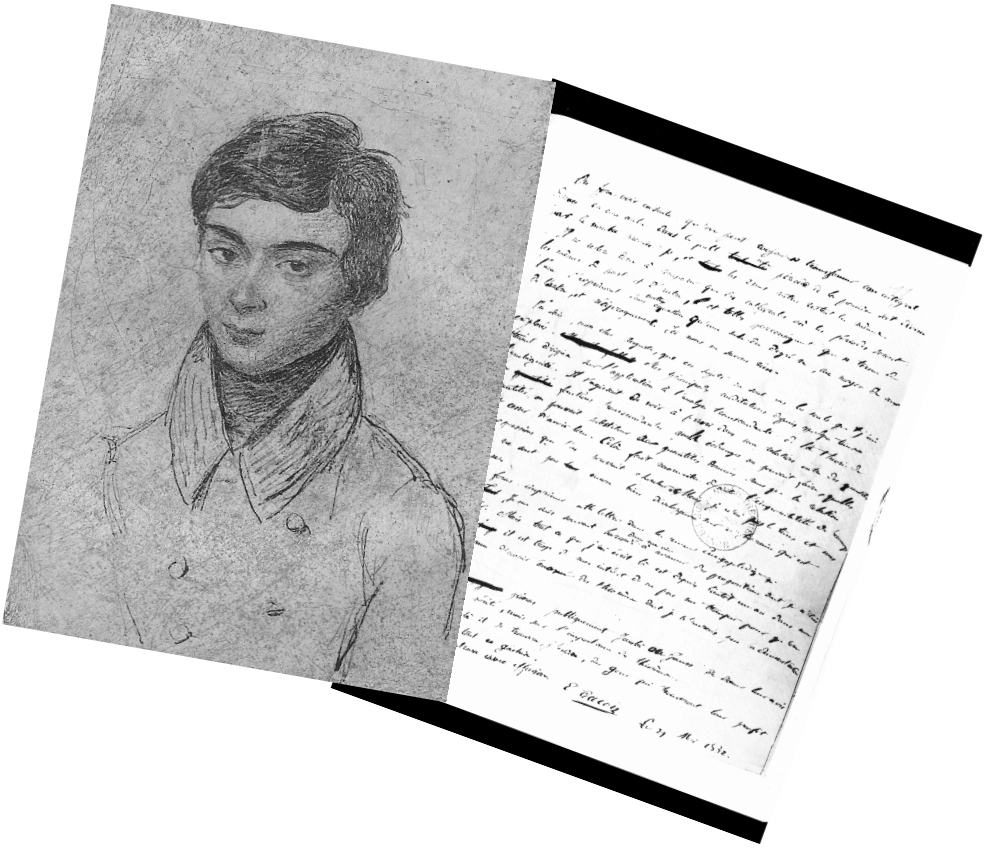
ÉLÉMENTS DE THÉORIE DES GROUPES

1re Option spécifique

Jean-Philippe Javet



Mon cher Auguste, [...]Je me suis souvent hasardé dans ma vie à avancer des propositions dont je n'étais pas sûr. Mais tout ce que j'ai écrit là est depuis bientôt un an dans ma tête, et il est trop de mon intérêt de ne pas me tromper pour qu'on me soupçonne d'avoir énoncé des théorèmes dont je n'aurais pas la démonstration complète. Tu prieras publiquement Jacobi et Gauss de donner leur avis, non sur la vérité, mais sur l'importance des théorèmes. Je t'embrasse avec effusion

Évariste Galois
29 mai 1832

Table des matières

Malgré le soin apporté lors de sa conception et surtout parce qu'il a été utilisé en classe qu'à une reprise, le polycopié que vous avez entre les mains contient certainement quelques erreurs et coquilles. Merci de participer à son amélioration en m'envoyant un mail :

jeanphilippe.javet@vd.educanet2.ch

Merci ;-)

;-) Votre prof de math vous a souvent reproché votre manque de rigueur dans la rédaction de vos exercices de mathématiques... Que pensez-vous de ceci ?

1 Mise en place

1.1 Préambule

Évariste Galois
mathématicien français
(1811-1832)

Évariste Galois a tout juste vingt ans lorsqu'il meurt dans un duel. Il restera pourtant comme l'un des plus grands mathématiciens de son temps pour avoir introduit la notion de groupe, alors qu'il avait à peine dix-sept ans.

- Vous savez résoudre les équations du deuxième degré :

$$ax^2 + bx + c = 0.$$

  Les solutions s'expriment en fonction de a, b, c et de la fonction racine carrée $\sqrt{\ }$.

- Pour les équations du troisième degré : $ax^3 + bx^2 + cx + d = 0$, il existe aussi des formules.
  Par exemple une solution de $x^3 + 3x + 1 = 0$ est :

$$x_1 = \sqrt[3]{\frac{\sqrt{5}-1}{2}} - \sqrt[3]{\frac{\sqrt{5}+1}{2}}.$$

- De telles formules existent aussi pour les équations du quatrième degré.

Niels Abel
mathématicien norvégien
(1802-1829)

Une préoccupation majeure au début du XIX^{e} siècle était de savoir s'il existait des formules similaires pour les équations de degré 5 ou plus. La réponse fut apportée par Galois et Abel :

Non il n'existe pas en général une telle formule.

Galois parvient même à dire pour quels polynômes c'est possible et pour lesquels ça ne l'est pas. Il définit pour sa démonstration la notion de groupe.
Les groupes sont à la base d'autres notions mathématiques comme les *anneaux*, les *corps*, les *matrices*, les *espaces vectoriels*, ... Mais vous les retrouvez aussi en *arithmétique*, en *géométrie*, en *cryptographie* !

Avant d'introduire la définition d'un groupe, nous commencerons par définir les notions de loi de composition interne et composition de fonctions.

1.2 Opération interne ou loi de composition interne

1.2.1 Exemples introductifs

Considérons la soustraction dans $\mathbb{N}$. Au couple $(3\,;2)$ peut être associé le nombre $3-2=1$; par contre, au couple $(2\,;3)$ le nombre $2-3=-1$ ne peut pas l'être, car -1 ne se trouve pas dans $\mathbb{N}$. La soustraction dans $\mathbb{N}$ apparaît donc comme une relation de $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$, mais qui ne s'applique pas à tous les couples de nombres entiers $(a\,;b)$. On constate en fait que les couples pour lesquels cette relation n'est pas possible sont ceux dont le deuxième terme est plus grand que le premier.
Considérons maintenant l'addition dans $\mathbb{N}$. Au couple $(3\,;2)$ peut-être associé le nombre $3+2=5$. Dans le cas de l'addition, à chaque couple $(a\,;b) \in \mathbb{N}^2$ est associé le nombre $a+b$. Nous avons donc une application $+$ de $\mathbb{N}^2$ dans $\mathbb{N}$ donnée par :

$$\begin{array}{rccc} + : & \mathbb{N}^2 & \to & \mathbb{N} \\ & (a\,;b) & \mapsto & a+b \end{array}$$

Définition: On appelle **opération interne** ou **loi de composition interne** dans un ensemble E toute application de $E \times E$ dans E définie pour tous les couples $(a\,;b) \in E \times E$.

Exemple 1: L'addition et la multiplication sont des opérations internes dans $\mathbb{N}$, au contraire de la soustraction et de la division.

1.2.2 Propriétés d'une loi de composition interne

Dans tout ce qui va suivre, le symbole $\star$ désignera une loi de composition (interne ou non) ; $\star$ est donc la procédure de calcul sur l'ensemble considéré.

Définition: On dit que $\star$ définie dans un ensemble E est **commutative** si et seulement si $a \star b = b \star a$ pour tout $a, b \in E$.

Exemple 2: Dans $\mathbb{R}$, définissons $(x\,;y) \mapsto x \star y$ par :

a) $x \star y = \dfrac{x+y}{2}$ (moyenne arithmétique)

b) $x \star y = \sqrt{x \cdot y}$ (moyenne géométrique)

Montrer, dans les deux cas, que $x \star y$ est commutative.

Exercice 1.1: Parmi les lois suivantes, lesquelles sont des opérations internes sur les ensembles considérés ? Justifier.

a) $\mathbb{Z}$ avec $\star$ la moyenne arithmétique ;

b) $\mathbb{R}$ avec $\star$ la moyenne géométrique ;

c) $E = \left\{ \frac{x}{3} \mid x \in \mathbb{Z} \right\}$ avec l'addition ;

d) $F = \{x \in \mathbb{R} \mid x > 3\}$ avec l'addition ;

e) $G = \{x \in \mathbb{R} \mid x \geqslant 5\}$ avec la multiplication ;

f) $\mathbb{Q}$ avec la moyenne arithmétique ;

g) $\mathbb{R}$ avec $x \star y = x \cdot y + y - x$;

h) $\mathbb{Z}$ avec $x \star y = x \cdot y + \frac{x}{y}$.

Exercice 1.2: Parmi les lois de composition interne découvertes ci-dessus, lesquelles sont commutatives ?

Définition: On dit que $\star$ définie dans un ensemble E est **associative** si et seulement si $(a \star b) \star c = a \star (b \star c)$ pour tout $a, b, c \in E$.

Exemple 3: La multiplication et l'addition dans $\mathbb{R}$ sont associatives.

Remarque: Si une opération interne $\star$ est associative dans E, on peut supprimer ou ajouter une ou des paires de parenthèses dans toutes les expressions contenant des éléments de E reliées par $\star$, mais sans changer l'ordre des éléments :

$$(a \star b) \star c = a \star (b \star c) = a \star b \star c$$

Exemple 4: La loi $\star$ définie dans $\mathbb{R} \times \mathbb{R}$ par $(x\,;y) \star (a\,;b) = (xa\,;yb)$, est-elle associative ?

Exercice 1.3: Montrer que la loi $x \star y = \dfrac{x+y}{1+xy}$ est associative sur $\mathbb{R}_+^\star$.

Exercice 1.4: Dans $E = \{1,2,3,4\}$ on pose $a \star b = \min(a\,,b)$ [1].

Étudier cette loi, *c'est-à-dire montrer si, oui ou non, elle est interne, commutative et associative.*

Exercice 1.5: Dans $\mathbb{R}^2$, étudier la loi + définie par :

$$(x\,;y) + (a\,;b) = (x+a\,;y+b)$$

Exercice 1.6: Dans $\mathbb{R}^2$ étudier la loi $\star$ définie par :

$$(x\,;y) \star (a\,;b) = (xa - yb\,;xb + ya).$$

Exercice 1.7: Dans $\mathbb{R}$ on envisage l'opération interne $x \star y = mxy + 1$.
Déterminer $m \in \mathbb{R}$ de sorte que $\star$ soit associative.

