$$

Montrons que φ est surjective. Soit $\overline{hk}$ un élément quelconque de HK/H avec

$$h \in H; k \in K.$$

On a

$$\overline{hk} = \overline{h}\,\overline{k} = \overline{k};$$

on déduit que

$$HK/H = p'(K) = (p' \circ j)(K).$$

On conclut d'après le 1^{er} théorème d'isomorphisme que φ est surjective.
Montrons que φ est injective.
Soit $k \in K$ un élément quelconque de $Ker(p' \circ j)$.
On a

$$\overline{e} = p'(j(k)) = p'(k) = \overline{k},$$

c'est-à-dire

$$k \in H.$$

Donc

$$k \in H \cap K;$$

on déduit que

$$Ker(p' \circ j) \subseteq H \cap K.$$

L'inclusion réciproque étant claire, on déduit que

$$Ker(p' \circ j) = H \cap K.$$

On conclut d'après le 1^{er} théorème d'isomorphisme que φ est injective.
On conclut que φ réalise un isomorphisme de $K/H \cap K$ sur HK/H.

Troisième théorème d'isomorphisme :

Théorème 3.3. *(Troisième théorème d'isomorphisme)*
Soient G un groupe, H et K des sous groupes de G. On suppose que $H \lhd G$ et que $K \lhd G$. On suppose de plus que $H \subset K$. Alors :

$$K/H \lhd G/H \quad et \quad \frac{G/H}{K/H} \simeq G/K.$$

Démonstration 3.8.
Soit g un élément de G. Notons $\overline{x}$ sa classe d'équivalence dans G/H et $\overline{\overline{x}}$ sa classe d'équivalence dans G/K.
Montrons que $K/H \lhd G/H$. Pour cela choisissons un élément $\overline{g}$ dans G/H et une élément $\overline{k}$ dans K/H. Alors

$$\overline{g} \cdot \overline{k} \cdot \overline{g}^{-1} = \overline{g \cdot k \cdot g^{-1}} = p'(xkx^{-1}).$$

Or

$$xkx^{-1} \in K.$$

puisque

$$K \lhd G,$$

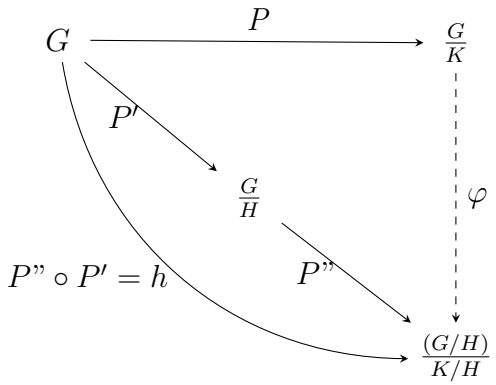
donc

$$\overline{x}\overline{k}\overline{x}^{-1} \in p'(K).$$

Ceci prouve que

$$K/H \lhd G/H.$$

D'après l'hypothèse on a $H \lhd K$*.On considéré le diagramme suivant :*



Pour montrer ***l'existence*** *de* φ *il suffit de montre que* $p'(K) \subset K/H$
soit

$$p'(k) \in p'(K) \quad avec \quad k \in K.$$

on a

$$p'(K) = k \cdot H \in K/H$$

donc

$$p'(K) \subset K/H.$$

Alors et d'après le lemme précédent il existe un unique morphisme φ *de* G/H *vers* $(G/H)/(K/H)$ *tell que*

$$h = (p" \circ p') = (\varphi \circ p)$$

montrons que φ ***injective*** *et* ***surjective*** *:*
On a :

$$\begin{aligned} kerh &= \{x \in G; h(x) = K/H\} \\ &= \{x \in G; p"(xH) = K/H\} \\ &= \{x \in G; (xH) \cdot K/H = K/H\} \\ &= \{x \in G; (xH) \in K/H\} \\ &= \{x \in G; x \in K\} \\ &= G \cap K = K \end{aligned}$$

donc φ *injective d'après la Premier théorème d'isomorphisme.*
• *D'autre part on utilise la Premier théorème d'isomorphisme pour montrer que* h *est surjective puisque* $h = (p" \circ p')$ *et* p', p' *deux application surjective donc* h *est surjective.*
Alors φ *est surjective d'après la premier théorème d'isomorphisme.*

