© 2025 - Gérard Lavau - https://gerardlavau.fr
Vous avez toute liberté pour télécharger, imprimer, photocopier ce cours et le diffuser gratuitement. Toute diffusion à titre onéreux ou utilisation commerciale est interdite sans accord de l'auteur.
Si vous êtes le gestionnaire d'un site sur Internet, vous avez le droit de créer un lien de votre site vers mon site, à condition que ce lien soit accessible librement et gratuitement. Vous ne pouvez pas télécharger les fichiers de mon site pour les installer sur le vôtre.

GROUPES

PLAN

I : Propriétés usuelles

1- Loi de composition interne

a) Définition

Soit E un ensemble. On appelle **loi de composition interne** de E, notée par exemple $*$, une opération qui permet d'associer, à deux éléments quelconques de E a et b, un troisième élément noté $a * b$.

Exemples : Les lois de compositions internes les plus courantes sont :

+ dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.
– dans les mêmes ensembles.
× dans les mêmes ensembles.
/ dans $\mathbb{Q}^*$, $\mathbb{R}^*$, ou $\mathbb{C}^*$.
div (division entière) dans $\mathbb{N}^*$ ou $\mathbb{Z}^*$.
∘ dans l'ensemble des applications de E dans E.
∩ dans l'ensemble E = $\mathfrak{P}(\Omega)$ des parties d'un ensemble Ω.
∪ dans l'ensemble des parties d'un ensemble.

b) Associativité

Soit E *un ensemble muni d'une loi de composition interne notée* $*$. *Cette loi est dite* ***associative*** *si :*

$$\forall\, a \in \mathrm{E},\ \forall\, b \in \mathrm{E},\ \forall\, c \in \mathrm{E},\ (a * b) * c = a * (b * c)$$

L'intérêt d'une telle notion est que les parenthèse deviennent inutiles, la notation $a * b * c$ valant indifféremment l'une ou l'autre des expressions. Les lois suivantes, dans les ensembles du paragraphe précédent, sont associatives : +, ×, ∘, ∩, ∪. Les lois suivantes ne le sont pas : –, /, div.

On notera que l'absence de parenthèses dans l'écriture :

$$7 - 5 - 1 = 1$$

signifie implicitement qu'une convention est adoptée pour distinguer entre $(7 - 5) - 1$ et $7 - (5 - 1)$, la convention étant ici *que le calcul se fait de gauche à droite*, mais rien ne nous aurait empêché de prendre la convention inverse : faire les calculs de droite à gauche. Ce qui aurait conduit au résultat, qui nous paraît faux : $7 - 5 - 1 = 3$!!
Quant à la notation $a/b/c$, elle est à éviter, aucune convention n'ayant été définie à son sujet.

c) Commutativité

Soit E *un ensemble muni d'une loi de composition interne notée* $*$. *Cette loi est dite* ***commutative*** *si :*

$$\forall\, a \in \mathrm{E},\ \forall\, b \in \mathrm{E},\ a * b = b * a$$

L'intérêt d'une telle notion est que l'ordre dans lequel les éléments sont placés est indifférent. Les lois suivantes, dans les ensembles du paragraphe précédent, sont commutatives : +, ×, ∩, ∪. Les lois suivantes ne le sont pas : ∘ (sauf si les fonctions sont définies sur un ensemble possédant un seul élément), –, /, div.

Dans le cas d'une loi $*$ commutative et associative, l'expression suivante possède un sens :

$$\mathop{\Large *}_{i \in \mathrm{I}} x_i$$

où I est un ensemble fini d'indices. Par exemple, si $\mathrm{I} = \{1,...,n\}$, l'expression précédente est égale à $x_1 * x_2 * ... * x_n$, l'ordre des termes étant indifférent.

Exemples :

$\sum_{i=1}^{n} x_i$ désigne la somme des éléments x_i

$\prod_{i=1}^{n} x_i$ désigne le produit des éléments x_i

$\bigcap_{i \in \mathrm{I}} \mathrm{A}_i$ désigne l'intersection des parties A_i

$\bigcup_{i \in \mathrm{I}} \mathrm{A}_i$ désigne la réunion des parties A_i

On notera, que, si I et J sont deux ensembles disjoints d'indices, on a :

$$\mathop{\Large *}_{i \in \mathrm{I} \cup \mathrm{J}} x_i = \mathop{\Large *}_{i \in \mathrm{I}} x_i * \mathop{\Large *}_{i \in \mathrm{J}} x_i \qquad \text{(i)}$$

d) Elément neutre

Soit E *muni d'une loi interne* $*$. *On dit que e est* ***élément neutre*** *de la loi* $*$ *si :*

$$\forall\ a \in \mathrm{E},\ a * e = e * a = a$$

EXEMPLES :
Le neutre de + est 0. Celui de × est 1. Celui de ∘ est Id. Celui de ∩ est Ω (l'ensemble entier). Celui de ∪ est ∅. – et / n'ont pas d'éléments neutres. Si $*$ est associative, commutative, et admet un élément neutre *e*, alors la formule (i) nous conduit à poser :

$$\mathop{*}_{i \in \varnothing} x_i = e$$

Le neutre, s'il existe est unique. En effet, si *e* et *e*' sont deux neutres, on a :

$e * e' = e$ car e' est neutre

$e * e' = e'$ car e est neutre

donc $e = e'$.

e) Elément symétrique

Soit E *muni d'une loi* $*$, *et d'un élément neutre e. On appelle* ***symétrique*** *d'un élément x un élément x' tel que* :

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

Le neutre *e* est son propre symétrique puisque $e * e = e$. Si la loi est associative et si *x* admet un symétrique *x*' et *y* un symétrique *y*', alors $x * y$ admet pour symétrique $y' * x'$. En effet :

$$(x * y) * (y' * x') = x * (y * y') * x' = x * e * x' = x * x' = e$$

et de même :

$$(x' * y') * (y * x) = e$$

EXEMPLES :

Le symétrique de *x* pour + est $-x$ (appelé opposé de x).

Le symétrique de *x* non nul pour × est $\frac{1}{x}$ (appelé inverse de *x*)

Le symétrique de *f* bijective pour ∘ est f^{-1} (appelé réciproque)

Il n'y a en général pas de symétrique pour ∩ et ∪.

– et /, n'ayant aucune propriété particulière, apparaissent ici comme symétrisations des opérations + et ×. On ne les considère donc plus comme des lois.

Le symétrique, s'il existe, et si la loi est associative, est unique. En effet, si *x*' et *x*'' sont deux symétriques de *x*, alors on a :

$$x' * x * x'' = (x' * x) * x'' = e * x'' = x''$$
$$= x' * (x * x'') = x' * e = x'.$$

donc $x' = x''$. Ce symétrique est souvent noté x^{-1}.

EXERCICE : Si $*$ est associative, commutative, admet un élément neutre *e*, et si tout élément admet un symétrique, alors on a, avec I et J quelconques :

$$\ast_{i \in I \cup J} x_i = \ast_{i \in I} x_i * \ast_{i \in J} x_i * (\ast_{i \in I \cap J} x_i)^{-1}$$

2- Définition d'un groupe

Un ensemble (G,∗) *est un* ***groupe*** *si* :

i) G *est non vide*.
ii) ∗ *est une loi de composition interne*.
iii) ∗ *est associative*.
iv) ∗ *admet un élément neutre e*.
v) *tout x de e admet un symétrique x'*.

Si, en outre, ∗ est commutative, le groupe est dit **commutatif** ou **abélien** (Niels Abel, mathématicien norvégien, 1802 – 1829).

Les axiomes des groupes permettent de simplifier les équations. Ainsi :

$a * x = a * y \Rightarrow x = y$ (composer à gauche par le symétrique de a)
$x * a = y * a \Rightarrow x = y$ (composer à droite par le symétrique de a)

On note parfois la loi du groupe multiplicativement (ab au lieu de $a * b$) ou additivement ($a + b$ au lieu de $a * b$), mais la notation additive est réservée aux groupes commutatifs.
$a * a * ... * a$ est alors noté a^n dans le cas multiplicatif ou na dans le cas additif.
Le neutre est noté 1 en notation multiplicative et 0 en notation additive.
Le symétrique de a est noté a^{-1} en notation multiplicative et $-a$ en notation additive.

3- Exemples de groupes

On peut citer le groupe des complexes de module 1, le groupe des racines $n^{ème}$ complexes de l'unité, le groupe des similitudes directes du plan, le groupe symétrique. Voici d'autres exemples.

EXEMPLE 1 :
Voici quelques groupes à deux éléments :
❑ {σ,Id} où σ est une symétrie, muni de la loi ∘.
❑ U_2 = {+1,–1} muni du produit (groupe des racines carrées de l'unité, ou règle des signes).
❑ $\mathbb{Z}/2\mathbb{Z}$ = {0,1} muni de la loi +. Dans cet ensemble, on pose 1 + 1 = 0.
❑ $\mathfrak{S}_2$, groupe symétrique à deux éléments, muni de la loi ∘
❑ {Croissance, Decroissance} muni de la loi ∘, et de la règle donnant le sens de variation de la composée de deux fonctions monotones.
❑ {true,false} (en programmation), muni de la loi xor (ou exclusif).