Exercice 1.8: Dans $\mathbb{R}$ on envisage l'opération interne $x \star y = 2x + 2y - 4xy - \dfrac{1}{2}$.
Étudier $\star$.

1. $\min(a\,,b)$ renvoie la plus petite des 2 valeurs. Par exple : $\min(4\,,1) = 1$

1.3 Composition de fonctions

Considérons les fonctions suivantes définies sur tout $\mathbb{R}$

$$f(x) = 2x + 1$$
$$g(x) = 3x - 1$$

Considérons alors $x = 1$. En calculant $f(1)$, on obtient 3. On peut alors calculer $g(3) = 8$. On a donc calculé d'abord l'image de 1 par f, puis l'image de 3 par g. On obtient donc :

$$g\left(f(1)\right) = g(3) = 8.$$

On vient d'effectuer ce que l'on appelle la **composition des fonctions** f puis g pour la valeur $x = 1$.

On pourrait également d'abord calculer $g(1)$ on obtient $g(1) = 2$ puis $f(2) = f\left(g(1)\right) = 5$. Dans ce cas, on a effectué la composition des fonctions g puis f.

On constate alors qu'effectuer f puis g n'est, en général, pas équivalent à effectuer g puis f.

Définition: Soient deux fonctions f et g définies respectivement sur les ensembles $E_D(f)$ et $E_D(g)$.

On définit la fonction $h = f \circ g$ appelée la **composée de f et g** par $h(x) = f(g(x))$ pour tous les x tels que $x \in E_D(g)$ et $g(x) \in E_D(f)$.

L'opération $\circ$ s'appelle la **composition** de fonctions.

On peut résumer cette opération par le diagramme suivant :

Exemple 5: Considérons les fonctions f et g définies par :

$$f(x) = 2x + 1 \qquad\qquad g(x) = 3x - 1.$$

Compléter alors pour tout $x \in \mathbb{R}$ les égalités suivantes :

$h(x) = (f \circ g)(x) = \ldots(\ldots(x)) = f(\ldots\ldots\ldots) = \ldots\ldots\ldots\ldots\ldots$

$= \ldots\ldots\ldots\ldots\ldots$

$k(x) = (g \circ f)(x) = \ldots(\ldots(x)) = g(\ldots\ldots\ldots) = \ldots\ldots\ldots\ldots\ldots$

$= \ldots\ldots\ldots\ldots\ldots$

Exemple 6: Considérons $f(x) = \sqrt{x-3}$ et $g(x) = x^2 + 1$.

On a $E_D(f) = [\ldots;\ldots[$ et $E_D(g) = \ldots$.

- Considérons la fonction $h = g \circ f$.

  $h(x) = \ldots(\ldots(x)) = g(\ldots\ldots) = \ldots\ldots\ldots\ldots\ldots\ldots$

  Pour autant que l'on considère $E_D(h) = [\ldots;\ldots[$.

- Si l'on considère $k = f \circ g$ on a :

  $k(x) = \ldots(\ldots(x)) = f(\ldots\ldots) = \ldots\ldots\ldots\ldots\ldots\ldots$

  avec $E_D(k) = \{x \in \mathbb{R} \mid x^2 - 2 \geqslant 0\} =]\ldots;\ldots] \cup [\ldots;\ldots[$

Remarque: La composition $f \circ g$ de deux fonctions f et g peut toujours être définie pour autant que si $x \in E_D(g)$, alors $g(x) \in E_D(f)$.

Exercice 1.9: On se donne les fonctions de $\mathbb{R}^\star$ dans $\mathbb{R}^\star$ suivantes :

$$i(x) = x \qquad f(x) = -x \qquad g(x) = \frac{1}{x} \qquad h(x) = -\frac{1}{x}.$$

Soit $E = \{i, f, g, h\}$ et considérons la composition des fonctions $\circ$ sur E.

a) Montrer qu'il s'agit bien d'une loi de composition interne.

b) Est-elle alors commutative ?

c) Est-elle associative ? Combien de calculs doit-on proposer pour l'affirmer ?

Nous admettons le résultat suivant sans démonstration :

Théorème: Soit A un ensemble quelconque et $\mathcal{F}_A$ l'ensemble de toutes les fonctions de A dans A.
La composition des fonctions $\circ$ est une opération interne sur $\mathcal{F}_A$.

1.3.1 Fonctions bijectives et fonctions réciproques

Définition: Soit f une application de E dans F. On dit que f est une **bijection** ou **une application bijective** si chaque élément y de F est l'image d'un élément unique x de E.

Exprimée en langage formel, cette définition devient :

Définition:

$$f \text{ est bijective} \iff \forall y \in F,\ \exists!\, x \in E \text{ tel que } y = f(x)$$

Remarque: Lorsque les ensembles considérés E et F sont des parties de $\mathbb{R}$, on parlera alors de **fonctions bijectives**.

Exemple 7: On considère la fonction f définie sur $\mathbb{R}$ par $f(x) = 2x + 3$. Montrer que f est une bijection.

Exercice 1.10: Soit f la fonction définie sur $\mathbb{Q}$ par :

$$f : x \mapsto ax + b \qquad a, b \in \mathbb{Q}$$

Quelles conditions doivent respecter a et b pour que f soit une bijection ?

Exercice 1.11: On considère la fonction f définie sur $\mathbb{R}$ par $f(x) = x^2$.

a) Montrer que f n'est pas une bijection.

b) Qu'en est-il si on considère f sur $\mathbb{R}_+$?

Définition: Si $f : E \to F$ est une bijection, alors on peut définir **la fonction réciproque** ${}^rf : F \to E$

$$\begin{array}{rccc} f: & E & \to & F \\ & x & \mapsto & f(x) = y \end{array} \qquad \begin{array}{rccc} {}^rf: & F & \to & E \\ & y & \mapsto & {}^rf(y) = x \end{array}$$

On vérifie que $({}^rf \circ f)(x) = x$ et que $(f \circ {}^rf)(y) = y$.

Pour trouver la fonction réciproque de f, on résout, par rapport à x, l'équation $y = f(x)$. On obtient ainsi l'expression $x = {}^rf(y)$.

Exemple 8: On considère la fonction bijective f définie par $f(x) = 2x + 3$. Déterminer ${}^rf$.

Exercice 1.12: Soit f la fonction définie sur $\mathbb{Q}$ par :

$$f : x \mapsto \frac{2x+3}{x-1}$$

a) Pour quelles valeurs de x, f est-elle bien définie ?

b) Déterminer ${}^{r}f$.

c) Préciser alors les sous-ensembles de $\mathbb{Q}$ à considérer pour que f soit bien une bijection.

2

Notion de groupe

2.1 Exemples introductifs

Introduction: Vous avez déjà rencontré en mathématiques des ensembles de nombres, de vecteurs, de fonctions, à priori de natures très différentes, et pourtant, une fois définies dans ces ensembles des lois notées $+$, $\cdot$, ou $\circ$, vous avez dû vous apercevoir que les règles de calcul offraient de grandes ressemblances.
Parfois, sans même en être conscient, vous utilisez des propriétés de l'addition et de la multiplication des nombres réels, (commutativité, associativité ou distributivité par exemple) dans des calculs de vecteurs, de fonctions ou ...
La similitude formelle des propriétés de calculs dans des ensembles si différents a conduit les mathématiciens à donner des noms à la donnée d'un ensemble et d'une loi vérifiant un certain nombre de propriétés bien définies. Nous en étudierons ici un exemple : **la structure de groupe**.

Exemple 1: Considérons $\mathbb{Z}$ muni de l'addition $+$. Nous savons déjà que $+$ est une opération interne associative dans $\mathbb{Z}$. Mais existe-t-il alors d'autres propriétés intéressantes de $+$?

Il existe un élément particulier : 0 ; en effet, $a+0=0+a=a$ pour tout $a \in \mathbb{Z}$. On dit alors que 0 est **neutre** pour l'addition.
Il existe aussi pour chaque nombre $a \in \mathbb{Z}$ le nombre $-a \in \mathbb{Z}$ qui lui est opposé, i.e. $a+(-a)=(-a)+a=0$.
Si l'on fait maintenant une synthèse de certaines propriétés de $+$ dans $\mathbb{Z}$, on voit que :

- $+$ est une opération interne
- $+$ est une opération associative
- il existe un élément neutre pour $+$: 0
- pour chaque élément $a \in \mathbb{Z}$ il existe un opposé $a' \in \mathbb{Z}$ tel que $a+a'=a'+a=0$. Dans ce cas, $a'=-a$

Problème: *Si l'on considère une opération interne $\star$ quelconque dans un ensemble non vide G, existe-t-il un élément de G analogue à 0, i.e. un élément particulier qui est neutre pour $\star$?*

Définition: Soit $\star$ une opération interne sur un ensemble G non vide.
On appelle **élément neutre** pour $\star$ tout élément $e \in G$ tel que $e \star g = g \star e = g$ pour tout $g \in G$.

Exemple 2: Si $\star$ est la multiplication sur $\mathbb{R}^\star$, un élément neutre est donné par 1.

Problème: *Si l'on considère une opération interne $\star$ quelconque dans un ensemble non vide G telle qu'il existe un élément neutre $e \in G$, existe-t-il pour tout élément $g \in G$ un élément $g' \in G$ de sorte que $g \star g' = g' \star g = e$?*

Définition: Soit $\star$ une opération interne sur un ensemble G non vide et $e \in G$ un élément neutre pour $\star$. Soit $g \in G$.
On appelle **élément symétrique de g par rapport à e** tout élément $g' \in G$ tel que $g \star g' = g' \star g = e$

Exemple 3: Si $\star$ est la multiplication sur $\mathbb{R}^\star$, un élément neutre est donné par 1 et un élément symétrique de $x \in \mathbb{R}^\star$ est donné par $x' = \dfrac{1}{x}$.

2.1.1 Définitions et propriétés

Définition: **Un groupe**, noté $(G,\star)$, est un ensemble G non vide auquel est associé une loi de composition $\star$ vérifiant les quatre propriétés :

- $\forall x, y \in G,\ x \star y \in G$ ($\star$ est une loi de composition interne) ;
- $\forall x, y, z \in G,\ (x \star y) \star z = x \star (y \star z)$ (la loi est associative) ;
- $\exists e \in G$ tel que $\forall x \in G$,
  $x \star e = x$ et $e \star x = x$ (e est l'élément neutre) ;
- $\forall x \in G,\ \exists x' \in G$ tel que
  $x \star x' = x' \star x = e$ (x' est l'élément symétrique) ;

Définition: Un groupe $(G,\star)$ est dit **abélien** ou **commutatif** si $\star$ est commutative.