3.3 Factorisation canonique d'un morphisme d'anneaux

Définition 3.4.
Considérons A et B deux anneaux et f un morphisme d'anneaux de A dans B, c'est-à-dire que pour tout a, b, c dans A on a

$$f(ab + c) = f(a)f(b) + f(c)$$

Définition 3.5.
Soit $f : A \longrightarrow B$ un morphisme d'anneaux. On appelle noyau de f et l'on note $Kerf$ l'ensemble des $a \in A$ tels que $f(a) = 0$

Proposition 3.6.
la relation "a et b ont même image par f " est la relation de congruence modulo $Kerf$

Démonstration 3.9.
la relation "a et b ont même image par f " définissent une relation d'équivalence sur A, déterminée par :

$$f(b) = f(a) \Longleftrightarrow f(b - a) = 0_B \Longleftrightarrow b - a \in Kerf \Longleftrightarrow b \in a + Kerf.$$

(cette fois au sens de la loi +).

Proposition 3.7.
On a l'ensemble quotient $\overline{A}$ est égal à $A/kerf$. Pour munir ce dernier d'une structure d'anneau pour les lois quotients, il suffit de montrer que $Kerf$ est un idéal bilatère de A.

Démonstration 3.10.
$Kerf$ est un sous-groupe de $(A; +)$ en tant que noyau d'un morphisme de groupes additifs, et de plus, pour tout i dans $Kerf$, pour tout a dans A, on a

$$f(ai) = f(a)f(i) = f(a)0_B = 0_B$$

d'où $ai \in Kerf$, et de même $ia \in Kerf$. Il en résulte que $Kerf$ est bien un idéal bilatère de A.

Proposition 3.8.
la bijection

$$\overline{f} : \begin{cases} A/Ker \longrightarrow Imf \\ \overline{a} \longmapsto f(a) \end{cases}$$

est un morphisme d'anneaux

Démonstration 3.11.

$$\overline{f}(\overline{a}\overline{b} + \overline{c}) = \overline{f}(\overline{ab + c}) = f(ab + c) = f(a)f(b) + f(c) = \overline{f}(\overline{a})\overline{f}(\overline{b}) + \overline{f}(\overline{c})$$

Remarque 3.5.
(remarquer encore une fois que ceci découle de ce que f est un morphisme, ainsi que des lois quotients), la projection canonique π est aussi un morphisme d'anneaux (par construction des lois quotients), et idem pour l'injection canonique ι

On a donc la décomposition canonique de f en morphismes d'anneaux $f = \iota \circ \overline{f} \circ \pi$, ce que l'on peut récapituler à l' aide du diagramme commutatif

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ A/kerf & \xrightarrow{\overline{f}} & Imf \end{array}$$

ainsi que l'isomorphisme d'anneaux

$$A/Kerf \simeq Imf$$

Le caractère bijectif a déjà été commenté et se voit bien (à une image $f(a)$ correspond son unique paquet d'antécédents : $a + Kerf$), et le caractère de morphisme découle comme dans le cas des groupes de celui de f ainsi que de la structure d'anneau qui passe de A à $A/Kerf$ via les lois quotients.
Petit supplément sur le caractère unitaire : si f est un morphisme d'anneaux unitaires, i.e. si A et B sont unitaires et si $f(1_A) = 1_B$, alors f est aussi un morphisme d'anneaux unitaires puisque :

$$\overline{f}(\overline{1_A}) = f(1_A) = 1_B = 1_{Imf}.$$

Corollaire 3.
retiendra de tout ceci que, si $f : A \longrightarrow B$ est un morphisme d'anneaux (unitaires), alors le noyau $Kerf$ est un idéal bilatère de A et on a l'isomorphisme d'anneaux (unitaires)

$$\begin{cases} A/kerf \simeq Imf \\ \overline{a} \longmapsto f(a) \end{cases}$$

Corollaire 4.
(Premier théorème d'isomorphisme des anneaux) : Soit $f : A \longrightarrow B$ un morphisme d'anneau, alors le quotient $A/Ker(f)$ est isomorphe à l'image de f.