Tous ces groupes sont en fait identiques au suivant :
Groupe à deux éléments {a,e}. La table de Pythagore de ce groupe est :

*	a	e
a	e	a
e	a	e

On a nécessairement $a^2 = e$ car si $a^2 = a$, en simplifiant par a, on obtient $a = e$.

La correspondance se fait de la façon suivante :

Groupe	$*$	a	e
$\{\sigma,Id\}$	$\circ$	σ	Id
$\{+1,-1\}$	$\times$	-1	$+1$
$\mathbb{Z}/2\mathbb{Z}$	$+$	1	0
{Croissance, Décroissance}	$\circ$	Decroissante	Croissante
{true,false}	xor	true	false

Tous ces groupes sont dits **isomorphes**. Un théorème démontré pour l'un d'entre eux l'est pour tous.

Par exemple : la valeur d'un produit en fonction de la parité du nombre de a est a si ce nombre est impair, e si ce nombre est pair. Ce résultat se traduit de la façon suivante dans quelques situations courantes :

$\sigma^{2p} = Id$ et $\sigma^{2p+1} = \sigma$ pour une symétrie σ

Le produit d'un nombre pair de termes négatifs est positif, le produit d'un nombre impair de termes négatifs est négatif.

La composée d'un nombre pair de fonctions décroissantes et d'un nombre quelconque de fonctions croissantes est croissante ; La composée d'un nombre impair de fonctions décroissantes et d'un nombre quelconque de fonctions croissantes est décroissante.

EXEMPLE 2 :

❑ L'exemple suivant n'est pas un groupe :

$*$	a	e
a	a	a
e	a	e

On trouve cependant cette situation dans les cas suivants :

$\{a, e\}$	$*$	a	e
$\mathbb{Z}/2\mathbb{Z}$	$\times$	0	1
{f paire, f impaire}	$\circ$	paire	impaire
{true, false}	or	true	false
{false, true}	and	false	true
$\{\Omega, \varnothing\}$	$\cap$	$\varnothing$	Ω
$\{\varnothing, \Omega\}$	$\cup$	Ω	$\varnothing$

Ici, a est dit **absorbant**. Il vérifie : $\forall\, x,\ x * a = a * x = a$.

EXEMPLE 3 : Groupes à trois éléments :

❑ Quels sont les groupes à trois éléments ?

Il n'y en a qu'un :

$*$	a	b	e
a	b	e	a
b	e	a	b
e	a	b	e

Pour le remplir, on remarque que, pour chaque élément y, l'application : $x \in G \rightarrow yx \in G$ est bijective. Chaque élément du groupe apparaît donc une fois et une seule dans chaque ligne y. De

même, l'application $x \to xy$ est bijective, donc chaque élément du groupe apparaît une fois et une seule dans chaque colonne y. En outre $ab = b$ est impossible car cela implique, en simplifiant par b, que $a = e$. De même $ab = a$ est impossible, donc $ab = e$, etc... Il est alors facile de compléter le tableau.

Tous les groupes à trois éléments sont donc isomorphes. En voici quelques exemples :

G	*	a	b	e
$U_3 = \{1, j, j^2\}$	×	j	j^2	1

où j est une racine cubique complexe de l'unité. U_3 est le groupe des racines cubiques de l'unité.

$\{1, \sigma, \sigma^2\}$	○	σ	σ^2	Id

où σ est une rotation de $2\pi/3$

$\mathbb{Z}/3\mathbb{Z}$	+	1	2	0

constitué des éléments {0,1,2} où le calcul se fait modulo 3

$\mathfrak{A}_3$	○	(1 2 3)	(1 3 2)	Id

groupe dit alterné des permutations paires de trois éléments

EXEMPLE 4 :

❑ Quels sont les groupes à 4 éléments ?

On n'en trouve que deux :

*	a	b	c	e
a	e	c	b	a
b	c	a	e	b
c	b	e	a	c
e	a	b	c	e

*	a	b	c	e
a	e	c	b	a
b	c	e	a	b
c	b	a	e	c
e	a	b	c	e

Le premier n'est autre que $(\mathbb{Z}/4\mathbb{Z}, +)$, c'est à dire le groupe des éléments {0,1,2,3} où les calculs se font modulo 4, ou bien le groupe $(U_4, \times)$ des racines quatrièmes de l'unité dans $\mathbb{C}$, selon la correspondance suivante :

G	*	c	a	b	e
$\mathbb{Z}/4\mathbb{Z}$	+	i	–1	$-i$	1
U_4	×	1	2	3	0

Le second est $(\mathbb{Z}/2\mathbb{Z})^2$, où les calculs se font modulo 2 sur chaque composante du couple :

G	*	a	b	c	e
$(\mathbb{Z}/4\mathbb{Z})$	+	(1,0)	(0,1)	(1,1)	(0,0)

Ce dernier groupe se trouve également dans la situation suivante : considérons un matelas. Il peut être laissé dans la position initiale (Id). On peut le tourner dans le sens de la longueur (σ). On peut le tourner dans le sens de la largeur (θ). On peut lui faire un demi–tour à plat (φ). {Id, σ, θ, φ} n'est autre que le second groupe.

EXEMPLE 5 :
Voici des groupes à n éléments :
❑ U_n groupe des racines $n^{ème}$ de l'unité dans $\mathbb{C}$, muni du produit
❑ $\mathbb{Z}/n\mathbb{Z}$ = {0, 1, 2, ..., n–1} où les calculs se font modulo n. Plus précisément, $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble quotient de $\mathbb{Z}$ par la relation d'équivalence de congruence modulo n :

$$x \equiv y \bmod n \Leftrightarrow \exists\, p \in \mathbb{Z},\ x - y = pn \Leftrightarrow \exists\, p \in \mathbb{Z},\ p \mid x - y$$

On définit sur $\mathbb{Z}/n\mathbb{Z}$ une addition de la façon suivante. Soient $C(x)$ et $C(y)$ deux classes. On pose : $C(x) + C(y) = C(x + y)$. Il faut réaliser que la valeur trouvée dépend a priori du choix fait de x et de y dans chacune des classes. Il est nécessaire de montrer que cette valeur ne dépend que des classes, et non des représentants x et y de chaque classe.

$$\begin{cases} C(x) = C(x') \\ C(y) = C(y') \end{cases} \Leftrightarrow \begin{cases} x \equiv x' \\ y \equiv y' \end{cases} \Rightarrow x + y \equiv x' + y' \Rightarrow C(x + y) = C(x' + y')$$

La possibilité d'une addition repose donc sur la compatibilité de la loi + dans $\mathbb{Z}$ avec la relation de congruence.

On vérifie facilement que la loi ainsi définie confère à ($\mathbb{Z}/n\mathbb{Z}$, +) une structure de groupe commutatif. L'élément neutre est $C(0)$, le symétrique de $C(p)$ est $C(–p) = C(n – p)$. Ce groupe est dit **cyclique**, engendré par $C(1)$.

EXEMPLE 6 :
❑ Voici un exemple d'**isomorphisme** entre deux groupes, c'est-à-dire d'application bijective compatible avec les lois de chaque groupe :

$$(\mathbb{R},+) \to (\mathbb{R}^{+}*,\times)$$
$$x \to e^{x}$$

La compatibilité entre les lois s'exprime par le fait que : $\forall\ (x, y) \in \mathbb{R}^2$, $e^{x+y} = e^x \times e^y$. Cet isomorphisme intervient dans le choix d'échelles logarithmiques, pour exemple pour la mesure du bruit, ou celle des mouvements telluriques.

EXEMPLE 7 :
❑ l'ensemble $\mathfrak{S}_n$ des permutations d'un ensemble à n éléments muni de la composée des applications forme un groupe appelé **groupe symétrique** (voir L1/GROUPSYM.PDF).

Soit G un groupe fini constitué de n élements. Pour tout a de G, considérons l'application σ_a de G dans G, qui à x associe ax. Cette application est bijective, sa réciproque étant $\sigma_{a'}$ où a' est le symétrique de a dans le groupe G. σ_a est donc une permutation de G. En outre, on a :

$$\sigma_a \circ \sigma_b = \sigma_{ab} \qquad \text{(i)}$$

On a donc l'association :

$$(G, *) \to (\mathfrak{S}_G, \circ)$$
$$a \to \sigma_a$$

qui définit une application Φ, qualifiée de **morphisme** du fait de la relation (i) qui fait correspondre le produit $\circ$ dans $\mathfrak{S}_G$ à la loi de composition $*$ dans G. Φ est injective. En effet :

$\sigma_a = \sigma_b \Rightarrow \sigma_a(e) = \sigma_b(e) \Rightarrow a = b$

Φ est surjective sur $\Phi(G) = \{\sigma_a \mid a \in G\}$. $(\Phi(G), \circ)$ est un sous-groupe de $\mathfrak{S}_G$, et l'on a montré que tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique.