Exemple 4:

a) $(\mathbb{N},+)$ n'est pas un groupe car 2, par exemple, n'a pas de symétrique dans $\mathbb{N}$;

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

c) $(\mathbb{Q},\cdot)$ n'est pas un groupe car 0 n'a pas de symétrique dans $\mathbb{Q}$; par contre $(\mathbb{Q}^\star,\cdot)$ est clairement un groupe.

Exemple 5: Le groupe trivial $(\{e\},\star)$, formé de l'unique élément e (un singleton) et muni de la seule opération possible $\star$ vérifiant que :

$$e \star e = e \qquad (e \text{ étant alors élément neutre...})$$

Exemple 6: Dans $E = \{-1\,;1\}$ on considère la loi $\star$ définie sur $E \times E$ de la manière suivante :

$$(x\,;y) \star (a\,;b) = (x \cdot a\,;y \cdot b)$$

S'agit-il d'un groupe ?

Exercice 2.1: **Suite de l'exercice 1.4**
Dans $E = \{1, 2, 3, 4, 5, 6\}$ on pose $a \star b = \min(a, b)$.
S'agit-il d'un groupe ? Si oui, est-il abélien ?

Exercice 2.2: **Suite de l'exercice 1.5**
Dans $\mathbb{R}^2$ on considère la loi + définie de la manière suivante :

$$(x\,;y) + (a\,;b) = (x + a\,;y + b)$$

S'agit-il d'un groupe ? Si oui, est-il abélien ?

Voici les premières propriétés des groupes, données avec démonstrations :

Pour prouver l'unicité d'un objet, on suppose qu'il a un "jumeau", et on applique alors les conditions imposées par la structure ambiante jusqu'à finalement constater que les deux objets sont égaux.

Proposition: Dans un groupe $(G,\star)$, l'élément neutre est unique.

Preuve:

Proposition: Dans un groupe $(G,\star)$, tout élément $g \in G$ admet un unique symétrique $g' \in G$.

Preuve:

Proposition: Dans un groupe $(G,\star)$, le symétrique du composé de deux éléments est égal au composé des symétriques de ces éléments dans l'ordre inverse.
Autrement dit, $(g \star h)' = h' \star g'$.

Preuve:

Remarque: Il existe plusieurs manières de noter un groupe :

Notation	Op. interne	Comp. de a et b	El. neutre	El. sym. de a	nom du sym.
générale	$\star$	$a \star b$	e	a'	
additive	$+$	$a+b$	0	$-a$	opposé de a
multiplicative	$\cdot$	$a \cdot b$	1	a^{-1} ou $1/a$	inverse de a
composition	$\circ$	$b \circ a$	Id	${}^r a$	réciproque de a

Exercice 2.3: Dire pourquoi les structures suivantes ne sont pas celles d'un groupe :

a) $x \star y = x - y$ dans $E = \{0, 1, 2, 3, 4\}$

b) $x \star y = x + y$ dans $E = \{z \in \mathbb{Q} \mid -1 \leqslant z \leqslant 1\}$

c) $x \star y = x$ dans $E = \{1, 2, 3, 4\}$

Définition: On dit qu'un groupe $(G,\star)$ est **d'ordre fini** s'il contient un nombre fini d'éléments.
On appelle **ordre** d'un groupe d'ordre fini le nombre de ses éléments.

Exemple 7: Dans l'exemple précédent (page 13), le groupe $(E \times E, \star)$ est d'ordre 4.

Exercice 2.4: **Suite de l'exercice 1.9**
On se donne les applications de $\mathbb{R}^\star$ dans $\mathbb{R}^\star$ suivantes :

$$i(x) = x \qquad f(x) = -x \qquad g(x) = \frac{1}{x} \qquad h(x) = -\frac{1}{x}.$$

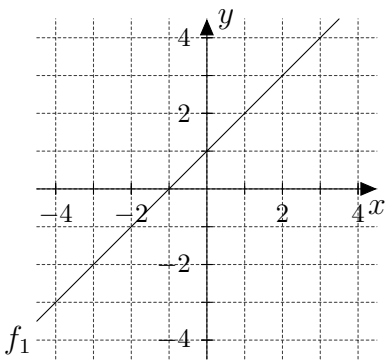
Soit $E = \{i, f, g, h\}$ et considérons la composition des fonctions $\circ$ sur E.

A-t-on une structure de groupe ? Si oui, précisez son ordre.

Exercice 2.5: Soit E l'ensemble de toutes les fonctions f_b de $\mathbb{R}$ dans $\mathbb{R}$ définies par :

$$f_b(x) = x + b \qquad \text{où } b \in \mathbb{Z}$$

a) On a représenté ci-dessous $f_1(x) = x+1$. Compléter ce graphe avec quelques autres éléments de E.



b) Montrer que $(E,\circ)$ est un groupe.

Exercice 2.6: Soit $E = \left\{(a\,;b) \in \mathbb{R}^2 \mid a^2 + b^2 = 1\right\}$ muni de l'opération $\star$:

$$(a\,;b) \star (c\,;d) = (ac - bd\,;ad + bc)$$

Montrer alors que $(E,\star)$ est un groupe.

Exercice 2.7: On considère l'ensemble

$$E = \left\{a + b\sqrt{2} \mid (a\,;b) \in \mathbb{Q}^2 \text{ avec } a \text{ et } b \text{ non nuls simultanément}\right\}$$

On munit cet ensemble de la multiplication habituelle.

a) Montrer que si $x = 1 + \frac{1}{2}\sqrt{2}$ et que $y = \frac{1}{3} + 2\sqrt{2}$ alors :

$$x \cdot y = \frac{7}{3} + \frac{13}{6}\sqrt{2}$$

Comme vous pouvez vous en douter, $(E,\cdot)$ est un groupe. Pour gagner en efficacité, nous ne montrerons pas que l'opération est interne et associative. Par contre :

b) Déterminer l'élément neutre.

c) Montrer que tout élément de E admet un élément symétrique.

3

Quelques groupes célèbres

3.1 Groupe fini de permutations

3.1.1 Exemple introductif

Soit $E = \{1, 2, 3, 4\}$. Considérons les 4-uplets $(1, 2, 3, 4)$ et $(2, 3, 4, 1)$. Soit σ l'application de E dans E telle que :

$$\sigma(1) = 2 \qquad \sigma(2) = 3 \qquad \sigma(3) = 4 \qquad \sigma(4) = 1$$

σ est une permutation des éléments de E et on peut la représenter par le tableau suivant :

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

Si l'on considère les triplets $(1, 2, 4)$ et $(4, 1, 2)$, on peut définir l'application τ de E dans E par :

$$\tau(1) = 4 \qquad \tau(2) = 1 \qquad \tau(3) = 3 \qquad \tau(4) = 2.$$

τ est aussi une permutation des éléments de E et on la représente par

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \text{ ou } \begin{pmatrix} 1 & 2 & 4 \\ 4 & 1 & 2 \end{pmatrix}$$

3.1.2 Permutations finies

Définition: Soit E un ensemble fini quelconque et considérons σ une application de E dans E ; σ est appelée **permutation** de E si σ est une bijection de E dans E.

On présentera volontiers une permutation sous la forme suivante :

$$\sigma = \begin{pmatrix} e_1 & e_2 & \dots & e_m & e_n \\ \sigma(e_1) & \sigma(e_2) & \dots & \sigma(e_m) & \sigma(e_n) \end{pmatrix}$$

En omettant éventuellement d'y faire apparaître les e_i pour lesquelles $\sigma(e_i) = e_i$.

Théorème: Soit E un ensemble fini d'ordre n et soit S_E l'ensemble de toutes les permutations de E ; alors $(S_E,\circ)$ est un groupe fini d'ordre $n!$.

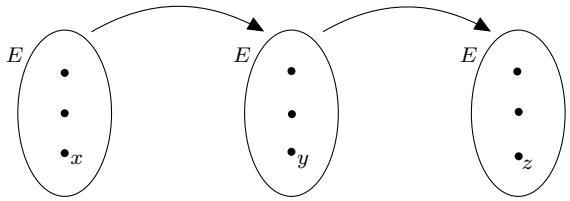
Preuve: En exercice

Exercice 3.1: Compléter la preuve du théorème précédent :

Appelons σ, τ et ρ, 3 permutations de .....

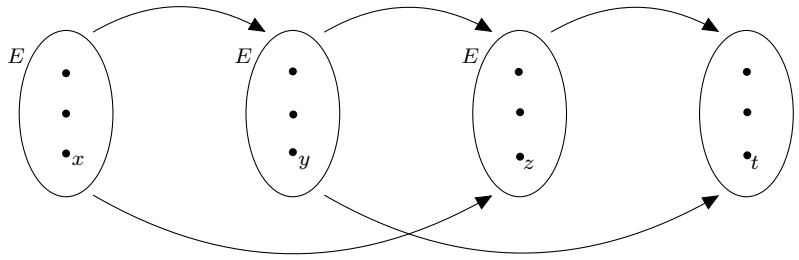
a) Montrons que la loi de composition $\circ$ est .....

La loi $\circ$ est interne $\iff \tau \circ \sigma \in$ .....
$\iff \tau \circ \sigma$ est une ..... de E



Comme σ et τ sont des ..... de E, tout $z \in E$ est l'image par τ d'un unique .. $\in E$ qui lui-même est l'image par σ d'un unique .. $\in E$. Ainsi $\tau \circ \sigma$ est donc bien une ..... de E.

b) Montrons que la loi de composition $\circ$ est .....



À montrer que $\forall x \in E, \big((\rho \circ \tau) \circ \sigma\big)(x) =$ .....

- $\big((\rho \circ \tau) \circ \sigma\big)(x) =$ .....
- $\big(\rho \circ (\tau \circ \sigma)\big)(x) =$ .....

c) L'existence de l'élément neutre de ..... L'identité : $id : E \to E$ vérifiant $id(x) = ..\ \ \forall x \in E$ est clairement l'élément neutre.

d) Tout élément de ..... admet un élément ..... Si σ est une ..... de E, c'est une bijection de E. On peut donc définir ${}^r\sigma$, ... de σ qui sera elle aussi une ..... de E. On a alors :

$$..... \circ ..... = ... \circ ..... = ...$$

e) $(S_E\,, \circ)$ est d'ordre $n!$
On rappelle que E est d'ordre n. Disons :

$$E = \{e_1\,; e_2\,; e_3\,; \ldots\,; e_{n-1}\,; e_n\}\,.$$

Observons le nombre de possibilités d'associer chaque e_i à l'aide d'une permutation σ dans le tableau suivant :

$$\sigma = \begin{pmatrix} e_1 & e_2 & e_3 & \cdots\cdots & e_{n-1} & e_n \\ \cdots & \cdots & \cdots & & \cdots & \cdots \end{pmatrix}$$

Remarque: Soit $E = \{1, 2, \ldots, n\}$. On note alors $S_E = S_n$.