Théorème 3.4.
(Factorisation par le quotient) Soient A,B deux anneaux, $f : A \to B$ un morphisme d'anneaux. Soit I un idéal bilatère de A et $\pi : A \to A/I$ le morphisme d'anneaux canonique.
Les assertions suivantes sont équivalentes :
(1) $f(I) = (0)$
(2) $I \subset Kerf$
(3) *Il existe un unique morphisme d'anneaux $\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ \pi$.*
De plus, si f est surjectif $(resp. I = Ker(f))$ alors f est surjectif $(resp. injectif.)$ Si A, B sont unitaires et si $f : A \to B$ est un morphisme d'anneaux unitaires, alors $\overline{f}$ en est aussi un.

Démonstration 3.12.
(1) $\Rightarrow$ (2) *Définition du noyau.*
(2) $\Rightarrow$ (3) *En vertu du résultat analogue en théorie des groupes, il existe un unique morphisme de groupes $\overline{f} : A/I \to B$ vérifiant $f = \overline{f} \circ \pi$.*
Vérifions la compatibilité de cette définition pour la multiplication.
Soit $x, y \in A$. On a $\overline{f}(\overline{xy}) = \overline{f}(\pi(xy)) = f(xy) = f(x)f(y)$.
Si f est surjectif, on a vu que $\overline{f}$ en tant que morphisme de groupes est surjectif, donc $\overline{f}$ est surjectif en tant que morphisme d'anneaux. Si $I = Kerf$, alors $\overline{f}$ est injective, donc $\overline{f}$ est injective en tant que morphisme d'anneaux.
Si $f : A \to B$ est unitaire, $f(1) = 1$, $\overline{f}(1) = 1$.
$3 \Rightarrow 1$ *Soit $x \in I = 0 + I$*
Alors $\overline{x} = 0$, donc $\overline{f}(x) = \overline{f}(0) = f(0) = 0$.

Proposition 3.9.
1) Un morphisme de factorisation $\tilde{f}$ existe si et seulement si $Ker(f)$ contient $Ker(p)$.
2) Quand $\tilde{f}$ existe, il est unique. Il est surjectif si, et seulement si, f est surjectif, et il est injectif si, et seulement si, $Ker(f) = Ker(p)$.

Démonstration 3.13.
1) Il est clair que si $\tilde{f}$ existe, alors $Ker(p)$ est inclus dans $Ker(\tilde{f} \circ p) = Ker(f)$. Réciproquement, supposons que $Ker(p)$ est inclus dans $Ker(f)$. Pour tout x dans Q, choisissons g dans G tel que $p(g) = x$. Posons $\tilde{f}(x) = f(g)$. Cette définition ne dépend pas du choix de g dans $p^{-1}(x)$ car deux éléments de même image ne diffèrent que par un élément du noyau : si $p(g') = x$, alors $p(gg'^{-1})$=$p(g)p(g')^{-1}$= $xx^{-1} = 1$, d'où $gg'^{-1} \in Ker(p)$. Comme $Ker(p) \subset Ker(f)$, $f(g') = f(g)$ Une fois que $\tilde{f}$ est bien définie, il est facile de vérifier qu'elle respecte les produits : si $p(g) = x$ et $p(g') = x'$ alors $p(gg') = xx'$ et donc $\tilde{f}(xx') = f(gg') = f(g)f(g) = \tilde{f}(x)$.
2) L'unicité résulte de la surjectivité de p. Il en résulte aussi que f et $\tilde{f}$ ont même image. Enfin, on observe que $Ker(\tilde{f}) = p(Ker(f))$, de sorte que $\tilde{f}$ est injectif si et seulement si $Ker(f) = Ker(p)$.