EXEMPLE 8 :

❑ Si on dispose de deux groupes G et H dont on notera la loi multiplicativement, alors $G \times H$ est un groupe dit **groupe produit** de G et H au moyen de la loi suivante :

$(a, b) * (c, d) = (ac, bd)$

le neutre est (e_G, e_H)

le symétrique de (a, b) est (a^{-1}, b^{-1})

II : Sous-groupes et morphismes de groupes

1- Sous-groupe

Soit (G,$*$) *un groupe et* G' *une partie de* G. *On dit que* G' *est un* **sous-groupe** *de* G *si, muni de la loi* $*$, (G',$*$) *est un groupe.*

Il suffit de vérifier les propriétés suivantes :

- ❑ G' est non vide
- ❑ G' est stable pour $*$ (ce qui signifie que $*$ est une loi interne à G') :

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

- ❑ G' est stable par passage au symétrique : $\forall x \in G', x^{-1} \in G'$

Il est inutile de vérifier que G' dispose d'un élément neutre. En effet, si e est le neutre de G, on montre que e est également neutre de G'. En effet :

G' est non vide, donc il existe x élément de G'

$x \in G'$ donc $x^{-1} \in G'$

$x \in G'$ et $x^{-1} \in G'$ donc $x * x^{-1} \in G'$ donc $e \in G'$

$\forall x \in G, e * x = x * e = x$ donc ceci reste vrai a fortiori pour x dans G'

On peut également condenser les deux dernières propriétés en une seule :

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

En effet, en prenant $x = y$, on en déduira que $e \in G'$, puis en prenant $x = e$, on en déduit que $y \in G' \Rightarrow y^{-1} \in G'$, et enfin, en prenant x et y^{-1}, on en déduira que $xy = x(y^{-1})^{-1} \in G'$.

L'associativité étant vraie dans G est a fortiori vraie dans G'. Il en est de même de l'éventuelle commutativité.

PROPOSITION

L'intersection de deux ou plusieurs sous-groupes est lui-même un sous-groupe.

Démonstration :

Soit $(G_i)_{i \in I}$ une famille de sous-groupes de G. Alors :

$\bigcap_{i\in I} G_i$ est non vide puisqu'il contient le neutre e, ce dernier appartenant à chacun des sous-groupes G_i.

Si x et y appartiennent à $\bigcap_{i\in I} G_i$, alors pour tout i, x et y appartiennent à G_i, donc xy^{-1} aussi, donc xy^{-1} appartient à $\bigcap_{i\in I} G_i$.

2- Exemples de sous-groupes

EXEMPLE 1 : Le groupe alterné $\mathfrak{A}_n$ des permutations paires est un sous-groupe du groupe symétrique $\mathfrak{S}_n$ (voir le chapitre GROUPESYM.PDF dans le cours de L1)

EXEMPLE 2 : Dans le plan $\mathbb{R}^2$, considérons les applications qui au vecteur (x,y) associe le vecteur $(x',y') = (ax + by, cx + dy)$, avec $ad - bc \neq 0$, ce qu'on note :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

L'ensemble de ces applications, muni de la loi de composition $\circ$, forme un groupe appelé groupe linéaire.
L'ensemble des applications pour lesquelles $ad - bc = \pm 1$ en forme un sous-groupe.
L'ensemble des applications orthogonales (rotations et symétries) forme un sous-groupe de ce sous-groupe appelé groupe orthogonal.
L'ensemble des rotations forme lui–même un sous-groupe du groupe orthogonal.

EXEMPLE 3 : l'ensemble des nombres pairs forme un sous-groupe de $(\mathbb{Z},+)$.

3- Morphismes, Exemples

Soit $(G,*)$ *et* $(G',\#)$ *deux groupes. On appelle* **morphisme** *(respectivement* **isomorphisme***) de* G *dans* G' *toute application f (respectivement toute application bijective) vérifiant :*

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

Si f est un isomorphisme, sa réciproque f^{-1} aussi. En effet, soit u et v éléments de G', images par f de x et de y. On a :

$f(x * y) = f(x)\ \#\ f(y)$
donc $f(x * y) = u\ \#\ v$
donc $x * y = f^{-1}(u\ \#\ v)$
donc $f^{-1}(u) * f^{-1}(v) = f^{-1}(u\ \#\ v)$
et on a montré que f^{-1} était un morphisme. Etant bijectif, c'est un isomorphisme.

Un isomorphisme de G dans G s'appelle un **automorphisme**. On pourra vérifier que l'ensemble des automorphismes de G constitue un groupe avec la composée des applications, de neutre l'application identique.

EXEMPLE 1 :
❑ L'application du groupe symétrique $(\mathfrak{S}_n, \circ)$ dans $(\{-1,1\},\times)$ qui, à chaque permutation σ associe sa signature $\varepsilon(\sigma)$ est un morphisme.

EXEMPLE 2 :

❑ L'application du groupe linéaire $GL_n(\mathbb{R})$ dans $\mathbb{R}^*$ qui à toute matrice M associe son déterminant det(M) est un morphisme.

D'autres exemples ont été vus dans le paragraphe I-3). L'intérêt d'un isomorphisme est que deux groupes isomorphes sont indiscernables en ce qui concerne leurs propriétés. On les discerne seulement par le *sens* que l'on donne aux éléments du groupe.

EXEMPLE 3 :

❑ $\mathbb{Z}/n\mathbb{Z}$ et le groupe U_n des racines $n^{èmes}$ complexes de 1 sont isomorphes. Il suffit de considérer l'application suivante :

$$\mathbb{Z}/n\mathbb{Z} \to U_n$$
$$p \quad \to \exp(\frac{2ip\pi}{n})$$

p étant défini modulo n, il convient de vérifier que son image ne dépend pas du représentant choisi, ce qui est bien le cas, puisque si, $p \equiv p'$ mod n, on a $\exp(\frac{2ip\pi}{n}) = \exp(\frac{2ip'\pi}{n})$. Autrement dit, l'application est bien définie de $\mathbb{Z}/n\mathbb{Z}$ dans U_n et pas seulement de $\mathbb{Z}$ dans U_n. Il est facile ensuite de vérifier que l'application est bijective et qu'il s'agit d'un morphisme.

EXEMPLE 4 :

❑ On considère $\mathbb{C}^* \times \mathbb{C}$, muni de la même loi suivante :

$$(a, b) * (a', b') = (aa', ab' + b)$$

Il s'agit bien d'une loi interne, associative car :

$$\begin{aligned}((a, b) * (a', b')) * (a'', b'') &= (aa', ab' + b) * (a'', b'') \\ &= (aa'a'', aa'b'' + ab' + b) \\ &= (a, b) * (a'a'', a'b'' + b') \\ &= (a, b) * ((a', b') * (a'', b''))\end{aligned}$$

Le neutre est (1, 0) et le symétrique de (a, b) est $(\frac{1}{a}, -\frac{b}{a})$

Ce groupe est isomorphe au sous-groupe de $GL_2(\mathbb{C})$ (voir L1/MATRICES.PDF) constitué des matrices de la forme $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, au moyen de l'isomorphisme $(a, b) \to \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. La loi $*$ dans $\mathbb{C}^* \times \mathbb{C}$ correspond en effet au produit de matrices puisque :

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab' + b \\ 0 & 1 \end{pmatrix}$$

Il est aussi isomorphe au groupe des similitudes directes du plan complexe muni de la composition des applications, une similitude directe étant une application de la forme $z \to az + b$ avec a et b complexes, a non nul (voir L1/COMPLEXE.PDF). La composée de $z \to a'z + b'$ par $z \to az + b$ donne l'application :

$$z \to a(a'z + b') + b = aa'z + ab' + b$$

et on reconnaît dans les coefficients la loi du groupe.

L'ensemble $\mathbb{R}^* \times \mathbb{C}$ forme un sous-groupe de $\mathbb{C}^* \times \mathbb{C}$. Il est isomorphe au groupe des matrices inversibles de la forme $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ à diagonale réelle et il est isomorphe au sous-groupe des similitudes constitué des homothéties et des translations (voir L1/GEOMAFF.PDF).

EXEMPLE 5 :
❑ Soit E un espace vectoriel, vu également comme espace affine. (Voir L1/GEOMAFF.PDF). Soit GA(E) le groupe affine de E et GL(E) le groupe linéaire de E. L'application $f \in GA(E) \to \Phi \in GL(E)$ où Φ est l'application linéaire associée à l'application affine f, est un morphisme de groupes.

4- Propriétés des morphismes
On pourra vérifier les propriétés suivantes sur les exemples de morphismes vus au II-3) et au I-3).