Exemple 1: Considérons S_3.

a) Combien y a-t-il d'éléments dans S_3 ?

b) Compléter les éléments de S_3 :

- **L'identité** : $id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
- **les transpositions** :

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ ... & ... & ... \end{pmatrix}$$

- **les cycles** :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ ... & ... & ... \end{pmatrix}$$

c) Calculer et comparer les compositions $\sigma_1 \circ \tau_1$ et $\tau_1 \circ \sigma_1$;

d) S_3 est-il un groupe abélien ?

e) Montrer que σ_2 est l'inverse de σ_1

f) Compléter alors la table composition de S_3

$\circ$ ↙	id	σ_1	σ_2	τ_1	τ_2	τ_3
id	id	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	id		τ_3	τ_1
σ_2	σ_2		σ_1	τ_3	τ_1	τ_2
τ_1	τ_1		τ_2	id	σ_2	σ_1
τ_2	τ_2	τ_1	τ_3	σ_1	id	σ_2
τ_3	τ_3	τ_2	τ_1	σ_2	σ_1	id

Exercice 3.2: Soit les permutations α et β suivantes

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 5 & 4 & 1 \end{pmatrix} \text{ et } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 6 & 2 & 4 \end{pmatrix}$$

Calculer $\alpha \circ \beta, \beta \circ \alpha, {}^r\alpha, {}^r\beta, {}^r(\alpha \circ \beta), {}^r(\beta \circ \alpha)$.

Exercice 3.3: Montrer que $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$ avec

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}, \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

Exercice 3.4: Soit le sous-ensemble $R = \{id, \sigma_1, \sigma_2\}$ de S_3. Montrer que R admet lui-aussi une structure de groupe.
On dira alors que R est un sous-groupe de S_3.

Exercice 3.5: Trouver tous les éléments de S_1 et S_2. Construire ensuite leur table de composition.

3.2 Classes de restes modulo n

Considérons dans $\mathbb{Z}$ la division par 3. Cette division n'est pas une opération interne de $\mathbb{Z}$. Par contre, considérons le reste de la division euclidienne de tout nombre entier par 3.

Par exemple : $6 = 2 \cdot 3 + 0 \quad 7 = 2 \cdot 3 + 1 \quad -4 = -2 \cdot 3 + 2 \quad$ etc...

Si $a \in \mathbb{Z}$, on peut écrire de manière unique $a = p \cdot 3 + q$ avec $0 \leqslant q < 3$. Cela revient à dire que $a - q$ est divisible par 3.

Par extension, on dira que x est **congru modulo 3** à y si et seulement si $x - y$ est divisible par 3 dans $\mathbb{Z}$. On note $x \equiv y \pmod 3$.

Définition: Soit $n \in \mathbb{N}^\star$ et $x, y \in \mathbb{Z}$. On dit que x est *congru à y modulo n* si $x - y$ est divisible par n.

On utilise la notation $x \equiv y \pmod n$. Autrement dit,

$$x \equiv y \pmod n \quad \Leftrightarrow \quad x - y = k \cdot n \qquad (\text{avec } k \in \mathbb{Z})$$

Exemple 2: Si l'on revient à l'exemple précédent, on constate que les restes possibles de la division par 3 sont 0, 1 ou 2. Par conséquent, tout entier sera donc congru modulo 3 à 0, 1 ou 2.

Proposition: Soit $n \in \mathbb{N}^\star$ et $a \in \mathbb{Z}$; a est congru modulo n à un unique nombre entier y tel que $0 \leqslant y \leqslant n-1$.

Preuve:

Définition: On note $C(a) = \overline{a}$ l'ensemble des éléments congrus à a modulo n. $C(a)$ est la **classe de** $a \pmod{n}$.

Exemple 3: Si $n = 4$, on a

$$
\begin{array}{lllll}
C(0) & = & \overline{0} & = & \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\
C(1) & = & \overline{1} & = & \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\
C(2) & = & \overline{2} & = & \{\ldots, -6, -2, 2, 6, 10, \ldots\} \\
C(3) & = & \overline{3} & = & \{\qquad\qquad\qquad\qquad\} \\
C(4) & = & \overline{4} & = & \{\ldots, -4, 0, 4, 8, 12, \ldots\} \quad = \\
C(5) & = & \overline{5} & = & \{\ldots, -3, 1, 5, 9, 13, \ldots\} \quad =
\end{array}
$$

Si l'on considère alors des éléments de la classe $\overline{1}$ et si on les somme avec des éléments de la classe $\overline{3}$ deux à deux, que constate-t-on ?

$$1+3=4 \in \qquad -7+3=4 \in \qquad 5+11=16 \in$$

Il semble que le résultat appartienne toujours à la même classe ...
On aurait alors envie d'écrire :

$$\overline{1}+\overline{3}=\overline{1+3}=\overline{4}=\overline{0}$$

Qu'en est-il avec la multiplication ?

$$1 \cdot 3=3 \in \qquad -7 \cdot 3=-21 \in \qquad 5 \cdot 11=55 \in$$

Il semble que le résultat appartienne toujours à la même classe ...
On aurait alors envie d'écrire

$$\overline{1} \cdot \overline{3}=\overline{1 \cdot 3}=\overline{3}$$

Nous allons montrer ces deux résultats en toute généralité.

Proposition: Soit $n \in \mathbb{N}^{\star}$.
Si dans $\mathbb{Z}$ on a $x \equiv x' \pmod{n}$ et $y \equiv y' \pmod{n}$, alors :

$$x+y \equiv x^{'}+y^{'} \pmod{n}$$
$$x \cdot y \equiv x' \cdot y' \pmod{n}$$

Preuve:

Constatation: On peut donc définir sur les classes modulo n $\quad (0 \leqslant a, b \leqslant n-1)$

- une **addition** en posant : $\quad \overline{a} + \overline{b} = \overline{a+b}$.
- une **multiplication** en posant : $\quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Si l'on note $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, alors l'addition et la multiplication définies ci-dessus sont toutes les deux des opérations internes dans $\mathbb{Z}_n$.

Exemple 4: Un exemple de la vie courante est le suivant : considérons seulement les minutes d'une montre. Celles-ci varient entre 0 et 59. Lorsque l'aiguille passe à 60, elle désigne aussi 0. Ainsi de suite : 61 s'écrit aussi 1, 62 s'écrit aussi 2, ... Cela correspond donc à l'ensemble $\mathbb{Z}_{60}$.
On peut aussi additionner des minutes : 50 minutes + 15 minutes font 65 minutes qui s'écrivent aussi 5 minutes. Continuons avec l'écriture dans $\mathbb{Z}_{60}$ par exemple : $\overline{135} + \overline{50} = \overline{185} = \overline{5}$.
Remarquons que si l'on écrit d'abord $\overline{135} = \overline{15}$ et $\overline{50} = \overline{-10}$, alors le calcul se simplifie en $\overline{135} + \overline{50} = \overline{15} + (\overline{-10}) = \overline{5}$.
C'est le fait que l'addition soit bien définie qui justifie que l'on trouve toujours le même résultat.

Exemple 5: Proposer la table d'addition sur $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, puis celle de la multiplication sur $\mathbb{Z}_3^*$.

Exercice 3.6: Proposer la table d'addition sur $\mathbb{Z}_4 = \{\overline{0}, \ldots, \overline{3}\}$

Exercice 3.7: Proposer la table de multiplication sur $\mathbb{Z}_5^\star$ et sur $\mathbb{Z}_4^\star$. Quelles singularités observez-vous sur ce dernier tableau ?

Exemple 6: Montrer que l'addition dans $\mathbb{Z}_n$ est associative

Exercice 3.8: Montrer que la multiplication dans $\mathbb{Z}_n$ est associative.

Exercice 3.9:

a) Montrer que l'ensemble $E = \{1\,;2\,;4\}$ muni de la multiplication modulo 7 forme un groupe.

b) Qu'en est-il si on munit E de la multiplication modulo 5 ?

Théorème: Soit $n \in \mathbb{N}^\star$; alors $(\mathbb{Z}_n\,,+)$ est un groupe abélien.

Preuve:

Théorème: Soit n un nombre premier ; alors $(\mathbb{Z}_n^\star, \cdot)$ est un groupe abélien.

Preuve: *Il faudrait montrer que pour tout n premier, l'inverse modulo n existe toujours. Ce résultat n'est pas très difficile, mais demande de mettre en place des nouveaux outils mathématiques comme le théorème de Bézout.*

3.3 Matrices de dimensions 2

Définition: Une **matrice** 2×2 est la donnée d'un tableau de la forme :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

avec a, b, c, d des nombres quelconques.
L'ensemble de ces matrices se note $M_2(\mathbb{R})$.

3.3.1 Groupe additif

Définition: Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, N = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in M_2(\mathbb{R})$, on définit **la somme de deux matrices** de la manière suivante

$$M + N = \begin{pmatrix} a+x & b+y \\ c+z & d+t \end{pmatrix}$$

On définit alors naturellement la **matrice nulle** par $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Exemple 7: Si $M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ et $N = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$, on a :

$$M + N = \begin{pmatrix} \cdots & \cdots \\ \cdots & \cdots \end{pmatrix}$$

Définition: Soit $M \in M_2(\mathbb{R})$ et $\lambda \in \mathbb{R}$. On définit la **multiplication scalaire matricielle** de la manière suivante

$$\lambda \cdot \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} = \begin{pmatrix} \lambda m_1 & \lambda m_2 \\ \lambda m_3 & \lambda m_4 \end{pmatrix}$$

Exemple 8: Si $M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ et $\lambda = 2$, on a :

$$2 \cdot M = \begin{pmatrix} \cdots & \cdots \\ \cdots & \cdots \end{pmatrix}$$

Remarque: Cette définition nous permet alors de définir la **soustraction de deux matrices** de la manière suivante : si $M, N \in M_2(\mathbb{R})$

$$M - N = M + (-N) = M + ((-1) \cdot N)$$

Exercice 3.10: Posons $A = \begin{pmatrix} 1 & 2 \\ -3 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$. Calculer

a) $A + A, A + B, A - B, B - A$

b) $2A, 3A, -5B$

Théorème: $M_2(\mathbb{R})$ muni de $+$ est un groupe abélien.

Preuve:

3.3.2 Groupe multiplicatif

Définition: Soit A et B deux matrices 2×2 ; on définit le **produit matriciel** $A \cdot B = C$ de la manière suivante :

$$A \cdot B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bt \\ cx + dz & cy + dt \end{pmatrix} = C$$

Exemple 9: Si $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}$, on a :

$$AB = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 \cdot 5 + 2 \cdot 7 & 1 \cdot 6 + 2 \cdot 8 \\ 3 \cdot 5 + 4 \cdot 7 & 3 \cdot 6 + 4 \cdot 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix}$$

$BA =$

Constatation: Le produit matriciel n'est donc en général **pas commutatif**.