Proposition 3.10.
Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Alors $kerf$ est un idéal.

Démonstration 3.14. *:*
Un morphisme d'anneaux est en particulier un morphisme de groupes abéliens. On sait donc que $Kerf$ est un sous groupe additif de A. De plus, si $x \in Kerf$ et si $a \in A$, alors on a $f(ax) = f(a)f(x) = f(a)0 = 0$. Ainsi $ax \in Kerf$ et $Kerf$ est donc bien un idéal.

Proposition 3.11.
Soit A un anneau et I un idéal de A. Pour tout morphisme d'anneaux $f : A \longrightarrow B$ s'annulant sur l'idéal I, il existe un unique morphisme d'anneaux $\tilde{f} : A/I \longrightarrow B$

Démonstration 3.15.
il existe un unique morphisme de groupes $\tilde{f}$,il est défini par : $\tilde{f}([a]) = f(a)$. Il est immédiat que $\tilde{f}$ est un morphisme d'anneaux.

Corollaire 5.
Tout homomorphisme d'anneaux $f : A \longrightarrow B$ se factorise par un isomorphisme d'anneaux $A/Kerf \longrightarrow f(A)$

3.4 Factorisation canonique d'une application linéaire

Définition 3.6.
Considérons E et F deux K-espaces vectoriels et f une application linéaire de E dans F, c'est-à-dire que :
pour tout x, y dans E et pour tout λ dans K on a :

$$f(\lambda x + y) = \lambda f(x) + f(y).$$

Définition 3.7.
La relation " x et y ont même image par f " définit une relation d'équivalence sur E, donnée par :

$$f(x) = f(y) \Leftrightarrow f(y - x) = 0 \Leftrightarrow y - x \in Kerf \Leftrightarrow y \in x + Kerf$$

i.e. la relation de congruence modulo $Kerf$ (au sens de la loi $+$).

Proposition 3.12.
On en déduit que l'ensemble quotient $\overline{E}$ est égal à $E/Kerf$. Pour munir ce dernier d'une structure d'espace vectoriel pour les lois quotients, il suffit de montrer que $Kerf$ est un sous-espace vectoriel de E.
Or,de montrer que ker f est stable par combinaisons linéaires.

Démonstration 3.16.
C'est immédiat, car pour tout x, y dans $Kerf$ et pour tout λ dans K, on a

$$f(\lambda x + y) = \lambda f(x) + f(y) = \lambda 0 + 0 = 0,$$

i.e. $\lambda x + y \in Kerf$, d'où $Kerf$ stable par combinaisons linéaires.

D'autre part,

Proposition 3.13.
On peut fait la décomposition canonique de f en applications linéaires $f = \iota \circ \overline{f} \circ \pi$.

Démonstration 3.17.
La bijection $\overline{f} : \begin{cases} E/Kerf \to Imf \\ \overline{x} \mapsto f(x) \end{cases}$ est linéaire puisque

$$\overline{f}(\lambda\overline{x} + \overline{y}) = \overline{f}(\overline{\lambda x + y}) = f(\lambda x + y) = \lambda f(x) + f(y) = \lambda\overline{f}(\overline{x}) + \overline{f}(\overline{y})$$

la projection canonique π est aussi linéaire (par construction des lois quotients), et idem pour l'injection canonique ι.
On a donc la décomposition canonique de f en applications linéaires $f = \iota \circ \overline{f} \circ \pi$.