Soit $f : G \to G'$ un morphisme de groupes.

a) Si e est le neutre de G, alors $f(e)$ est le neutre de G'. En effet, si e' est le neutre de G' :
$f(e) = f(e * e) = f(e) \# f(e)$ et d'autre part, $f(e) = f(e) \# e'$
donc $f(e) \# f(e) = f(e) \# e'$, et en composant à gauche par $f(e)^{-1}$, on obtient $f(e) = e'$

b) $\forall x \in G$, $f(x^{-1}) = f(x)^{-1}$.
En effet $f(x^{-1}) \# f(x) = f(x^{-1} * x) = f(e) = e'$ et de même $f(x) \# f(x^{-1}) = e'$.

PROPOSITION
On appelle ***noyau*** *de f l'ensemble* $\mathrm{Ker}(f) = \{x \mid f(x) = e'\}$. *Alors* :
i) $\mathrm{Ker}(f)$ *est un sous-groupe de* G.
ii) *f est injective si et seulement si* $\mathrm{Ker}(f) = \{e\}$.

Démonstration :
i) $\mathrm{Ker}(f)$ est non vide puisqu'il contient e. Si x et y appartiennent à $\mathrm{Ker}(f)$, alors :
$f(xy^{-1}) = f(x) \# f(y)^{-1} = e' \# e' = e'$
donc xy^{-1} appartient à $\mathrm{Ker}(f)$.

ii) Si f est injective, alors e' a au plus un antécédent. Or e est un antécédent de e'. Donc $\mathrm{Ker}(f) = \{e\}$.
Réciproquement, si $\mathrm{Ker}\, f = \{e\}$, alors :
$f(x) = f(y)$
$\Rightarrow$ $f(x) \# f(y)^{-1} = e'$
$\Rightarrow$ $f(x) \# f(y^{-1}) = e'$
$\Rightarrow$ $f(x * y^{-1}) = e'$
$\Rightarrow$ $x * y^{-1} \in \mathrm{Ker}(f)$
$\Rightarrow$ $x * y^{-1} = e$ d'après l'hypothèse
$\Rightarrow$ $x = y$
et f est bien injective

PROPOSITION
On appelle ***image*** *de f l'ensemble* $\mathrm{Im}(f) = \{y \mid \exists\, x, f(x) = y\}$. *Alors* :
i) $\mathrm{Im}(f)$ *est un sous-groupe de* G'.

ii) *f est surjective si et seulement si* Im(*f*) = G'.

Démonstration :
i) Im(*f*) est non vide puisqu'il contient *e'* = *f*(*e*). Si *x* et *y* appartiennent à Im(*f*), alors il existe *u* et *v* élements de E tels que *x* = *f*(*u*) et *y* = *f*(*v*), donc :

$x \# y = f(u) \# f(v) = f(u * v) \in \mathrm{Im}(f)$

De même, $x^{-1} = f(u)^{-1} = f(u^{-1}) \in \mathrm{Im}(f)$

ii) est évident.

EXEMPLE 1 :
❑ Le noyau de l'application $\sigma \in (\mathfrak{S}_n, \circ) \to \varepsilon(\sigma) \in (\{-1,1\},\times)$ est le groupe alterné.

EXEMPLE 2 :
❑ Le noyau de l'application $M \in GL_n(\mathbb{R}) \to \det(M) \in \mathbb{R}^*$ est le groupe $SL_n(\mathbb{R})$.

EXEMPLE 3 :
❑ Le noyau de l'application $f \in GA(E) \to \Phi \in GL(E)$ où Φ est l'application linéaire associée à l'application affine *f*, est le groupe des translations de E.

5- Sous-groupes engendrés par une partie

PROPOSITION
Soit G *un groupe* (*on notera sa loi multiplicativement*) *et* M *une partie de* G. *Soit* G' *l'ensemble des produits de la forme* $x_1...x_n$, $n \in \mathbb{N}$, avec $x_i \in M$ *ou* $x_i^{-1} \in M$. *Alors*

i) G' *est un sous-groupe de* G

ii) *Si* F *est un sous-groupe de* G *contenant* M, *alors* G' *est inclus dans* F. G' *est donc le plus petit sous-groupe de* G *contenant* M.

iii) G' *est égal à l'intersection de tous les sous-groupes contenant* M.

Démonstration :
i) Le produit vide (pour $n = 0$) est égal au neutre *e* de G, donc *e* appartient à G'. Si *x* et *y* appartiennent à G', alors il existe des $(x_i)_{1\le i\le n}$ et des $(y_j)_{1\le j\le m}$ éléments de M ou dont les inverses appartiennent à M tels que $x = x_1...x_n$ et $y = y_1...y_m$. Comme $xy = x_1...x_n y_1...y_m$ et $x^{-1} = x_n^{-1}...x_1^{-1}$, *xy* et x^{-1} sont bien de la forme voulue pour appartenir à G'. Donc G' est un sous-groupe de G

ii) Soit F un sous-groupe contenant M et *x* un élément de G'. Il existe $(x_i)_{1\le i\le n}$ éléments de M ou dont les inverses appartiennent à M tels que $x = x_1...x_n$. Par conséquent les x_i appartiennent à F et leur produit aussi, donc *x* appartient à F. Ainsi G' est inclus dans F.

iii) L'intersection de tous les sous-groupes contenant M est un sous-groupe F (comme intersection d'une famille de sous-groupes) contenant M (puisque chacun des sous-groupes considéré contient M). Donc G' est inclus dans F. Mais G' lui-même est un sous-groupe contenant M donc fait partie de la famille dont on prend l'intersection. G' contient donc cette intersection F et F est inclus dans G'.

On dit que G' est **engendré** par M ou que M est un **système de générateurs** de G'.

EXEMPLE 1 :

❑ Le groupe symétrique $\mathfrak{S}_n$ est engendré par l'ensemble des transpositions.

EXEMPLE 2 :
❑ $\mathbb{Z}$ est engendré par {1}.

EXEMPLE 3 :
❑ $\mathbb{Z}/n\mathbb{Z}$ est engendré par {1}

6- Groupes monogènes et groupes cycliques

On appelle groupe **monogène** un groupe G engendré par un seul élément *a*. Les éléments du groupe sont donc de la forme a^n, *n* élement de $\mathbb{Z}$ si la loi est notée multiplicativement, ou *na* si elle est notée additivement.

En notation multiplicative, on dispose des règles de calcul suivantes :

$a^n \times a^m = a^{n+m}$ pour *n* et *m* éléments de $\mathbb{N}$

$(a^{-1})^n = (a^n)^{-1}$. On notera cette quantité a^{-n}. Dans ce cas, la relation précédente est vraie pour *n* et *m* éléments de $\mathbb{Z}$. On a également :

$(a^n)^m = a^{nm}$ pour *n* et *m* éléments de $\mathbb{Z}$.

L'application de $(\mathbb{Z},+)$ dans G qui à *n* associe a^n est donc un morphisme de groupes surjectif. Il y a alors deux cas :

❑ Ce morphisme est aussi injectif, ce qui signifie que :

$\forall\, n \in \mathbb{Z}^*,\ a^n \neq e$

ou encore $\forall\, n \in \mathbb{Z},\ \forall\, m \in \mathbb{Z},\ n \neq m \Rightarrow a^n \neq a^m$

Dans ce cas, G est infini et isomorphe à $\mathbb{Z}$.

❑ Ce morphisme n'est pas injectif. Dans ce cas, il existe *n* non nul tel que $a^n = e$. On peut supposer $n > 0$ car si $a^n = e$, on a aussi $a^{-n} = e$. Soit *n* le plus petit entier strictement positif vérifiant cette relation. Nous allons prouver que G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Soit $\Phi : \mathbb{Z}/n\mathbb{Z} \to G$

$m \quad \to a^m$

m est en fait défini modulo *n*. a^m est cependant parfaitement défini sans ambiguïté car $a^{m+kn} = a^m(a^n)^k = a^m e^k = a^m$. Φ est donc bien une application de $\mathbb{Z}/n\mathbb{Z}$ sur G.

Φ est un morphisme.

Φ est injective. En effet, soit *m* un entier tel que $a^m = e$. Divisons *m* par *n*. On a $m = qn + r$ avec $0 \leq r < n$. Donc $e = a^m = a^{mn+r} = a^r$. Or, par définition de *n*, $a^r = e$ donc $r = 0$ puisque *n* est le plus petit entier strictement positif tel que $a^n = e$, que $0 \leq r < n$ et que $a^r = e$. Donc $m = qn \equiv 0 \bmod n$ et $\mathrm{Ker}(\Phi) = \{0\}$.

Φ est surjective par hypothèse.

En particulier, G est constitué de *n* éléments. $G = \{e, a, a^2, ..., a^{n-1}\}$. Un groupe monogène de cardinal fini *n* est dit groupe **cyclique** d'ordre *n*. Son élément générateur *a* est un **élément d'ordre** *n*.