Exemple 10: Si $A = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} -2 & 2 \\ 1 & -1 \end{pmatrix}$, on a $AB = \begin{pmatrix} \cdots & \cdots \\ \cdots & \cdots \end{pmatrix}$.

Constatation: Le produit de deux éléments non nuls peut être nul.

Exercice 3.11: Posons $A = \begin{pmatrix} 1 & 2 \\ -3 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$. Calculer

a) AB, BA, ABA

b) A^2, A^3

Définition: Soit

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Cette matrice est appelée **la matrice identité**.

Remarque:

- On constate de manière évidente que si $A \in M_2(\mathbb{R})$, on a $I_2 \cdot A = A \cdot I_2 = A$.
  Cette matrice identité est donc l'**élément neutre** pour la multiplication des matrices.
- On vérifie par le calcul que le produit matriciel est **associatif**, i.e. si A, B, C sont trois matrices, nous avons :

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C$$

On peut donc définir la puissance d'une matrice de la manière suivante :

Définition: Soit A une matrice 2×2 ; on définit **l'élévation à la puissance** par la formule récurrente suivante :

$$A^n = A(A^{n-1}) \quad \text{avec } n \geqslant 2, n \in \mathbb{N}$$

On dit que A est **d'ordre fini** s'il existe un nombre $n \in \mathbb{N}$ de sorte que

$$A^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Exercice 3.12: On considère les 4 matrices suivantes :

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

Déterminer l'ordre de chacune de ces matrices.

Exercice 3.13: Posons $E = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} ; \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} ; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} ; \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}$.

Montrer que E, muni de la multiplication matricielle est un groupe.

Exercice 3.14: Posons $A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$.

a) À l'aide de votre formulaire, montrer que :

$$A^2 = \begin{pmatrix} \cos(2\alpha) & -\sin(2\alpha) \\ \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

b) Calculer A^3 puis A^4

c) En déduire une formule A^n pour $n \in \mathbb{N}$. Saurez-vous la prouver ?

Question: $M_2(\mathbb{R})$ muni de sa multiplication est-il un groupe ?

Par ce qui précède, l'opération interne, l'élément neutre et l'associativité sont acquis. Qu'en est-il de l'inverse ?
Pour ce faire, nous avons besoin d'une définition supplémentaire.

Définition: Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$; on appelle **déterminant** de M le nombre :

$$\det M = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

Exemple 11: Si $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, on a $\det A = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = \ldots\ldots$

Exercice 3.15: Montrer que si $M, N \in M_2(\mathbb{R})$, alors $\det(MN) = \det(M) \cdot \det(N)$.

Ce résultat peut paraître étonnant à la vue de la définition du produit matriciel qui ne semble pas du tout intuitive !

Définition: Soit $M \in M_2(\mathbb{R})$ avec $\det M \neq 0$. L'ensemble de toutes ces matrices se note $GL_2(\mathbb{R})$.

Théorème: Si $M \in GL_2(\mathbb{R})$, il existe une matrice M^{-1}, appelée **inverse de** M de sorte que $M \cdot M^{-1} = M^{-1} \cdot M = I_2$.

Preuve:

Exemple 12: Si $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, on a $\det A = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 1 \cdot 4 - 2 \cdot 3 = -2$.
On en déduit $A^{-1} = -\frac{1}{2}\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix}$.

Exercice 3.16: Posons $A = \begin{pmatrix} 1 & 2 \\ -3 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$. Calculer A^{-1}, B^{-1}

Remarque: La notion d'inverse nous permet alors de définir $A^{-n} = (A^n)^{-1}$ si $n \in \mathbb{N}^\star$. On a donc A^n défini pour tout $n \in \mathbb{Z}$ en posant $A^0 = I_2$
Nous pouvons donc conclure par le théorème suivant :

Théorème: $GL_2(\mathbb{R})$ muni de la multiplication matricielle est un groupe.

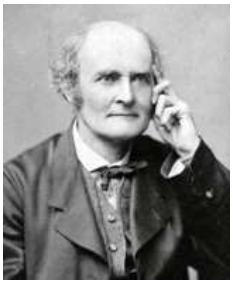
Remarques: On constate que $(M_2(\mathbb{R}),+)$ est un groupe, alors que $(M_2(\mathbb{R}),\cdot)$ ne l'est pas. Il faut dans ce dernier cas se restreindre à $GL_2(\mathbb{R})$, appelé **groupe linéaire** de dimension 2.

Soit $A \in GL_2(\mathbb{R})$, alors $\{A^n \mid n \in \mathbb{Z}\}$, muni de la multiplication, admet aussi une structure de groupe. *Mais ceci est une autre histoire...*

4

Table de Cayley et isomorphisme de groupes

Définition: Soit un ensemble $E = \{x_1 ; \ldots ; x_n\}$ muni d'une opération $\star$.
On appelle **table de Cayley**, le tableau carré de n lignes et n colonnes obtenu en inscrivant à la i-ème colonne et à la j-ième ligne l'élément $x_i \star x_j$.



Arthur Cayley
mathématicien britannique
(1821-1895)

$\star\swarrow$	x_1	x_2	$\cdots$	x_i	$\cdots$	x_n
x_1						
x_2						
$\vdots$						
x_j				$x_i \star x_j$		
$\vdots$						
x_n						

Exemple 1: Soit $E = \{1 ; 2 ; 3 ; 4\}$ muni des opérations $\star$ définies ci-dessous. Compléter les tables de Cayley. Que constatez-vous ?

a) $a \star b = \text{PPMC}(a ; b)$.

$\star\swarrow$	1	2	3	4
1				
2				
3				
4				

b) $a \star b = \text{PGDC}(a ; b)$.

$\star\swarrow$	1	2	3	4
1				
2				
3				
4				

Exercice 4.1: On munit l'ensemble $E = \{a\,;b\,;c\,;d\}$ d'une loi de composition interne, dont la table de Cayley est :

$\overset{\star}{\swarrow}$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	d	c	b	a
d	c	d	a	b

a) Cette loi possède-t-elle un élément neutre ? Lequel ?

b) Chaque élément, admet-il un symétrique ? Préciser le symétrique de c.

c) Cette loi est-elle commutative ?

d) Pour vérifier que $\star$ est associative, vous devrez contrôler que

$$(x \star y) \star z = x \star (y \star z),\ \forall x,\ y \text{ et } z \in E.$$

Contrôlez-en quelques-uns par vous-même puis estimez le temps nécessaire pour effectuer toutes les vérifications.

e) $(E,\star)$, semble-t-il être un groupe ?

f) Et si la table était de taille 8×8. Que deviendrait l'estimation en **d)** ?

Exercice 4.2: Justifier l'affirmation suivante :

La table de Cayley d'un groupe fini a une particularité : c'est toujours un tableau carré dans lequel dans chaque ligne et chaque colonne apparait une et une seule fois chaque élément du groupe.

Idée : Supposons que G soit un groupe fini d'ordre n muni de l'opération interne $\star$. Sa table de Cayley consistera en :

$\overset{\star}{\swarrow}$	a_1	a_2	$\cdots$	a_i	$\cdots$	a_n
a_1	b_{11}	b_{12}	$\cdots$	b_{1i}	$\cdots$	b_{1n}
a_2	b_{21}	b_{22}	$\cdots$	b_{2i}	$\cdots$	b_{2n}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_i	b_{i1}	b_{i2}	$\cdots$	b_{ii}	$\cdots$	b_{in}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_n	b_{n1}	b_{n2}	$\cdots$	b_{ni}	$\cdots$	b_{nn}

Il s'agit alors de montrer $\forall i,\ 1 \leqslant i \leqslant n$, l'existence de deux indices j, k différents vérifiant que $b_{ij} = b_{ik}$ n'est pas possible. Cela montrera donc la propriété sur chaque ligne. Il s'agira encore de raisonner sur les colonnes.

Exercice 4.3: On considère l'ensemble $E = \{a\,;b\,;c\,;d\}$ muni de la loi de composition interne, dont la table de Cayley est :

$\star\swarrow$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

a) Montrer que la loi de composition $\star$ n'est pas associative.

b) Qu'en déduisez-vous à propos de l'exercice précédent ?

Exercice 4.4: Compléter les deux tables suivantes de telle sorte que $E = \{r\,;s\,;t\,;u\}$ muni des deux lois $\star$ forment un groupe

a)

$\star\swarrow$	r	s	t	u
r	s	r		
s	r	s	t	u
t		t	s	
u		u		s

b)

$\star\swarrow$	r	s	t	u
r	r	s	t	u
s	s	t		
t	t			
u	u	r		

Exemple 2: **Groupe d'ordre 1 :**
On considère $G = \{e\}$ muni d'une loi de composition $\star$.
À l'aide d'une table de Cayley, montrer qu'il existe une et une seule façon de définir ainsi un groupe.

Ce groupe porte le nom de **groupe trivial**.

Exercice 4.5: **Groupe d'ordre 2 :**
On considère $G = \{e\,;a\}$ muni d'une loi de composition $\star$ où e est l'élément neutre.

a) À l'aide d'une table de Cayley, déterminer le nombre de façons de définir ainsi un groupe.

b) A-t-on déjà croisé (dans les exemples ou les exercices) des exemples de groupe d'ordre 2. Comparer alors leur table de Cayley.

Exercice 4.6: **Groupe d'ordre 3 :**
On considère $G = \{e\,;a\,;b\}$ muni d'une loi de composition $\star$ où e est l'élément neutre.

a) À l'aide d'une table de Cayley, déterminer le nombre de façons de définir ainsi un groupe.

b) A-t-on déjà croisé (dans les exemples ou les exercices) des exemples de groupe d'ordre 3. Comparer alors leur table de Cayley.

Exercice 4.7: **Groupe d'ordre 4 :**
On considère $G = \{e\,;a\,;b\,;c\}$ muni d'une loi de composition $\star$ où e est l'élément neutre.

a) À l'aide des tables de Cayley proposées ci-dessous montrer, en tentant de les compléter, que seules 2 tables différentes (à permutation des éléments de G près) sont possibles.

$\star\swarrow$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

$\star\swarrow$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			

$\star\swarrow$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b			
c	c			

$\star\swarrow$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Dans ce dernier cas de figure, il est recommandé de recopier, le nombre de fois nécessaire, ce tableau dans votre cahier afin de tenter de les compléter de différentes manières.

b) A-t-on déjà croisé (dans les exemples ou les exercices) des exemples de groupe d'ordre 4. Comparer alors leur table de Cayley.