Proposition 3.14.
On a le diagramme commutatif qui va avec

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ E/kerf & \xrightarrow{\overline{f}} & imf \end{array}$$

et l'isomorphisme d'espaces vectoriels

$$E/Kerf \simeq Imf.$$

Démonstration 3.18.
Si E est de dimension finie, on en déduit en particulier que Imf est de dimension finie et que

$$dimImf = dim(E/Kerf) = codimKerf,$$

d'où l'importantissime ***théorème du rang*** *:*

$$rgf + dimKerf = dimE.$$

Corollaire 6.
On retiendra de tout ceci trois choses :
- *si $f : E \to F$ est linéaire, alors le noyau $Kerf$ est un sous-espace vectoriel de E*
- *on a l'isomorphisme d'espaces vectoriels*

$$\begin{cases} E/Kerf \simeq Imf \\ \overline{x} \mapsto f(x) \end{cases}$$

- *si de plus E est de dimension finie alors*

$$rgf + dimKerf = dimE.$$

3.5 Factorisation canonique d'un morphisme d'algèbres unitaires

Considérons A et B deux K-algèbres unitaires et f un morphisme d'algèbres unitaires de A dans B, c'est-à-dire que pour tout a, b, c dans A et pour tout λ dans K on a :

$$f(\lambda a + bc) = \lambda f(a) + f(b)f(c)$$

et

$$f(1_A) = 1_B.$$

f est en particulier un morphisme d'anneaux unitaires, donc $Kerf$ est un idéal bilatère de A et on a l'isomorphisme d'anneaux unitaires

$$\overline{f} : \begin{cases} A/kerf \simeq Imf \\ \overline{a} \longmapsto f(a) \end{cases}$$

f étant par ailleurs une application linéaire, f est également un isomorphisme d'espaces vectoriels.

Conclusion 3.1.
Si $f : A \longrightarrow B$ est un morphisme d'algèbres unitaires, alors le noyau $Kerf$ est un idéal bilatère de A.
Et on a l'isomorphisme d'algèbres unitaires

$$\begin{cases} A/kerf \simeq Imf \\ \overline{a} \longmapsto f(a) \end{cases}$$

Conclusion

L'espace quotient d'une relation d'équivalence $\Re$ définie sur un ensemble X est ensemble $X/\Re$ des classes d'équivalence de la relation $\Re$.
Dans ce travail on a donnée les méthodes de construction d'une structure algébrique à partir de cette structure et on a vue que ce n'est pas toujours évident il faut qu'il possède des propriété particulière.
Ce travail permet d'après les théorèmes fondamental des factorisations et les théorèmes d'isomorphismes et quelque autre théorèmes de factoriser les morphismes qui sont triviale sur les sous structure.

Bibliographie

[1] A.Fontaine, *Leçon 103 exemples et applications des notions de sous-groupes distingués et de groupe quotient*, 21 décembre 2013.

[2] C.Bertault, *Une introduction aux quotients en mpsi.*

[3] D.Dos santos ferreira, *Espaces vectoriels quotient.*

[4] D.Perrin, *Cours d'algèbre*, Ellipses, 1996.

[5] F.Dumas, *Cours de licence mathématiques*, Université Blaise Pascal U.F.R. sciences et technologies département de mathématiques et informatique, 2007-2008.

[6] L.Bérlai et Christophe Hohlweg, *MAT2000 algèbre2* , 13 décembre 2011.

[7] M.Sage, *Introduction au espaces quotients*, 7 février 2005.

[8] P.Milan, *Morphismes de groupes*, 20 aout 2017.

[9] Y.Driencourt, *Résumé du cours d'algèbre générale l3 maths*, Printemps,2007.

[10] http ://www.maths-france.fr.

[11] http ://www.bibmath.net.

Résumé

Lorsque on passe au quotient on regroupe les éléments équivalent (pour une relation d'équivalence) pour une propriété qui s'intéresse puis on travail sur ces "regroupements" (sur l'ensemble quotient) avec une structure semblable à celle de l'ensemble initial.
L'objet de ce mémoire est étude les notion des espaces quotients et de donnée les théorème de factorisation.