Les groupes monogènes sont donc tous isomorphes à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$.

Un sous-groupe H d'un groupe monogène G est lui-même monogène. En effet, soit a générateur de G, et soit p la plus petite puissance strictement positive telle que a^p soit élément de H. Alors a^p est générateur de H. En effet, soit a^m élément de H. Effectuons la division euclidienne de m par p :

$\exists\ (q, r),\ m = pq + r$ avec $0 \leq r < p$.

On a alors $a^r = a^{m-pq} = a^m(a^p)^{-q}$ élément de H. Or $0 \leq r < p$ et p est la plus petite puissance strictement positive telle que a^p soit élément de H. Donc $r = 0$ et $a^m = a^{pq}$ est une puissance de a^p.
Si G possède n éléments, p est nécessairement un diviseur de n, car $a^n = e$ est élément de H.
Si on pose k tel que $n = kp$, les éléments de H sont alors $\{e, a^p, a^{2p}, ..., a^{(k-1)p}\}$. Puis $a^{kp} = a^n = e$. Le nombre d'éléments de H est donc $k = \frac{n}{p}$. Les éléments précédemment cités de H sont bien distincts, car si on avait $0 \leq i < j \leq k - 1$ tels que $a^{ip} = a^{jp}$ alors $a^{(j-i)p} = e$ avec $0 < (j - i)p \leq (k - 1)p < n$, en contradiction avec le fait que n est le plus petit entier strictement positif tel que $a^n = e$.

7- Groupes finis

Soit G un groupe fini. Le nombre d'éléments de G s'appelle l'**ordre du groupe** et est noté Card(G) ou $|G|$. On appelle également **ordre d'un élément** l'ordre du sous-groupe engendré par cet élément.

Dans la recherche sur la classification des groupes finis dits simples, on a mis en évidence des groupes dit sporadiques. L'un d'eux est un groupe d'ordre

$$2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$$
$$= 808017424794512875886459904961710757005754368000000000$$

Ce groupe s'appelle *Le Monstre*. Le premier groupe simple sporadique, découvert en 1861, est le groupe de Mathieu M_{11}, composé de 7920 éléments. Il s'agit du sous-groupe de $\mathfrak{S}_{11}$, engendré par les permutations (1 2 3 4 5 ... 10 11) et (5 6 4 10)(11 8 3 7).

THEOREME DE LAGRANGE :
Soit H *un sous-groupe de* G. *Alors, l'ordre de* H *divise l'ordre de* G.

Pour tout x élément de G, on note $xH = \{xy \mid y \in H\}$. L'application qui à $y \in H$ associe $z = xy \in xH$ est une bijection de réciproque $z \to y = x^{-1}z$, donc xH et H ont même nombre d'éléments. La relation binaire définie par :

$$x\ \mathcal{R}\ x' \Leftrightarrow xH = x'H$$

est une relation d'équivalence. Montrons que la classe d'équivalence de x est précisément xH. Il faut donc montrer l'équivalence entre :

i) $xH = x'H$ ($x\ \mathcal{R}\ x'$)

ii) $x' \in xH$ (x' appartient à la classe de x)

Supposons i). x' est élément de $x'H$, puisque $x' = x'e$ et que e est élément de H. Comme $x'H = xH$, on en déduit que x' est élément de xH.
Supposons ii). Il existe h élément de H tel que $x' = xh$. Comme $x'H$ est l'ensemble des éléments de la forme $x'y$, $y \in H$, il est également de la forme xhy, avec y et h et donc yh éléments de H. Ce sont donc des éléments de xH. Ainsi $x'H$ est inclus dans xH. Inversement, xH est l'ensemble des éléments de la forme xy, $y \in H$, donc de la forme $x'h^{-1}y$. Ces éléments sont bien dans $x'H$ car $h^{-1}y$ est élément de H. Ainsi, $xH = x'H$.

Les parties xH, étant des classes d'équivalence, forment une partition de G, et toutes ces parties ont même nombre d'éléments. On a donc :

Card(G) = Card(H) × NbreCl où NbreCl désigne le nombre de classes d'équivalence.

et Card(H) divise Card(G).

CONSEQUENCES :

❑ L'ordre d d'un élément x divise l'ordre du groupe. On prend pour H le sous-groupe $\{e, x, ..., x^{d-1}\}$.

❑ La propriété précédente peut également s'exprimer sous la forme :

$\forall\, x \in G, x^n = e$ où $n = |G|$

En effet, si d est l'ordre de x et si k est tel que $n = kd$, alors $x^n = x^{kd} = (x^d)^k = e^k = e$. Cette dernière relation peut se montrer directement dans un groupe commutatif en constatant que, pour x donné, l'application $y \in G \to xy \in G$ est bijective et donc que :

$$\prod_{y\in G} y = \prod_{y\in G} xy = \prod_{y\in G} x \prod_{y\in G} y = x^n \prod_{y\in G} y$$

et on simplifie par $\prod_{y\in G} y$.

❑ Si G est un groupe d'ordre un nombre premier, alors G est cyclique et engendré par n'importe lequel de ses éléments différents de e.

En effet, soit a un tel élément et $H = \{a^n \mid n \in \mathbb{Z}\}$. H est un sous-groupe de G comportant au moins deux éléments (a et e). Card(H) divise Card(G), Card(G) est premier et Card(H) est supérieur ou égal à 2, donc Card(H) = Card(G) donc H = G.

Ainsi, il n'existe qu'un seul groupe à 3, 5, 7, 11 éléments, ce sont $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/11\mathbb{Z}$.

❑ On peut montrer que tout groupe commutatif fini est produit de groupes cycliques. Les groupes finis non commutatifs sont, quant à eux, beaucoup plus difficiles à décrire.

Annexe : Un peu de littérature

Nous conclurons ce chapitre par un extrait du roman de Georges Perec, *La disparition*. Ce roman est entièrement rédigé sans comporter une seule fois la lettre *e*. L'humour de l'extrait ci-dessous ne peut être pleinement apprécié que par ceux qui ont suivi un cours sur les groupes ☺ :

> On groups.
> (Traduction d'un travail dû à Marshall Hall jr L.I.T. 28, folios 5 à 18 inclus).
> La notion-là, qui la conquit, qui la trouva, qui la fournit ? Gauss ou Galois ? L'on n'a jamais su. Aujourd'hui, tout un chacun connaît ça. Pourtant, on dit qu'au fin fond du noir, avant sa mort, dans la nuit, Galois grava sur son pad (Marshall Hall jr, op. cit. fol. 8) un long chaînon à sa façon. Voici :
> $aa^{-1} = bb^{-1} = cc^{-1} = dd^{-1} = ff^{-1} = gg^{-1} = hh^{-1} = ii^{-1} = jj^{-1} = kk^{-1} = ll^{-1} = mm^{-1} = nn^{-1} = oo^{-1} = pp^{-1} = qq^{-1} = rr^{-1} = ss^{-1} = tt^{-1} = uu^{-1} = vv^{-1} = ww^{-1} = xx^{-1} = yy^{-1} = zz^{-1} =$
> Mais nul n'a jamais pu savoir la conclusion à quoi Galois comptait aboutir dans son manuscrit non fini.
> Cantor, Douady, Bourbaki, ont cru, par un, par dix biais (du corps parfait aux topos, du local ring aux C^{star}, du K-functor qu'on doit à Shih aux ❑ du grand

Thom, n'oubliant ni distributions, ni involutions, ni convolutions, Schwartz ni Koszul ni Cartan ni Giorgiutti) saisir un vrai fil sûr pour franchir l'abrupt hiatus. Tout fut vain.
Pontryagin y passa vingt ans, finissant par n'y plus voir du tout.
Or voici qu'il y a huit mois Kan, travaillant sur un adjoint à lui (voir D. Kan Adjoint Functors Transactions, V, 3, 18) montra par induction, croit-on, (il raisonnait – a-t-il dit à Jaulin – sur un grand cardinal, par "forcing" pour part) la Proposition Soit G soit H soit K ($H \subset G$, $K \subset G$) trois magmas (nous suivons Kuroch) où l'on a $a(bc) = (ab)c$; où, pour tout a, $x \to xa$, $x \to xa$ sont surs, sont monos, alors on a $G \approx H \times K$, si $G = H \cup K$; si H, si K sont invariants ; si H, K n'ont qu'un individu commun $H \cap K =$ Las ! Kan mourut avant d'avoir fini son job. Donc, à la fin, l'on n'a toujours pas la solution.

Exercices

1- Enoncés

Exo.1) On considère l'ensemble $G = \{(a, b) \in \mathbb{R}^2 \mid b^2 - ab - a^2 \neq 0\}$. On définit sur G une loi :

$$(a, b) * (c, d) = (ad + bc - ac, ac + bd)$$

a) Montrer que $(G, *)$ est un groupe.

b) Calculer $(1,1)^{*n}$ pour tout entier n strictement positif, (où $*^n$ signifie qu'on itère n fois le produit $*$).

c) Montrer que l'application $N : (a, b) \in G \to b^2 - ab - a^2$ est un morphisme du groupe $(G, *)$ dans le groupe $(\mathbb{R}^*, \times)$.