Exercice 4.8: Montrer que les 2 tables suivantes décrivent un même groupe d'ordre 4 :

$\overset{\star}{\swarrow}$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\overset{\star}{\swarrow}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Définition: L'**ordre d'un élément** a d'un groupe est le plus petit nombre entier positif m tel que $\underbrace{a \star a \star \cdots \star a}_{m \text{ fois}} = e$. Si aucun m de la sorte n'existe, a est dit d'ordre infini.

Exemple 3: On considère les 2 tables suivantes :

$\overset{\star}{\swarrow}$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\overset{\star}{\swarrow}$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Montrer que même si on permute lignes et colonnes de la première table, il n'est pas possible d'obtenir la deuxième.

Définition: Deux groupes $(G,\star)$ et $(E,\bullet)$ sont dits **isomorphes** si une table de Cayley de $(G,\star)$ peut être transformée en une table de Cayley de $(E,\bullet)$ terme à terme.

Remarque: Ceci traduit bien l'idée d'une **même structure** comme le dénote l'étymologie de ce terme : *iso* signifiant *même* et *morphisme* étant issu du grec et signifiant *forme*.
Cette notion d'isomorphisme est commune à toutes les parties des mathématiques. Dès qu'on crée une structure, on veut pouvoir la faire communiquer avec une autre déjà étudiée. On pourra ainsi transférer des propriétés (calculs) de l'une pour les appliquer dans l'autre.
Par exemple, les simplifications des écritures vectorielles :

$$\vec{a} - \frac{1}{2}\vec{b} + 2\vec{a} - 3\vec{b}$$

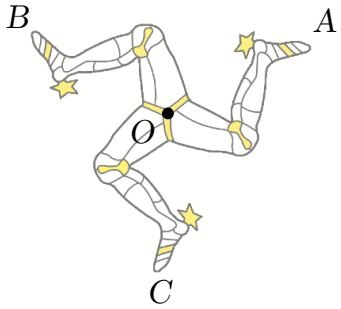
se manipulent comme les simplifications du calcul littéral :

$$a - \frac{1}{2}b + 2a - 3b = 3a - \frac{7}{2}b$$

Exercice 4.9: Dans les exercices qui précèdent, cherchez des groupes (différents) d'ordre 2, 3 et 4 qui sont isomorphes.

Exercice 4.10:

Un triskèle, représentant trois jambes, est présent sur le drapeau de l'île de Man depuis 1931.
À l'origine, il est probable que ce symbole représentait, dans l'iconographique celtique, les trois points du mouvement vertical du soleil : le lever, le zénith et le coucher.
Considérons l'ensemble $E = \{A\,;B\,;C\}$ des sommets du triskèle représenté ci-dessous.



Considérons l'ensemble $S = \{r_0\,;r_1\,;r_2\}$ des bijections de l'ensemble E vers lui-même définies par :

- $r_0(A) = A \quad , \quad r_0(B) = B \quad , \quad r_0(C) = C\,;$
- $r_1(A) = B \quad , \quad r_1(B) = C \quad , \quad r_1(C) = A\,;$
- $r_2(A) = C \quad , \quad r_2(B) = A \quad , \quad r_2(C) = B.$

a) À quoi correspondent géométriquement ces bijections ?

b) Montrer que $(S,\circ)$ est un groupe d'ordre 3.

Exercice 4.11: Soit $m \in \mathbb{N}_+^\star$ et posons $S = \{0, 1, 2, \ldots, m-1\}$.
Définissons l'opération $\star$ sur S de la manière suivante :

$$\begin{cases} a \star b = a + b & \text{si } a + b < m, \\ a \star b = r & \text{si } a + b = m + r,\ 0 \leqslant r < m. \end{cases}$$

Montrer alors que $(S,\star)$ est un groupe.

Indication : Commencez par étudier la table de Cayley pour $m = 4$.

5 Sous-groupe

Définition: Soit H un sous-ensemble non vide du groupe $(G,\star)$. On dit que H est un **sous-groupe** de $(G,\star)$ si $(H,\star)$ est lui-même un groupe.

Exemple 1: $(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Q},+)$, car $\mathbb{Z} \subset \mathbb{Q}$ et $(\mathbb{Z},+)$ est lui-même un groupe.

Remarque: Tout groupe $(G,\star)$ ayant plus de deux éléments distincts possède toujours deux sous-groupes au moins, à savoir G lui-même et le groupe formé du seul élément neutre.

Théorème: Soit $(G,\star)$ un groupe et H un sous-ensemble non vide de G ; alors H est un sous-groupe de $(G,\star)$ si et seulement si

a) $\star$ est une opération interne dans H $\qquad (\forall x, y \in H,\ x \star y \in H\ )$

b) le symétrique de tout élément de H est dans H, $\qquad (x \in H \Rightarrow x' \in H\ )$

Preuve:

Exemple 2:

- Considérons l'ensemble $2\,\mathbb{Z}$ des nombres entiers pairs ; alors $2\,\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}\,,+)$. En effet les deux critères sont satisfaits car :
  - **a)** la somme de deux nombres pairs est paire ;
  - **b)** l'opposé d'un nombre pair est pair.
- À contrario, si $\mathbb{Z}-2\,\mathbb{Z}$ est l'ensemble des nombres entiers impairs, alors $\mathbb{Z}-2\,\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z}\,,+)$ car par exemple 1 et 3 sont dans $\mathbb{Z}-2\,\mathbb{Z}$, mais $1+3=4$ ne l'est pas ; il ne s'agit donc pas d'une opération interne.

Exercice 5.1: Démontrer que l'intersection de deux sous-groupes d'un groupe $(G,\star)$ est aussi un sous-groupe de $(G,\star)$.

Exercice 5.2: Montrer, à l'aide d'un exemple bien choisi, que la réunion de deux sous-groupes d'un groupe $(G,\star)$ n'est pas forcément un sous-groupe de $(G,\star)$ (utiliser l'exercice 1.9 pour *construire* un exemple).

Exercice 5.3: Soit $\mathcal{F}$ l'ensemble de toutes les applications de $\mathbb{R}$ dans $\mathbb{R}$ et considérons la composition des applications $\circ$. $(\mathcal{F},\circ)$ est-il un groupe ? Si non, donner le plus grand sous-ensemble $\mathcal{E}$ de $\mathcal{F}$ tel que $(\mathcal{E},\circ)$ soit un groupe.

Exercice 5.4: Dans le groupe $(\mathbb{R}\,,+)$, on considère $S=\left\{x+y\sqrt{2}\mid x,y\in\mathbb{Q}\right\}$. $(S,+)$ est-il un sous-groupe de $(\mathbb{R}\,,+)$?

Exercice 5.5: Dans le groupe multiplicatif $(\mathbb{R}^\star\,,\cdot)$, on considère l'ensemble :

$$\mathbb{S}=\{x+y\sqrt{2}\mid x,y\in\mathbb{Q},x\text{ et }y\text{ non simultanément nuls}\}$$

$(\mathbb{S},\cdot)$ est-il un sous-groupe de $(\mathbb{R}^\star;\cdot)$?

Exercice 5.6: Dans le groupe $(\mathbb{R}^2\,,+)$ muni de l'addition habituelle :

$$(x\,;y)+(a\,;b)=(x+a\,;y+b)$$

on considère les sous-ensembles suivants :

- **a)** $E=\{(x\,;y)\mid 2x+3y=0\}$
- **b)** $E=\{(x\,;y)\mid x+y=1\}$
- **c)** $E=\{(4x+3y\,;y)\mid x,y\in\mathbb{R}\}$
- **d)** $E=\{(2x+y\,;y-x)\mid x,y\in\mathbb{R}\}$

Chaque $(E,+)$ est-il un sous-groupe de $(\mathbb{R}^2\,,+)$?

Exercice 5.7: Dans le groupe $(\mathbb{R}^2, \bullet)$ muni de la multiplication :

$$(x\,;y) \bullet (a\,;b) = (xa - yb\,; xb + ya)$$

on considère les sous-ensembles suivants :

a) $E = \{(x\,;0) \mid x \in \mathbb{R}^\star\}$

b) $E = \{(2x\,;x) \mid x \in \mathbb{R}^\star\}$

c) $E = \{(1\,;x) \mid x \in \mathbb{R}\}$

d) $E = \{(0\,;x) \mid x \in \mathbb{R}^\star\}$

e) $E = \{(-x\,;x) \mid x \in \mathbb{R}^\star\}$

Chaque $(E,\bullet)$ est-il un sous-groupe de $(\mathbb{R}^2, \bullet)$?

Exemple 3: Soient $(G,\star)$ un groupe quelconque, $g \in G$ et $n \in \mathbb{N}$.
Posons :
$g^n = \underbrace{g \star g \star .... \star g}_{n \text{ fois}}$ (avec $g^0 = e$ élément neutre) et

$g^{-n} = \underbrace{g^{-1} \star g^{-1} \star .... \star g^{-1}}_{n \text{ fois}}$ (avec g^{-1} élément symétrique de g).

On pose par définition la relation suivante : $g^n \star g^m = g^{n+m}$.

Considérons alors $H = \{g^n \mid n \in \mathbb{Z}\} \subset G$. On montrera que $(H,\star)$ est un sous-groupe de $(G,\star)$.

Définition: Soit $(G,\star)$ un groupe et considérons $g \in G$; soit $H = \{g^n \mid n \in \mathbb{Z}\}$. Le sous-groupe $(H,\star)$ s'appelle le **groupe engendré par** g et g s'appelle le **générateur de** H. On note $H =< g >$.

Exemple 4: $< 2 >= \{..., -4, -2, 0, 2, 4, ...\}$ est un sous-groupe de $(\mathbb{Z}, +)$.

Exemple 5: Soit $g \in G$ avec $(G,\star)$ un groupe tel que $g^3 = e$.
On pose $H = \{e, g, g^2\}$. Montrer alors que $(H,\star)$ est bien un groupe (on montrera en particulier que $g^{-1} = g^2$).

Considérons $g_1, g_2, \ldots, g_p \in G$ avec $g_i \neq g_j$ si $i \neq j$.
Nous pouvons alors construire tous les produits de la forme

$$g_k^{n_k} \star g_l^{n_l} \star \cdots \star g_z^{n_z} \quad \text{avec } k, l, \ldots, z \in \{1, 2, \ldots, p\}.$$

Soit H l'ensemble de tous ces éléments. On a alors le résultat suivant (sans démonstration)

Théorème: Soit $(G,\star)$ un groupe et $g_1, g_2, \ldots, g_p \in G$ avec $g_i \neq g_j$ si $i \neq j$, et posons H défini comme ci-dessus.
$(H,\star)$ est alors un sous-groupe de $(G,\star)$.

Définition: Soit $(G,\star)$ un groupe et $g_1, g_2,\ldots..,g_p \in G$ avec $g_i \neq g_j$ si $i \neq j$ et posons H défini comme ci-dessus.

$(H,\star)$ s'appelle le **groupe engendré par** $g_1, g_2, \ldots, g_p$ et les éléments $g_1, g_2, \ldots, g_p$ s'appellent les **générateurs de** H. On note $H =< g_1, g_2, \ldots, g_p >$.

Un produit de la forme $g_k^{n_k} \star g_l^{n_l} \star \cdots \star g_z^{n_z}$ s'appelle un **mot de** H.

Exemple 6: $< 2, 3 >= \{2^\alpha 3^\beta \mid \alpha, \beta \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Q}^\star, \cdot)$.

Exemple 7: Soit $g \in G$ et $h \in G$ de sorte que $g^3 = h^2 = g \star h = e$.
On a $< g, h >= \{e, g, g^2, h, h \star g\}$. En effet, par exemple :
$g^2 \star h = g \star (g \star h) = g \star e = g$, ou
$(h \star g) \star h = h \star (g \star h) = h \star e = h$.

Remarque: Si $(G,\star)$ est un groupe et $g_1, g_2, \ldots, g_j$ un système générateur de H, on note $g_p^{n_p}\, g_q^{n_q}$ le composé $g_p^{n_p} \star g_q^{n_q}$

Exercice 5.8: Soit $(G,\star)$ un groupe et $g \in G$. Posons $H =< g >$. Montrer que $(H,\star)$ est un sous-groupe de $(G,\star)$.

Définition: Soit $(G,\star)$ un groupe et $H =< g_1, g_2, \ldots, g_p >$.

Un mot $g_k^{n_k}\, g_l^{n_l}\, \ldots\, g_z^{n_z}$ est **réduit** si l'écriture du mot comporte le minimum de facteurs.

Exemple 8:

- Soit $g, h \in G$ et considérons le mot $ghghh^{-1}$ qui a 5 facteurs. Il n'est pas réduit car $ghghh^{-1} = ghg(hh^{-1}) = ghg$.
- Les mots gh et $g^{-1}hghg^{-1}$ sont par contre réduits si $\star$ n'est pas commutative.

Exercice 5.9: Soit $(G,\star)$ un groupe et $x, y, z \in G$; considérons $H =< x, y, z >$

a) Écrire trois éléments distincts de H

b) Est-ce que $xyz(yz)^{-1}$ est un mot réduit ?

c) Est-ce que $xyy^{-1}z^{-1}yx$ est égal à $xz^{-1}yzz^{-1}x$?

d) Exprimer $x^2y^3(y^3x^2)^{-1}y^{-3}$ et $(xzy)^{-1}xzy^2$ sous forme réduite.

Exercice 5.10: Trouver tous les sous-groupes de :

a) $(\mathbb{Z}_{12}, +)$

b) $(\mathbb{Z}_8, +)$

c) $(\mathbb{Z}_7^\star, \cdot)$

A

Bibliographie et ressources Internet

Bibliographie

1. Eric Laydu, *Groupes et action de groupes (2011)*, Gymnase d'Yverdon
2. Louis Gred, *Notions fondamentales de la mathématique élémentaire (1980)*, LEP
3. Tony Crilly, *Juste assez de maths pour briller en société (2009)*, Dunod

Ressources Internet

1. Professeurs des Universitéés de Lille, Rennes et Marne la Vallée, *Exo7 Groupes*,

   `http://exo7.emath.fr/cours/ch_groupe.pdf`

2. Farouk Boucekkine, *Introduction à la théorie des Groupes*,

   `http://www.math.ens.fr/culturemath/maths/pdf/algebre/groupesFirst.pdf`

3. S. F. Ellermeyer, *Introduction to Groups (2006)*

   `http://science.kennesaw.edu/~sellerme/sfehtml/classes/math4361/...`

4. S. F. Ellermeyer, *Subgroups of Groups (2006)*

   `http://science.kennesaw.edu/~sellerme/sfehtml/classes/math4361/...`

5. Et encore d'autres idées à trouver sur Google :

   `https://www.google.ch/search?q=théorie+des+groupes`
   `https://www.google.ch/search?q=group+theory`

B

Quelques éléments de solutions

B.1 Mise en place

Exercice 1.1:

a) non, car $\dfrac{x+y}{2}$ n'appartient pas forcément à $\mathbb{Z}$. ($x = 1$ et $y = 2$)

b) non, car $\sqrt{xy}$ n'appartient pas forcément à $\mathbb{R}$. ($x = 1$ et $y = -4$)

c) oui **d)** oui **e)** oui **f)** oui **g)** oui

h) non, car $x \cdot y + \dfrac{x}{y}$ n'appartient pas forcément à $\mathbb{Z}$. ($x = 1$ et $y = 2$)

Exercice 1.2:

c) commutative **d)** commutative **e)** commutative
f) commutative **g)** non commutative

Exercice 1.3:

$(x \star y) \star z = \dfrac{x+y+z+xyz}{xy+xz+yz+1}$ qui est bien égal à $x \star (y \star z)$

Exercice 1.4:

$\star$ est une loi de composition interne commutative et associative.

Exercice 1.5:

$+$ est une loi de composition interne commutative et associative.

Exercice 1.6:

$\star$ est une loi de composition interne commutative et associative.

Exercice 1.7:

La seule valeur possible est $m = 0$ en effet :

$$(x \star y) \star z = xyzm^2 + zm + 1 \qquad \text{et} \qquad x \star (y \star z) = xyzm^2 + xm + 1$$

Exercice 1.8:

$\star$ est une loi de composition interne commutative et associative.

Exercice 1.9:

a) Le plus simple est de présenter ceci sous la forme d'un tableau :

$\overset{\circ}{\swarrow}$	i	f	g	h
i	i	f	g	h
f	f	i	h	g
g	g	h	i	f
h	h	g	f	i

b) $\circ$ est commutative.

c) $\circ$ est associative. Formellement, il s'agirait d'effectuer $4^3 = 64$ vérifications. Peut-on en éviter quelques-unes ?

Exercice 1.10:

Pas de condition sur b et $a \neq 0$

Exercice 1.11:

a) Deux bonnes raisons :

- Il existe des valeurs de $y \in \mathbb{R}$ pour lesquelles, il n'existe pas de x vérifiant $y = x^2$.
- Il existe des valeurs de $y \in \mathbb{R}$ pour lesquelles, la valeur x vérifiant $y = x^2$ existe mais n'est pas unique.

b) f est alors bien bijective.

Exercice 1.12:

a) $x \in \mathbb{Q} \setminus \{1\}$

b) ${}^r f(x) = \dfrac{x+3}{x-2}$

c) $f : \mathbb{Q} \setminus \{1\} \to \mathbb{Q} \setminus \{2\}$

B.2 Notion de groupe

Exercice 2.1:

n'a pas de structure de groupe, car il n'existe pas d'opposé.

Exercice 2.2:

$\left(\mathbb{R}^2, +\right)$ est un groupe abélien.

Exercice 2.3:

a) $\star$ n'est pas une opération interne.

b) $\star$ n'est pas une opération interne.

c) $\star$ n'a pas d'élément neutre à gauche, ($e \star x = x$ n'est pas vérifié pour tout x).

Exercice 2.4:

Oui, d'ordre 4.

Exercice 2.5:

b)

- Il s'agit bien d'une loi de composition interne, c'est-à-dire : $f_b \circ f_a = f_{a+b} \in E$.
- Elle est bien associative :

  $\big(f_c \circ (f_b \circ f_a)\big)(x) = (f_c \circ f_{a+b})(x) = (x+a+b)+c = x+a+b+c$

  $\big((f_c \circ f_b) \circ f_a\big)(x) = (f_{b+c} \circ f_a)(x) = (x+a)+b+c = x+a+b+c$
- L'élément neutre : f_0.
- le symétrique de tout f_b est f_{-b}.

Exercice 2.6:

- Il s'agit bien d'une loi de composition interne, c'est-à-dire :

  $(ac-bd)^2 + (ad+bc)^2$ est bien égal à 1.
- Elle est bien associative :

  $((a\,;b) \star (c\,;d)) \star (e\,;f) = (ace - adf - bcf - bde\,;acf + ade + bce - bdf)$

  $(a\,;b) \star ((c\,;d) \star (e\,;f)) = (ace - adf - bcf - bde\,;acf + ade + bce - bdf)$
- L'élément neutre : $(1\,;0)$ (*s'obtient et se justifie par un système d'équations*)
- Le symétrique de tout $(a\,;b)$ est bien défini : $(a\,;-b)$ (*même remarque*)

Exercice 2.7:

b) L'élément neutre : $1 + 0\sqrt{2}$ (*s'obtient intuitivement mais doit être justifé*)

c) Le symétrique de tout $a + b\sqrt{2}$ est $\dfrac{a}{a^2-2b^2} + \dfrac{-b}{a^2-2b^2}\sqrt{2}$

(*s'obtient et se justifie par un système d'équations*)

B.3 Quelques groupes célèbres

Exercice 3.1:

Pourra être vu ensemble à votre demande.

Exercice 3.2:

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 1 & 3 & 5 \end{pmatrix} \qquad \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 6 & 1 \end{pmatrix}$$

$$^r\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 5 & 4 & 3 \end{pmatrix} \qquad ^r\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 3 & 4 \end{pmatrix}$$

$$^r(\beta \circ \alpha) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 3 & 2 & 5 \end{pmatrix} \qquad ^r(\alpha \circ \beta) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 3 & 6 & 2 \end{pmatrix}$$

Exercice 3.3:

$$\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$$

Exercice 3.4:

La loi est bien interne, l'associativité est issue de S_3, l'élément neutre est id, les 2 éléments restants sont symétriques l'un de l'autre.

Exercice 3.5:

$S_1 = \{id\}$ avec $id = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $S_2 = \{id, \beta\}$ avec $id = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ et $\beta = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

Exercice 3.6:

$\overset{+}{\swarrow}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Exercice 3.7:

$\overset{\cdot}{\swarrow}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\overset{\cdot}{\swarrow}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Contrairement au tableau précédent, la loi n'est pas interne, $\overline{2}$ n'admet pas d'inverse et on ne retrouve pas tous les éléments du groupe dans chaque ligne et chaque colonne.