Exo.2) Soit (G, +) est un groupe fini commutatif de neutre noté 0, x un élément de G d'ordre n, y un élément de G d'ordre m. Montrer que, si n et m sont premiers entre eux, alors $x + y$ a pour ordre nm.

Exo.3) Soit G un groupe dont la loi est notée multiplicativement, engendré par deux éléments a et b distincts, différents de l'élément neutre e. On suppose que $a^2 = b^2 = (ab)^2 = e$. Montrer que G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exo.4) Soit G un groupe de neutre e dont la loi est notée multiplicativement. On suppose que G possède 8 éléments, et que, pour tout a de G, $a^2 = e$. Montrer que G est isomorphe à $((\mathbb{Z}/2\mathbb{Z})^3, +)$.

Exo.5) Soit $SO_n(\mathbb{R})$ le groupe des isométries directes de $\mathbb{R}^n$, et soit r une réflexion par rapport à un hyperplan donné. r enhendre un sous-groupe H de $O_n(\mathbb{R})$. On note multiplicativement la composée des isométries. Soit G l'ensemble $SO_n(\mathbb{R}) \times H$ muni de la loi :

$$\forall\, u \in SO_n(\mathbb{R}),\ \forall\, v \in SO_n(\mathbb{R}),\ \forall\, m \in \mathbb{Z},\ \forall\, p \in \mathbb{Z},\ (u, r^m) * (v, r^p) = (ur^m v r^m, r^{m+p})$$

a) Montrer que G est un groupe.

b) Montrer qu'il est isomorphe à $O_n(\mathbb{R})$, groupe des isométries de $\mathbb{R}^n$.

Exo.6) Déterminer tous les groupes d'ordre 9.

Exo.7) Soit $f : F \to G$ un morphisme de groupes.

a) Montrer que, pour tout sous-groupe H de F, f(H) est un sous-groupe de G.

b) Montrer que, pour tout sous-groupe K de G, $f^{-1}(K)$ est un sous-groupe de F.

Exo.8) Soient G et G' des groupes finis, f un morphisme de G dans G', H un sous-groupe de G, g : H $\rightarrow$ G' la restriction de f à H.

a) Montrer que Card(G) = Card(Im(f)) Card(Ker(f))

b) Montrer que : $\dfrac{\text{Card(G)}}{\text{Card(H)}} = \dfrac{\text{Card(Im}(f))}{\text{Card(Im}(g))} \dfrac{\text{Card(Ker}(f))}{\text{Card(Ker}(g))}$

Exo.9) Pour tous entiers n et m supérieurs ou égaux à 2 et tels que m divise n, on note f_{mn} l'application de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ définie par :

$$\forall\ x \in \mathbb{Z}/m\mathbb{Z},\ f_{mn}(x) = \frac{n}{m}\,x$$

a) Montrer que f_{mn} est bien définie, et est un morphisme de groupes additifs.

On note $\mathbb{Q}/\mathbb{Z}$ le groupe additif où les opérations sont menées modulo 1. Ainsi, dans ce groupe :

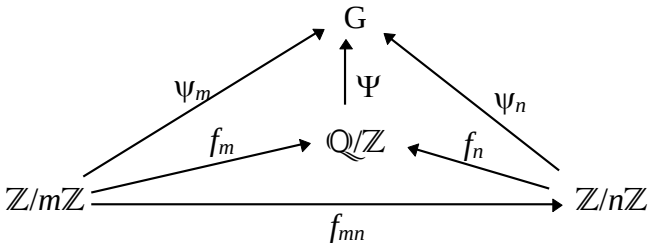
$$\frac{3}{5} + \frac{2}{3} = \frac{19}{15} = 1 + \frac{4}{15} = \frac{4}{15}$$

Pour tout $n \geq 2$, on note f_n l'application de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Q}/\mathbb{Z}$ définie par :

$$\forall\ x \in \mathbb{Z}/n\mathbb{Z},\ f_n(x) = \frac{x}{n}$$

b) Montrer que f_n est bien définie, est un morphisme de groupes, et que, pour tout m divisant n, $f_m = f_n \circ f_{mn}$.

c) Soit G est un groupe muni, pour tout $n \geq 2$, de morphismes $\psi_n : \mathbb{Z}/n\mathbb{Z} \rightarrow$ G tels que, pour tout m divisant n, $\psi_m = \psi_n \circ f_{mn}$. Montrer qu'il existe un unique morphisme $\Psi : \mathbb{Q}/\mathbb{Z} \rightarrow$ G tel que, pour tout n, $\psi_n = \Psi \circ f_n$:



Exo.10) Soit p un nombre premier. Pour tout $n \geq m \geq 2$, on note g_{nm} le morphisme de groupes de $\mathbb{Z}/p^n\mathbb{Z}$ dans $\mathbb{Z}/p^m\mathbb{Z}$ défini par :

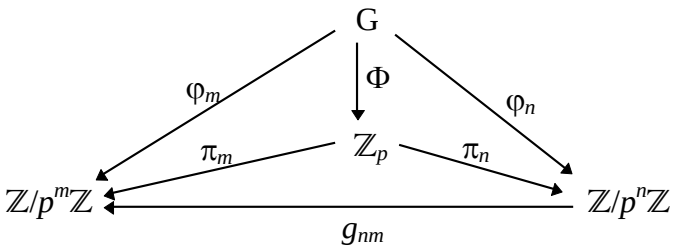
$$\forall\ x \in \mathbb{Z}/p^n\mathbb{Z},\ g_{nm}(x) = x \bmod p^m$$

a) Montrer que g_{nm} est bien défini.

On note $\mathbb{Z}_p$ le groupe constitué des suites $x = (x_n)_{n\geq 2}$ telles que, pour tout n, x_n appartient à $\mathbb{Z}/p^n\mathbb{Z}$, et $x_n = x_{n+1} \bmod p^n$. On note π_n la projection $x \in \mathbb{Z}_p \rightarrow x_n \in \mathbb{Z}/p^n\mathbb{Z}$.

b) Montrer que, pour tout $n \geq m \geq 2$, $\pi_m = g_{nm} \circ \pi_n$

c) Soit G est un groupe muni, pour tout $n \geq 2$, de morphismes φ_n : G $\rightarrow \mathbb{Z}/p^n\mathbb{Z}$ tels que, pour tout $m \leq n$, $\varphi_m = g_{nm} \circ \varphi_n$. Montrer qu'il existe un unique morphisme Φ : G $\rightarrow \mathbb{Z}_p$ tel que, pour tout n, $\varphi_n = \pi_n \circ \Phi$:



Exo.11) Soit G un groupe multiplicatif, *e* son neutre, *a* élément de G, *n* et *m* deux entiers premiers entre eux. Montrer que $a^n = a^m = e \Rightarrow a = e$.

Exo.12) Soit la matrice $A = \begin{pmatrix} 0 & -2/3 & -2/3 \\ 2/3 & 0 & -1/3 \\ 2/3 & 1/3 & 0 \end{pmatrix}$. Montrer que $(\{A, A^2, A^3, A^4\}, \times)$ forme un groupe G commutatif. Comment se fait-il que cet ensemble puisse être un groupe alors que la matrice A n'est pas inversible ?

2- Solutions

Sol.1) a) Il convient d'abord de montrer que la loi est bien une loi de composition interne, c'est-à-dire que, si $b^2 - ab - a^2 \neq 0$ et $d^2 - cd - c^2 \neq 0$, alors :

$(ac + bd)^2 - (ad + bc - ac)(ac + bd) - (ad + bc - ac)^2 \neq 0$

Il suffit pour cela de vérifier que le membre de gauche est égal à $(b^2 - ab - a^2)(d^2 - cd - c^2)$.

La loi est associative :

$((a, b) * (a', b')) * (a'', c'') =$

$(ab'b'' + a'bb'' + a''bb' + 2aa'a'' - aa''b' - aa'b'' - a'a''b, aa''b' + a'a''b + aa'b'' + bb'b'' - aa'a'')$

et qu'il en est de même de $(a, b) * ((a', b') * (a'', c''))$

Le neutre est (0, 1) qui est bien élément de G.