Exercice 3.8:

Soit $\overline{a}$, $\overline{b}$ et $\overline{c} \in \mathbb{Z}_n$, on a :

$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a \cdot b} \cdot \overline{c} = \overline{a \cdot b \cdot c} = \overline{a} \cdot \overline{b \cdot c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$$

Exercice 3.9:

a) La loi est bien interne, l'associativité est issue de celle de $\mathbb{Z}_n$, l'élément neutre est 1 et 2 et 4 sont inverse l'un de l'autre. On peut également observer ceci dans la table de multiplication.

b) La loi n'est pas interne et 2 n'admet pas d'inverse.

$\swarrow$	$\overline{1}$	$\overline{2}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$
$\overline{4}$	$\overline{4}$	$\overline{1}$	$\overline{2}$

a)

$\swarrow$	$\overline{1}$	$\overline{2}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{1}$

b)

Exercice 3.10:

a) $A + A = \begin{pmatrix} 2 & 4 \\ -6 & 2 \end{pmatrix}, A + B = \begin{pmatrix} 3 & 1 \\ -2 & 2 \end{pmatrix}, A - B = \begin{pmatrix} -1 & 3 \\ -4 & 0 \end{pmatrix}, B - A = \begin{pmatrix} 1 & -3 \\ 4 & 0 \end{pmatrix}$

b) $2A = \begin{pmatrix} 2 & 4 \\ -6 & 2 \end{pmatrix}, 3A = \begin{pmatrix} 3 & 6 \\ -9 & 3 \end{pmatrix}, -5B = \begin{pmatrix} -10 & 5 \\ -5 & -5 \end{pmatrix}$

Exercice 3.11:

a) $AB = \begin{pmatrix} 4 & 1 \\ -5 & 4 \end{pmatrix}, BA = \begin{pmatrix} 5 & 3 \\ -2 & 3 \end{pmatrix}, ABA = \begin{pmatrix} 1 & 9 \\ -17 & -6 \end{pmatrix}$

b) $A^2 = \begin{pmatrix} -5 & 4 \\ -6 & -5 \end{pmatrix}, A^3 = \begin{pmatrix} -17 & -6 \\ 9 & -17 \end{pmatrix}$

Exercice 3.12:

La matrice I_2 est d'ordre 1, les autres sont d'ordre 2.

Exercice 3.13:

En utilisant le même codage que précédemment, on obtient la table :

$\swarrow$	I_2	A	B	C
I_2	I_2	A	B	C
A	A	I_2	C	B
B	B	C	I_2	A
C	C	B	A	I_2

qui permet de visualiser que la loi est interne, l'existence des éléments symétriques. L'associativité est issue de celle de $M_2(\mathbb{R})$.

Exercice 3.14:

a) $A^2 = \begin{pmatrix} \cos^2\alpha - \sin^2\alpha & -\cos\alpha\sin\alpha - \sin\alpha\cos\alpha \\ \cos\alpha\sin\alpha + \sin\alpha\cos\alpha & -\sin^2\alpha + \cos^2\alpha \end{pmatrix} = \begin{pmatrix} \cos 2\alpha & -\sin 2\alpha \\ \sin 2\alpha & \cos 2\alpha \end{pmatrix}$

b) $A^3 = \begin{pmatrix} \cos 2\alpha & -\sin 2\alpha \\ \sin 2\alpha & \cos 2\alpha \end{pmatrix} \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} =$

$= \begin{pmatrix} \cos 2\alpha\cos\alpha - \sin 2\alpha\sin\alpha & -\cos 2\alpha\sin\alpha - \sin 2\alpha\cos\alpha \\ \sin 2\alpha\cos\alpha + \cos 2\alpha\sin\alpha & -\sin 2\alpha\sin\alpha + \cos 2\alpha\cos\alpha \end{pmatrix} = \begin{pmatrix} \cos 3\alpha & -\sin 3\alpha \\ \sin 3\alpha & \cos 3\alpha \end{pmatrix}$

$A^4 = \begin{pmatrix} \cos 3\alpha & -\sin 3\alpha \\ \sin 3\alpha & \cos 3\alpha \end{pmatrix} \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} =$

$= \begin{pmatrix} \cos 3\alpha\cos\alpha - \sin 3\alpha\sin\alpha & -\cos 3\alpha\sin\alpha - \sin 3\alpha\cos\alpha \\ \sin 3\alpha\cos\alpha + \cos 3\alpha\sin\alpha & -\sin 3\alpha\sin\alpha + \cos 3\alpha\cos\alpha \end{pmatrix} = \begin{pmatrix} \cos 4\alpha & -\sin 4\alpha \\ \sin 4\alpha & \cos 4\alpha \end{pmatrix}$

c) Exercice BONUS (avec la démonstration !!)

Exercice 3.15:

En posant $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $N = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, on obtient dans les 2 cas : $adeh - adfg - bceh + bcfg$

Exercice 3.16:

$A^{-1} = \frac{1}{7}\begin{pmatrix} 1 & -2 \\ 3 & 1 \end{pmatrix}, B^{-1} = \frac{1}{3}\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}$

B.4 Tables de Cayley et isomorphisme

Exercice 4.1:

a) Oui, l'élément a.

b) Oui, on retrouve l'élément neutre a dans chacune des colonnes. $c' = d$

c) Non, le tableau n'est pas symétrique par rapport à la diagonale $\ddots$.

d) Il s'agirait formellement d'effectuer $4 \cdot 4 \cdot 4 = 64$ vérifications. Même si certaines sont immédiates par l'apparition de l'élément neutre dans le calcul, on peut compter une bonne dizaine de minutes pour effectuer tous les contrôles.

e) Oui, $(E,\star)$ est bien un groupe.

f) La réponse n'est bien sûr pas 2 fois plus longue, mais d'environ 8 fois.

Exercice 4.2:

Supposons $j \neq k$,

$$\begin{aligned} b_{ij} = b_{ik} &\Rightarrow a_i \star a_j = a_i \star a_k \Rightarrow a_i' \star (a_i \star a_j) = a_i' \star (a_i \star a_k) \\ &\Rightarrow (a_i' \star a_i) \star a_j = (a_i' \star a_i) \star a_k \Rightarrow e \star a_j = e \star a_k \\ &\Rightarrow a_j = a_k \Rightarrow j = k \end{aligned}$$

Raisonnement sur les colonnes avec $j \neq k$: il s'agit de construire la même contradiction à partir de $b_{ji} = b_{ki}$.

Exercice 4.3:

a) Par exemple : $b \star (a \star d) = b \star c = d$
$(b \star a) \star d = c \star d = b$

b) L'affirmation de l'exercice précédent ne doit pas être interprétée comme une équivalence :

Groupe $\Rightarrow$ *Particularité* **mais**
Particularité $\not\Leftarrow$ *Groupe* car l'associativité n'est pas vérifiée :-/

Exercice 4.4:

a)

$\star\swarrow$	r	s	t	u
r	s	r	u	t
s	r	s	t	u
t	u	t	s	r
u	t	u	r	s

b)

$\star\swarrow$	r	s	t	u
r	r	s	t	u
s	s	t	u	r
t	t	u	r	s
u	u	r	s	t

Avez-vous vraiment contrôlé l'associativité dans tous les cas ? ?

Exercice 4.5:

a) Il s'agit du groupe trivial

$\cdot\swarrow$	e	a
e	e	a
a	a	e

b) À voir ensemble.

Exercice 4.6:

a) Il n'y en a qu'un possible dont la table de Cayley est :

$\cdot\swarrow$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

b) À voir ensemble.

Exercice 4.7:

a) Les 2 tables sont :

$\star\swarrow$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\star\swarrow$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

b) À voir ensemble.

Exercice 4.8:

Il suffit de permuter les lignes et colonnes a et b puis de substituer les étiquettes a par b et b par a.

Exercice 4.9:

À voir ensemble

Exercice 4.10:

a) r_0 : l'identité, r_1,r_2 : rotation de centre O et d'angle 120°, respectivement 240°.

b) Sa table de Cayley est isomorphe à celle du groupe d'ordre 3 (cf. exercice **4.6**).

$\circ\swarrow$	r_0	r_1	r_2
r_0	r_0	r_1	r_2
r_1	r_1	r_2	r_0
r_2	r_2	r_0	r_2

isomorphe à

$\cdot\swarrow$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Exercice 4.11:

Les tables de Cayley obtenues (pour différentes valeurs de n) ne sont-elles pas isomorphes à celles obtenues sur des groupes déjà étudiés ?

B.5 Sous-groupes

Exercice 5.1:

Pas de réponse proposée, pourra être vu ensemble.

Exercice 5.2:

Si G est l'ensemble de l'exercice 1.9.
$A = \{i(x), f(x)\}$ et $B = \{i(x), g(x)\}$ répondent à la question.

Exercice 5.3:

$(\mathcal{F},\circ)$ n'est pas un groupe, car le symétrique de f n'existe pas toujours.
$\mathcal{E}$ est l'ensemble contenant toutes les bijections de $\mathbb{R}$ dans $\mathbb{R}$.

Exercice 5.4:

Oui, il suffit de montrer que la loi est bien interne et que tout élément de S admet bien un symétrique dans S.

Exercice 5.5:

Oui, il suffit de montrer que la loi est bien interne et que tout élément de S admet bien un symétrique dans S.

Exercice 5.6:

a) oui

b) non, car $(x\,;y)$ n'a pas d'inverse dans E

c) oui

d) oui

Exercice 5.7:

a) non, $(1\,;1) \notin E$

b) non, car l'opération n'est pas interne

c) non, car $(1\,;0)$ n'a pas d'inverse

d) non, car $(1\,;0)$ n'a pas d'inverse

e) non, car l'opération n'est pas interne

Exercice 5.8:

$\star$ est bien une opération interne de H ; si $a, b \in H, a = g^n$ et $b = g^m \Rightarrow g^n g^m = g^{n+m} \in H$.
Si $a = g^n \in H$, alors $a^{-1} = g^{-n}$ car $g^n g^{-n} = g^{n-n} = g^0 = e$.

Exercice 5.9:

a) x, y, z ou x, x^2, x^3 ou x, xy, xz.

b) non car $xyz(yz)^{-1} = xyzz^{-1}y^{-1} = x$

c) oui car $xyy^{-1}z^{-1}yx = xz^{-1}yzz^{-1}x = xz^{-1}yx$

d) $x^2y^3(y^3x^2)^{-1}y^{-3} = x^2y^3x^{-2}y^{-6}, (xzy)^{-1}xzy^2 = y^{-1}z^{-1}x^{-1}xzy^2 = y$

Exercice 5.10:

a) $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}_{12}$

b) $\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_8$

c) $< 1 >, < 2 >=< 4 >, < 6 >, \mathbb{Z}_7^\star$

Si vous souhaitez commander ou utiliser ce polycopié dans vos classes, merci de prendre contact avec son auteur en passant par son site web :

http ://www.javmath.ch