Le symétrique de (a, b) est $\frac{1}{b^2 - ab - a^2}(-a, b - a)$. Il est bien dans G car :

$(b - a)^2 - (b - a)(-a) - a^2 = b^2 - ab - a^2$ est non nul.

b) Par récurrence, $(1, 1)^{*n} = (F_n, F_{n+1})$ où (F_n) est la suite de Fibonacci définie par $F_1 = F_2 = 1$, et, pour tout *n*, $F_{n+2} = F_{n+1} + F_n$. Cette relation est en effet vérifiée pour $n = 1$, et si elle est vraie au rang *n*, alors :

$(1, 1)^{*(n+1)} = (F_n, F_{n+1}) * (1, 1) = (F_n + F_{n+1} - F_n, F_n + F_{n+1}) = (F_{n+1}, F_{n+2})$

c) Il s'agit de montrer que, pour tout élément (a, b) et (c, d) de G, on a :

$N((a, b) * (c, d)) = N(a, b)N(c, d)$

mais cela a été vu en a) pour prouver que la loi $*$ est interne.

Sol.2) En effet, on a $nm(x + y) = mnx + nmy = m0 + n0 = 0$. Par ailleurs, si N est un entier tel que $N(x + y) = 0$, alors, a fortiori, $mN(x + y) = 0$ et comme $my = 0$, on a donc $mNx = 0$, donc mN est un multiple de l'ordre *n* de *x*. Comme *n* et *m* sont premiers entre eux, *n* divise N. Symétriquement, *m* divise N et donc *mn* divise N.

Sol.3) On a $ab = ba$ car $abab = e \Rightarrow abab^2 = b = aba \Rightarrow ab = a^2ba = ba$. Le groupe est donc commutatif, et on peut donc remplacer systématiquement *ba* par *ab*. *a* et *b* sont leurs propres inverses. Les éléments de G sont donc des produits de *a* et *b*, sans que deux *a* se suivent (car $a^2 = e$),

ni deux b, ni deux ab (pour la même raison) et sans qu'il y ait de ba. Il y a donc au plus les élément suivants :

e
a
b
ab

ab est différent de a, sinon aurait $b = e$. De même, il est différent de b. Il est différent de e sinon on aurait $ab = a^2$ et donc $a = b$. G est donc constitué de ces quatre éléments distincts. Il s'agit du groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ avec la correspondance $a = (1,0)$ et $b = (0,1)$.

Sol.4) Pour tout a et b de G, on a $(ab)^2 = e = abab$ donc, en multipliant à gauche par a et à droite par b, $ab = a^2bab^2 = ebae = ba$, ce qui prouve que G est commutatif. Remarquons par ailleurs que $a^2 = e$ signifie que a est égal à son symétrique.
Prenons a élément de G différent de e, puis b élément de G différent de e et a, puis c élément de G différent de e, a, b et ab. $\{a, b, c\}$ engendre le sous-groupe $\{e, a, b, c, ab, ac, bc, abc\}$. Vérifions que les éléments sont tous distincts.
On a $ab \neq e$ sinon $b = a^{-1} = a$. On $ab \neq a$ sinon $b = e$. De même $ab \neq b$.
On a $ac \neq e$ sinon $c = a^{-1} = a$. $ac \neq a$ sinon $c = e$. $ac \neq b$ sinon $c = ab$. $ac \neq c$ sinon $a = e$. $ac \neq ab$ sinon $c = b$.
$bc \neq a$ sinon $c = b$. $bc \neq a$ sinon $c = ba = ab$. $bc \neq b$ sinon $c = e$. $bc \neq c$ sinon $b = e$. $bc \neq ab$ sinon $c = bab = ab^2 = a$. $bc \neq ac$ sinon $b = c$. $bc \neq ac$ sinon $a = b$.
$abc \neq e$ sinon $c = ba = ab$. $abc \neq a$ sinon $bc = e$ et $c = b$. $abc \neq b$ sinon $c = bab = a$. $abc \neq c$ sinon $ab = e$ et $b = a$. $abc \neq ab$ sinon $c = e$. $abc \neq ac$ sinon $b = e$. $abc \neq bc$ sinon $a = e$.
G ayant huit éléments, on a $G = \{e, a, b, c, ab, ac, bc, abc\}$. On obtient un isomorphisme de G vers $(\mathbb{Z}/2\mathbb{Z})^3$ par exemple en posant :

$f(a) = (1, 0, 0)$
$f(b) = (0, 1, 0)$
$f(c) = (0, 0, 1)$

puis :

$f(ab) = (1, 1, 0)$
$f(ac) = (1, 0, 1)$
$f(bc) = (0, 1, 1)$
$f(abc) = (1, 1, 1)$
$f(e) = (0, 0, 0)$

Sol.5) a) On a $r^2 = \mathrm{Id}$, donc $H = \{\mathrm{Id}, r\}$. La loi $*$ est bien interne, puisque, si u et v sont directes, il en est de même de ur^mvr^m. Par ailleurs, r^{m+p} appartient à H.
La loi est associative. En effet :

$$((u, r^m) * (v, r^p)) * (w, r^s) = (ur^mvr^m, r^{m+p}) * (w, r^s) = (ur^mvr^m\ r^{m+p}wr^{m+p}, r^{m+p+s})$$
$$= (ur^mvr^pwr^{m+p}, r^{m+p+s})$$

et on vérifiera qu'il en est de même de $(u, r^m) * ((v, r^p) * (w, r^s))$.
Le neutre est (Id, r^0).
Le symétrique de (u, r^m) est $(r^mu^{-1}r^m, r^m)$ qui est bien dans G, $r^mu^{-1}r^m$ étant directe.
b) Considérons l'application $f : G \to O_n(\mathbb{R})$ définie par :

$f(u, r^m) = ur^m$

Il s'agit d'un morphisme de groupes. En effet :

$f((u, r^m) * (v, r^p)) = f(ur^m vr^m, r^{m+p}) = ur^m vr^m\, r^{m+p} = ur^m vr^p = f(u, r^m)\, f(v, r^p)$

L'application f est injective. Soit (u, r^m) appartenant à son noyau. On a alors ur^m = Id, donc ur^m est une isométrie directe, donc m est pair, donc r^m = Id = r^0 et donc u = Id.

L'application f est surjective. Si v est un isométrie directe, $v = f(v, r^0)$ et si v est indirecte, $v = f(vr, r)$.

Sol.6) On utilise le fait que l'ordre d'un élément divise l'ordre du groupe. Donc tout élément autre que le neutre e est d'ordre 3 ou 9.

S'il existe un élément a d'ordre 9, alors le groupe est égal à $\{a^k, 0 \le k < 9\}$, isomorphe à $\mathbf{Z}/9\mathbf{Z}$.

Sinon, tous les éléments autres que e sont d'ordre 3. Soit a un tel élément, et soit b un autre élément, différents de e, a, a^2. On a donc $a^3 = b^3 = e$. Montrons que $a^i b^j = e \Rightarrow i = j = 0$ (mod 3). En effet, $b^j = a^{3-i}$ donc $b^{j^2} = (b^j)^j = a^{(3-i)j}$. On a alors $j = 0$ car si $j = 1$ ou 2 mod 3, $j^2 = 1$ mod 3 donc $b^{j^2} = b = a^{(3-i)j}$ ce qui est contraire à l'hypothèse. Puisque $j = 0$, on a $a^i = e$, donc $i = 0$. Si l'on a maintenant $a^i b^j = a^k b^l$, alors, en multipliant à gauche par l'inverse de a^k et à droite par l'inverse de b^l, on obtient $a^{i-k} b^{j-l} = e$, donc $i = k$ et $j = l$. On a montré que tous les éléments e, a, a^2, b, b^2, ab, a^2b, ab^2, a^2b^2 sont tous distincts.

Comme $\{e, a, a^2, b, b^2, ab, a^2b, ab^2, a^2b^2\}$ contient neuf éléments, il s'agit de tous les éléments du groupe. Montrons maintenant qu'il est commutatif. ba est élément du groupe donc fait partie de la liste précédente. Il suffit de montrer qu'il est différent de tous les éléments, sauf ab. Par exemple, $ba \ne ab^2$, car si $ba = ab^2$, alors $bab = ab^3 = a$ donc $babab = (bab)ab = a^2b = ba(bab) = ba^2$, donc $a^2b = ba^2$, donc $ab = a^4b = a^2a^2b = a^2ba^2 = ba^2a^2 = ba^4 = ba$. Donc a et b commutent, mais alors $ba = ab^2$ donne $ab = ab^2$ et donc $b = e$ ce qui est exclu. De même $ba \ne a^2b$ par un raisonnement analogue. On a aussi $ba \ne a^2b^2$ sinon on aurait $bab = a^2b^3 = a^2$ donc $baba = a^3 = e$ donc ba est d'ordre inférieur ou égal à 2 donc $ba = e$ donc $b = a$, etc.

Une fois montré la commutativité, le groupe est égal à $\{a^i b^j, 0 \le i \le 2, 0 \le j \le 2\}$, isomorphe à $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.

Sol.7) a) f(H) est non vide, puisque H est non vide. Soient u et v éléments de f(H). Il existe x et y éléments de H tels que $u = f(x)$ et $v = f(y)$. Donc :

$$uv^{-1} = f(x)f(y)^{-1} = f(xy^{-1}) \in f(\mathrm{H})$$

b) f^{-1}(K) est non vide car le neutre e de G a pour image le neutre ε de F qui est aussi celui de K. Soient x et y éléments de f^{-1}(K). On a :

$f(x)$ et $f(y)$ éléments de K
donc $f(x)f(y)^{-1}$ aussi
donc $f(xy^{-1})$ aussi, puisque $f(xy^{-1}) = f(x)f(y)^{-1}$
donc $xy^{-1} \in f^{-1}(\mathrm{K})$

Sol.8) a) Ker(f) est un sous-groupe de G, et dans la démonstration du théorème de Lagrange, on a montré que les parties xKer(f) constituaient une partition de G, et qu'elles avaient toutes même nombre d'éléments. Si on note p le nombre de telles parties, il existe x_1, ..., x_p tel que :

$\mathrm{G} = x_1\mathrm{Ker}(f) \cup ... \cup x_p\mathrm{Ker}(f)$, réunion disjointe

avec, pour tout $i \ne j$, $x_i\mathrm{Ker}(f) \ne x_j\mathrm{Ker}(f)$, i.e. $x_j^{-1}x_i \notin \mathrm{Ker}(f)$.Le nombre p n'est autre que $\dfrac{\mathrm{Card(G)}}{\mathrm{Card(Ker}(f))}$.

On a alors :

$\mathrm{Im}(f) = \{f(x_1), ..., f(x_p)\}$

De plus, les $f(x_i)$ sont distincts car $x_j^{-1}x_i \notin \text{Ker}(f) \Rightarrow f(x_j^{-1}x_i) \neq e_{G'} \Rightarrow f(x_i) \neq f(x_j)$. Donc $p = \text{Card}(\text{Im}(f))$. Donc $\text{Card}(\text{Im}(f)) = \dfrac{\text{Card}(G)}{\text{Card}(\text{Ker}(f))}$

b) On a de même $\text{Card}(H) = \text{Card}(\text{Im}(g))\ \text{Card}(\text{Ker}(g))$, donc :

$$\frac{\text{Card}(G)}{\text{Card}(H)} = \frac{\text{Card}(\text{Im}(f))\ \text{Card}(\text{Ker}(f))}{\text{Card}(\text{Im}(g))\ \text{Card}(\text{Ker}(g))}$$

Sol.9) a) Il s'agit de montrer que $f_{mn}(x)$ ne dépend du représentant choisi dans la classe de x mod m. Or si $y \equiv x \bmod m$, il existe k tel que $y = x + km$ donc $\frac{n}{m}y = \frac{n}{m}x + kn \equiv \frac{n}{m}x \bmod n$, donc $\frac{n}{m}y$ et $\frac{n}{m}x$ ont même valeur dans $\mathbb{Z}/n\mathbb{Z}$. C'est cette valeur qu'on attribue à $f_{mn}(x)$. Le fait que f_{mn} est un morphisme ne pose pas de difficulté.

b) x est défini modulo n donc $\frac{x}{n}$ est défini modulo 1 et est donc un unique élément de $\mathbb{Q}/\mathbb{Z}$. Il n'y a pas de difficulté à montrer que f_n est un morphisme de groupes. Enfin, si m divise n, on a, pour tout x de $\mathbb{Z}/m\mathbb{Z}$:

$$(f_n \circ f_{mn})(x) = f_n(\frac{n}{m}x) = \frac{1}{n}(\frac{n}{m}x) = \frac{x}{m} = f_m(x)$$

c) Soit q élément de $\mathbb{Q}/\mathbb{Z}$. q est défini modulo 1. Si n est un entier tel que nq soit entier, cet entier est défini modulo n donc est élément de $\mathbb{Z}/n\mathbb{Z}$. On doit donc nécessairement avoir :

$$\psi_n(nq) = (\Psi \circ f_n)(nq) = \Psi(\frac{nq}{n}) = \Psi(q)$$

ce qui prouve l'unicité de Ψ. Pour prouver son existence, définissons $\Psi(q)$ par $\psi_n(nq)$ pour tout entier n tel que nq soit entier. Il convient de vérifier que $\Psi(q)$ ne dépend pas du multiple n choisi. Soit m un autre entier tel que mq soit entier. Posons $q = \frac{a}{b}$ avec a et b premiers entre eux (a est défini modulo b près), et soit d le PGCD de n et m. Posons $n = dn'$, $m = dm'$ avec n' et m' premiers entre eux. Comme $nq = \frac{na}{b}$ est entier (modulo n) et que b est premier avec a, cela signifie que b divise n. De même, il divise m. Donc il divise leur PGCD d et il existe k tel que $d = kb$. Donc :

$nq = \frac{na}{b} = \frac{dn'a}{b} = \frac{kbn'a}{b} = kn'a$ élément de $\mathbb{Z}/n\mathbb{Z}$

De même :

$mq = km'a$ élément de $\mathbb{Z}/m\mathbb{Z}$

On a :

$$\psi_n(nq) = \psi_n(kn'a) = \psi_{dn'}(kn'a) = \psi_{dn'}(\frac{dn'}{d}ka) = (\psi_{dn'} \circ f_{d,dn'})(ka) = \psi_d(ka)$$

car $\psi_{dn'} \circ f_{d,dn'} = \psi_d$, et le calcul de $\psi_m(mq)$ conduit au même résultat. Ainsi, Ψ est bien défini.
On a bien, pour tout n, $\psi_n = \Psi \circ f_n$ puisque, pour tout x de $\mathbb{Z}/n\mathbb{Z}$:

$$(\Psi \circ f_n)(x) = \Psi(\frac{x}{n}) = \psi_n(n\frac{x}{n}) = \psi_n(x)$$

Ψ est bien un morphisme de groupes. Si q et q' sont élément de $\mathbb{Q}/\mathbb{Z}$, prendre n tel que nq et nq' soient tous deux entiers et utiliser le fait que ψ_n est un morphisme de groupes.
$\mathbb{Q}/\mathbb{Z}$ s'appelle la limite inductive des $\mathbb{Z}/n\mathbb{Z}$.

Sol.10) a) x étant défini modulo p^n et m étant inférieur ou égal à n, p^m divise p^n donc x est défini modulo p^m. La quantité x mod p^m est donc bien définie sans ambiguïté.
b) Montrons par récurrence sur n que, pour $n \geq m$, $x_m = x_n \bmod p^m$. C'est trivial pour $n = m$ et vrai pour $n = m + 1$ par hypothèse. Si c'est vrai au rang n, alors :

$$x_m = x_n \bmod p^m = (x_{n+1} \bmod p^n) \bmod p^m = x_{n+1} \bmod p^m \qquad \text{puisque } p^m \text{ divise } p^n$$

c) Puisqu'on doit avoir, pour tout z de G, $\varphi_n(z) = (\pi_n \circ \Phi)(z) = \pi_n(\Phi(z))$ et que π_n désigne la n-ème composante de $\Phi(z)$, on ne peut que prendre $\Phi(z) = (\varphi_n(z))_{n\geq 2}$. D'où l'unicité.
Il reste à montrer que $\Phi(z)$ est bien élément de $\mathbb{Z}_p$, à savoir :

$$\forall\ n,\ \varphi_n(z) = \varphi_{n+1}(z) \bmod p^n$$

mais cela résulte du fait que $\varphi_n = g_{n+1,n} \circ \varphi_{n+1}$. Enfin, il est facile de montrer que Φ est un morphisme de groupes en utilisant le fait que les φ_n le sont.
$\mathbb{Z}_p$ s'appelle limite projective des $\mathbb{Z}/p^n\mathbb{Z}$, et également groupe p-adique.

Sol.11) n et m étant premiers entre eux, il existe x et y entiers tels que $xn + ym = 1$ (identité de Bézout, voir L1/ARITHMQ.PDF). On a alors :

$$a = a^1 = a^{xn+ym} = (a^n)^x * (a^m)^y = e^x * e^y = e$$

Sol.12) On vérifiera que $A^5 = A$, ce qui permet de montrer ensuite par récurrence que tout A^n, $n \geq 1$, est élément de G. Le produit est associatif (et même ici commutatif). Le neutre est A^4. Le symétrique de A^k, $1 \leq k \leq 3$, est A^{4-k}.
G est un exemple montrant que $\mathcal{M}_4(\mathbb{R})$ peut contenir des groupes multiplicatifs qui ne sont pas des sous-groupes de $GL_4(\mathbb{R})$. Mais dans ce cas, le neutre n'est pas I_4 et le symétrique d'une matrice n'est pas son inverse usuel. On comprend mieux la situation en diagonalisant A dans $\mathbb{C}$. On verra alors que A est semblable à la matrice $\begin{pmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Les puissances de $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ forment un sous-groupe de $GL_2(\mathbb{C})$. On s'est amusé à rajouter une composante nulle dans une troisième dimension pour rendre la matrice A non inversible.

◆